

PEDIDO

SOLICITAÇÃO DE COMPRAS / SERVIÇO

1. Dados do Solicitante

1.1. Nome da Unidade Solicitante

DIRETORIA DE DESENVOLVIMENTO SISTEMAS E PROJETOS –
DDSP/STI

1.2. Data da Solicitação

01 / 04 / 2023

1.3. Servidor Solicitante (contato)

ANTÔNIO LOPES
JÚNIOR

1.4. Telefone / Ramal

(31) 2522-8690

2. Dados do Produto ou Serviço

2.1. Descrição detalhada do bem ou serviço:

Aquisição de solução de segurança de rede com gerenciamento e instalação com configuração, observadas as condições e especificações técnicas estabelecidas no Termo de Referência (Documento SEI nº 0105943).

2.2. Justificativa/Finalidade da Aquisição/Contratação:

Compete a Superintendência de Tecnologia da Informação assegurar que a plataforma tecnológica, equipamentos e sistemas, adotados pela DPMG atenda plenamente as demandas das áreas, para o desenvolvimento da prestação do serviço de assistência jurídica integral e gratuita com qualidade, eficiência e presteza.

A continuidade dos serviços de Tecnologia da Informação e Comunicação -TIC é um dos atributos principais a ser levado em conta, tendo em vista que a interrupção dos serviços públicos tem potencial de causar transtornos a Administração.

Em virtude da criação de novos sistemas corporativos implantados na DPMG, essenciais por se tratar da melhoria do atendimento Público, existe uma necessidade de manter e proteger o ambiente tecnológico.

Com a contratação da solução de segurança pretende-se alcançar os seguintes benefícios de aumentar a segurança da informação para os serviços de tecnologia prestados pela Instituição, assegurar a sustentabilidade dos serviços que envolvem a infraestrutura de TIC, aumento da confidencialidade de dados sigilosos, disponibilidade e integridade de sistemas críticos e adotar medidas de privacidade e proteção das informações dos servidores, colaboradores, prestadores de serviços e usuários.

Diante do exposto, a aquisição da solução de segurança, incluindo a garantia dos equipamentos e instalação/configuração, faz-se necessário para continuar manter a integridade, disponibilidade e confidencialidade, dos dados e informações da Instituição.

2.3.Quantidade:	2.4. Unidade de Aquisição:	2.5. Código SIAD:	2.6. Valor Unitário Estimado/Mensal Estimado:	2.7. Valor Total Estimado/Anual Estimado:
2.8. Valor Total Estimado:				
2.9. Assinatura do Solicitante:				



Documento assinado eletronicamente por **Antônio Lopes Junior**, **Diretor de Desenvolvimento de Sistemas e Projetos**, em 18/05/2023, às 17:57, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://defensoria.mg.def.br/portal-sei> informando o código verificador **0105677** e o código CRC **80CE9747**.

9990000001.003832/2023-69

0105677v4

1. OBJETO

O presente termo de referência tem por objeto a aquisição de solução de segurança de rede com gerenciamento e instalação com configuração, observadas as condições e especificações técnicas estabelecidas nesse documento.

2. DA QUANTIDADE E DESCRIÇÃO DO OBJETO

2.1.DO LOTE

LOTE 1

ITEM	QUANT.	UNIDADE	DESCRIÇÃO	CÓDIGO SIAD
01	01	UN	FIREWALL (HARDWARE), com 36 meses de garantia.	1910434
02	01	UN	SOLUCAO GERENCIAMENTO DE EVENTOS DE SEGURANCA	1910418
03	08	UN	MODULO TRANSCEPTOR PARA FIBRA OPTICA - PADRAO: SFP; CONECTOR: TIPO LC-DUPLEX;	19100027
04	08	UN	MÓDULO TRANSCEPTOR PARA FIBRA ÓPTICA - PADRAO: SPF+; CONECTOR: LC PADRAO SR 10GB;	1726145
05	02	UN	SERVICO DE MONTAGEM, INSTALACAO, CONFIGURACAO E PADRONIZACAODE SOFTWARE E EQUIPAMENTO DA SOLUCAO DE DATACENTER	46000

3. DETALHAMENTO DO OBJETO

Configurações mínimas conforme ANEXO I – Especificação Técnica.

4. DO LOTE:

4.1.Lote Único

Justificativa: aquisição de o item único com prestação de serviço de instalação. A unicidade do objeto não restringe a competitividade, sendo comum a forma de contratação pelo mercado e impede lançar luzes acerca da centralização de responsabilidade, a qual é considerada não apenas em vista do acompanhamento de problemas, mas, para em termos claros, prover a verificação de casos e, mormente a atribuição de responsabilidade. Aufere-se então nítido controle sobre a execução contratual.

Ademais, a unicidade do objeto busca evitar contratação dispendiosa e resguardar a segurança da informação para a Administração, cujos fatores técnicos objetivam a satisfação do interesse público, com racionalização de recursos (humanos e orçamentários), otimização da gestão administrativa com a gerência de contrato único, conferindo eficácia e segurança na execução do objeto quando o mesmo fornecedor fica responsável pela instalação do equipamento.

5. JUSTIFICATIVA DA CONTRATAÇÃO

- 5.1. Compete a Superintendência de Tecnologia da Informação assegurar que a plataforma tecnológica, equipamentos e sistemas, adotados pela DPMG atenda plenamente as demandas das áreas, para o desenvolvimento da prestação do serviço de assistência jurídica integral e gratuita com qualidade, eficiência e presteza.
- 5.2. A continuidade dos serviços de Tecnologia da Informação e Comunicação -TIC é um dos atributos principais a ser levado em conta, tendo em vista que a interrupção dos serviços públicos tem potencial de causar transtornos a Administração.
- 5.3. Em virtude da criação de novos sistemas corporativos implantados na DPMG, essenciais por se tratar da melhoria do atendimento Público, existe uma necessidade de manter e proteger o ambiente tecnológico.
- 5.4. Com a contratação da solução de segurança pretende-se alcançar os seguintes benefícios de aumentar a segurança da informação para os serviços de tecnologia prestados pela Instituição, assegurar a sustentabilidade dos serviços que envolvem a infraestrutura de TIC, aumento da confidencialidade de dados sigilosos, disponibilidade e integridade de sistemas críticos e adotar medidas de privacidade e proteção das informações dos servidores, colaboradores, prestadores de serviços e usuários;
- 5.5. Diante do exposto, a aquisição da solução de segurança, incluindo a garantia dos equipamentos e instalação/configuração, faz-se necessário para continuar manter a integridade, disponibilidade e confidencialidade, dos dados e informações da Instituição.

6. DA METODOLOGIA

- 6.1 O critério de aceitação das propostas será o de **Menor Preço Global por Lote**, de acordo com as especificações constantes neste Termo de Referência.

7. DA CLASSIFICAÇÃO DE BENS

7.1 Os bens a serem contratados enquadram-se na classificação de bens comuns, nos termos da Lei 10.520/2002 e do art. 2º da Lei Estadual 14.167/02.

8. QUALIFICAÇÃO TÉCNICA:

8.1 Não será necessário a comprovação de atestado(s) de capacidade técnica.

9. DA PROVA DE CONCEITO:

9.1 Não será exigida prova de conceito.

10. DA EXECUÇÃO DO OBJETO:

10.1 PRAZO DE ENTREGA DO ITEM: a entrega do item deverá ser de, no máximo, 120 (cento e vinte) dias CORRIDOS, contados a partir da assinatura do contrato.

11. DO LOCAL DE ENTREGA:

11.1 Na Companhia de Tecnologia da Informação do Estado de Minas Gerais - Prodemge, situada na Rua da Bahia, 2277 - Lourdes, Belo Horizonte - MG.

11.2 CONDIÇÕES DE RECEBIMENTO:

11.2.1 O recebimento dos produtos, objeto deste Termo de Referência, deverá ser realizado perante gestor(es), a ser designado pela CONTRATANTE.

12. DO PAGAMENTO:

12.1 O pagamento será realizado por item no valor integral através do Sistema Integrado de Administração Financeira – SIAFI/MG, a crédito do beneficiário em qualquer instituição bancária, no prazo de até 30 (trinta) dias corridos a partir da apresentação da nota fiscal devidamente atestada pela Diretoria de Suporte e Administração de Redes, acompanhado dos documentos fiscais.

12.2 As Notas Fiscais que apresentarem incorreções serão devolvidas à CONTRATADA e o prazo para o pagamento passará a correr a partir da data da reapresentação do documento, considerado válido pela CONTRATANTE.

12.3 Na hipótese de irregularidade no CAGEF, a CONTRATADA deverá regularizar sua situação perante o cadastro. O prazo para pagamento será interrompido, reiniciando a contagem a partir da data de sua regularização.

13. DO CONTRATO:

- 13.1** Encerrado o procedimento licitatório, o representante legal do licitante declarado vencedor será convocado para firmar o termo de contrato, aceitar ou retirar o instrumento equivalente, de acordo com os art. 62, da Lei 8.666/93 e art. 4º, XXI, da Lei 10.520/2002.
- 13.2** O contrato terá vigência por 12 (doze) meses, a partir da publicação de seu extrato no Diário Oficial do Estado de Minas Gerais.

14. DOS PROCEDIMENTOS DE FISCALIZAÇÃO E GERENCIAMENTO DA RELAÇÃO JURÍDICA:

Atendendo às exigências contidas no inciso III do art. 58 e §§ 1º e 2º, do artigo 67 da Lei nº. 8.666 de 1993, serão designados:

- 14.1** Para a Gestão, o Diretor de Desenvolvimento de Sistemas e Projetos - DDSP.
- 14.2** Para a Fiscalização, o Diretor de Informação e Dados, sendo este o Agente Fiscalizador.
- 14.3** Em caso de eventual irregularidade, inexecução ou desconformidade na execução do contrato ou instrumento equivalente, o Agente Fiscalizador dará ciência à CONTRATADA, por escrito, para adoção das providências necessárias para sanar as falhas apontadas.
- 14.4** A fiscalização de que trata esta cláusula não exclui, nem reduz a responsabilidade da CONTRATADA por quaisquer irregularidades, inexecuções ou desconformidades havidas na execução do objeto, aí incluídas imperfeições de natureza técnica ou aquelas provenientes de vício redibitório, tal como definido pela lei civil.
- 14.5** O CONTRATANTE reserva-se o direito de rejeitar, no todo ou em parte, o objeto da contratação, caso ele afaste-se das especificações do Edital, seus anexos e da proposta da CONTRATADA.
- 14.6** As decisões e providências que ultrapassarem a competência do Fiscal do Contrato serão encaminhadas à autoridade competente da CONTRATANTE para adoção das medidas convenientes, consoante disposto no § 2º do art. 67, da Lei nº. 8.666/93.
- 14.7** Caberá ao gestor os controles administrativos/financeiros necessários ao pleno cumprimento dos requisitos das especificações do Edital.

15. DAS GARANTIAS:

15.1 GARANTIA FINANCEIRA DA EXECUÇÃO:

- 15.1.1** Não será exigida garantia de execução contratual.

15.2 GARANTIA DO PRODUTO

15.2.1 A garantia de funcionamento para todos os itens será de 36 (trinta e seis) meses, na modalidade On-site, contada a partir do recebimento definitivo do equipamento entregue, sem prejuízo de qualquer política de garantia adicional oferecida pelo fabricante.

16. DA SUBCONTRATAÇÃO:

16.1 Não se aplica.

17. OBRIGAÇÕES ESPECÍFICAS DAS PARTES:

17.1 DA CONTRATADA:

- 17.1.1 Fornecer os produtos nas quantidades, prazos e condições pactuadas, de acordo com as exigências constantes neste Termo de Referência.
- 17.1.2 Emitir faturas no valor pactuado, apresentando-as à CONTRATANTE para ateste e pagamento.
- 17.1.3 Atender prontamente às orientações e exigências inerentes à execução do objeto adquirido.
- 17.1.4 Assegurar à CONTRATANTE o direito de sustar, recusar, mandar desfazer ou refazer qualquer serviço/produto que não esteja de acordo com as normas e especificações técnicas recomendadas neste Termo de Referência.
- 17.1.5 Assumir inteira responsabilidade pela prestação dos serviços, responsabilizando-se por eventual transporte, acondicionamento e descarregamento dos materiais necessários a prestação, se houver.
- 17.1.6 Executar ou acompanhar (caso seja realizado pelo fabricante do equipamento) os serviços conforme especificações deste Termo de Referência e de sua proposta, para o perfeito cumprimento da instalação do objeto ora adquirido, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas neste Termo de Referência e em sua proposta.
- 17.1.7 Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado ao Estado ou à entidade estadual, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a CONTRATANTE autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos.

- 17.1.8 Responsabilizar-se pela garantia dos materiais empregados na prestação dos serviços, dentro dos padrões adequados de qualidade, segurança, durabilidade e desempenho, conforme previsto na legislação em vigor e na forma exigida neste Termo de Referência.
- 17.1.9 Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do objeto deste Termo de Referência.
- 17.1.10 Não transferir para a CONTRATANTE a responsabilidade pelo pagamento dos encargos estabelecidos no item anterior, quando houver inadimplência da CONTRATADA, nem onerar o objeto deste Termo de Referência.
- 17.1.11 Manter, durante toda a execução do objeto, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
- 17.1.12 Manter preposto, caso necessário, aceito pela Administração, para representá-lo no local da instalação do objeto adquirido.

17.2 DA CONTRATANTE:

- 17.2.1 Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis.
- 17.2.2 Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com os termos de sua proposta.
- 17.2.3 Notificar a CONTRATADA por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas.
- 17.2.4 Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA.
- 17.2.5 Aplicar à CONTRATADA as sanções regulamentares.

18. SANÇÕES ADMINISTRATIVAS:

- 18.1 A licitante/adjudicatária que cometer qualquer das infrações, previstas na Lei Federal nº 8.666, de 21 de junho de 1993, na Lei Federal nº 10.520, de 17 de julho de 2002, Lei Estadual nº 14.167, de 10 de janeiro de 2002 e no Decreto Estadual nº 45.902, de 27 de janeiro de 2012, e no do Decreto nº 48.012, de 22 de julho de 2020, ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

- 18.1.1 Advertência por escrito;

18.1.2 Multa de até:

18.1.2.1 0,3% (três décimos por cento) por dia, até o trigésimo dia de atraso, sobre o valor do objeto não executado;

18.1.2.2 2,0% (dois por cento) sobre o valor total do contrato ou instrumento equivalente, em caso de descumprimento das demais obrigações contratuais ou norma da legislação pertinente.

18.1.2.3 20,0% (vinte por cento) sobre o valor do objeto após ultrapassado o prazo de 30 dias de atraso, ou no caso de não entregue objeto, ou entrega com vícios ou defeitos ocultos que o torne impróprio ao uso a que é destinado, ou diminua-lhe o valor ou, ainda fora das especificações contratadas;

18.1.3 Suspensão do direito de participar de licitações e impedimento de contratar com a Administração, pelo prazo de até 2 (dois) anos;

18.1.4 Impedimento de licitar e contratar com a Administração Pública Estadual, nos termos do art. 7º da Lei Federal nº 10.520, de 17 de julho de 2002;

18.1.5 Declaração de inidoneidade para licitar ou contratar com a Administração Pública;

18.2 A sanção de multa poderá ser aplicada cumulativamente às demais sanções previstas nos itens 18.1.1, 18.1.2, 18.1.3, 18.1.4, 18.1.5.

18.3 A multa será descontada da garantia do contrato, quando houver, e/ou de pagamentos eventualmente devidos ao infrator e/ou cobrada administrativa e/ou judicialmente.

18.4 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo incidental apensado ao processo licitatório ou ao processo de execução contratual originário que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto no Decreto Estadual nº. 45.902, de 27 de janeiro de 2012, bem como o disposto na Lei Federal nº 8.666, de 21 de junho de 1993 e Lei Estadual nº 14.184, de 31 de janeiro de 2002.

18.5 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

18.5.1 Não serão aplicadas sanções administrativas na ocorrência de casos fortuitos, força maior ou razões de interesse público, devidamente comprovados.

18.6 A aplicação de sanções administrativas não reduz nem isenta a obrigação da CONTRATADA de indenizar integralmente eventuais danos causados a Administração ou a terceiros, que poderão ser apurados no mesmo processo administrativo sancionatório.

- 18.7** As sanções relacionadas nos itens 18.1.3 a 18.1.5 serão obrigatoriamente registradas no Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual – CAFIMP e no CAGEF.
- 18.8** As sanções de suspensão do direito de participar em licitações e impedimento de licitar e contratar com a Administração Pública poderão ser também aplicadas àqueles que:
- 18.8.1 Retardarem a execução do objeto;
 - 18.8.2 Comportar-se de modo inidôneo;
- Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances;
- 18.8.3 Apresentarem documentação falsa ou cometerem fraude fiscal.
- 18.9** Durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei Federal nº 12.846, de 1º de agosto de 2013, e pelo Decreto Estadual nº 46.782, de 23 de junho de 2015, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à Controladoria-Geral do Estado, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

Belo Horizonte, 03 de abril de 2023.

LEONARDO BRUNO
POSSA
ANDRADE:70005160

Assinado de forma digital por
LEONARDO BRUNO POSSA
ANDRADE:70005160
Dados: 2023.06.15 16:07:32 -03'00'

Diretoria de Informação e Dados
Superintendência de Tecnologia da Informação

ANEXO I DO TERMO DE REFERÊNCIA – ESPECIFICAÇÃO TÉCNICA

1. CARACTERÍSTICAS GERAIS

- 1.1. Deverão ser entregues todos os itens e acessórios necessários para interligação dos equipamentos adquirido.
- 1.2. Todos os equipamentos e componentes ofertados devem ser novos, sem uso anterior, não remanufaturados, não reconicionados e estar em linha de fabricação pelos fabricantes.
- 1.3. Devem ser fornecidas, junto com o equipamento, todas as licenças de software necessárias para todas as portas ativas ofertadas em todas as funcionalidades exigidas neste Termo de Referência.
- 1.4. Todos os componentes dos produtos ofertados devem ser do mesmo fabricante do componente principal, ou serem homologados por ele, podendo a CONTRATANTE realizar diligências junto ao mesmo para esta comprovação, quando da etapa de recepção técnica.

2. Firewall – características mínimas

- 2.1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do datacenter da CONTRATANTE;
- 2.2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante;
- 2.3. Cada appliance físico deve possuir, pelo menos, 16 (dezesesseis) interfaces 1 Gigabit Ethernet padrão 1000Base-T, 4 (quatro) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede, 2 (duas) interfaces 40 Gigabit Ethernet padrão 40GBase-LR e 2 (duas) interfaces 25 Gigabit Ethernet padrão 25GBase-LR. Caso sejam ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX;
- 2.4. Deve possuir interface console com conector RJ-45 ou USB para gerenciamento local;
- 2.5. Cada appliance físico deve suportar fonte de alimentação redundante (Hot Swappable) com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação;
- 2.6. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas;

- 2.7. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
- 2.8. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo;
- 2.9. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica;
- 2.10. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso;
- 2.11. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
- 2.12. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
- 2.13. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
- 2.14. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados;
- 2.15. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 9.408 (nove mil e quatrocentos e oito mil) portas de switch ou um total de 196 (cento e noventa e seis) switches;
- 2.16. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas;
- 2.17. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados;
- 2.18. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
- 2.19. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
- 2.20. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
- 2.21. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE

- nas interfaces dos switches;
- 2.22. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
- 2.23. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;
- 2.24. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;
- 2.25. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
- 2.26. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 2000 (dois mil) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor;
- 2.27. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;
- 2.28. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet;
- 2.29. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
- 2.30. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6;
- 2.31. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
- 2.32. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
- 2.33. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel;

- 2.34. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
- 2.35. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel;
- 2.36. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;
- 2.37. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso;
- 2.38. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos;
- 2.39. A solução deverá ser capaz de encaminhar 48 Gbps de tráfego encapsulado via VPN IPSec;
- 2.40. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- 2.41. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 2.42. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- 2.43. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs;
- 2.44. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec;
- 2.45. A solução deverá ser capaz de atuar como um cliente de VPN SSL;
- 2.46. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
- 2.47. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL;
- 2.48. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN –

ADVPN ou tecnologia similar;

- 2.49. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
- 2.50. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;
- 2.51. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;
- 2.52. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
- 2.53. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
- 2.54. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
- 2.55. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;
- 2.56. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
- 2.57. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
- 2.58. A solução deve permitir ao administrador da rede determinar os horários e dias da

- semana que as redes (SSIDs) estarão disponíveis aos usuários;
- 2.59. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
- 2.60. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 2.61. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
- 2.62. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
- 2.63. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
- 2.64. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
- 2.65. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio;
- 2.66. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
- 2.67. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;
- 2.68. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados;
- 2.69. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;
- 2.70. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy)

nos pontos de acesso;

- 2.71. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;
- 2.72. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;
- 2.73. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;
- 2.74. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;
- 2.75. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
- 2.76. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões Mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor;
- 2.77. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:
 - 2.78. a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);
 - 2.79. b. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;
 - 2.80. c. ASLEAP;
 - 2.81. d. Null Probe Response or Null SSID Probe Response;
 - 2.82. e. Long Duration;
 - 2.83. f. Ataques contra Wireless Bridges;
 - 2.84. g. Weak WEP;
 - 2.85. h. Invalid MAC OUI.
- 2.86. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela

- infraestrutura através do envio de pacotes de deauthentication;
- 2.87. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio;
- 2.88. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID;
- 2.89. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- 2.90. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
- 2.91. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
- 2.92. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
- 2.93. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP;
- 2.94. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários;
- 2.95. A solução deverá suportar SingleSign-On (SSO);
- 2.96. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada;
- 2.97. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS;
- 2.98. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada;
- 2.99. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;
- 2.100. A solução deve permitir a customização da página de autenticação do captive portal, de

forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;

- 2.101. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
- 2.102. A solução deve permitir a configuração do captive portal com endereço IPv6;
- 2.103. A solução deve permitir o cadastramento de contas para usuários visitantes localmente.
A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
- 2.104. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
- 2.105. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
- 2.106. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários;
- 2.107. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários;
- 2.108. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente;
- 2.109. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede;
- 2.110. A solução deverá ser capaz de inspecionar 8.4 Gbps de tráfego SSL;
- 2.111. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria;
- 2.112. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários;
- 2.113. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo continuar;
- 2.114. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados;

- 2.115. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas;
- 2.116. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução;
- 2.117. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios préconfigurados em sua base de conhecimento;
- 2.118. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos;
- 2.119. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS;
- 2.120. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig;
- 2.121. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6;
- 2.122. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução;
- 2.123. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas;
- 2.124. A solução deverá ser capaz de tratar 9.8 Gbps de tráfego por meio do filtro de aplicações;
- 2.125. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede;
- 2.126. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações;
- 2.127. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução;
- 2.128. A solução deverá permitir a criação manual de novos padrões de aplicações;

- 2.129. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;
- 2.130. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra;
- 2.131. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;
- 2.132. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede;
- 2.133. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;
- 2.134. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;
- 2.135. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC;
- 2.136. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall;
- 2.137. A solução deverá ser capaz de tratar 27(vinte e sete) Gbps de tráfego por meio das regras de firewall stateful;
- 2.138. A solução deverá ser capaz de suportar 8.000.000 (oito milhões) de sessões simultâneas/concorrentes e 500.000 (quinhentos mil) novas sessões por segundo;
- 2.139. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT;
- 2.140. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura;
- 2.141. A solução deverá suportar PBR – Policy Based Routing;
- 2.142. A solução deverá suportar roteamento multicast;
- 2.143. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar;
- 2.144. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323;

- 2.145. A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas;
- 2.146. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego;
- 2.147. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública;
- 2.148. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada;
- 2.149. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada;
- 2.150. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada;
- 2.151. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego;
- 2.152. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada;
- 2.153. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec;
- 2.154. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo.
- 2.155. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link;
- 2.156. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover).
- 2.157. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6;
- 2.158. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de

acesso;

- 2.159. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados;
- 2.160. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica;
- 2.161. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes;
- 2.162. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados;
- 2.163. A solução deverá suportar Netflow ou sFlow;
- 2.164. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6;
- 2.165. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS;
- 2.166. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
- 2.167. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;
- 2.168. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap;
- 2.169. A solução deve possuir ferramentas de diagnósticos e debug;
- 2.170. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha;
- 2.171. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários;
- 2.172. A solução deve suportar comunicação com elementos externos através de REST API;
- 2.173. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo;
- 2.174. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;
- 2.175. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do

fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução.

2.176. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.

3. Solução de Gerenciamento Centralizado de Segurança da Rede

3.1. Solução que permita administrar de maneira centralizada todos os elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede do datacenter da CONTRATANTE;

3.2. Deverá ser totalmente compatível com a solução proposta para gerenciamento da segurança e infraestrutura de rede do datacenter da CONTRATANTE;

3.3. A solução deverá estar devidamente licenciada para administrar todos os pontos de acesso, switches e elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede deste processo pelo período do contrato;

3.4. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;

3.5. A solução deverá ser composta por elemento ou elementos fornecido(s) na forma de appliance virtual (máquina virtual) compatível com Vmware ESXi, Microsoft Hyper-V ou Linux KVM;

3.6. A solução deverá garantir a integridade da configuração de um determinado item através de bloqueio de alterações quando ocorrer acesso simultâneo de dois ou mais administradores no mesmo ativo;

3.7. A solução deverá possibilitar a criação e administração de políticas de firewall, controle de aplicação e filtro de URL;

3.8. A solução deverá permitir criar, de forma centralizada, novos objetos que poderão ser utilizados nas políticas;

3.9. A solução deverá permitir que o administrador localize em quais regras um determinado objeto (ex: computador, serviço, etc.) está sendo utilizado;

3.10. A solução deverá atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;

3.11. A solução deverá permitir a criação de regras de filtragem de tráfego que fiquem ativas

- apenas em horários pré-definidos;
- 3.12. A solução deverá permitir a criação de regras de filtragem de tráfego com data de expiração;
- 3.13. A solução deve possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem/conflitem com outras (shadowing) ou ainda garantir que esta exigência seja plenamente atendida por meio diverso;
- 3.14. A solução deve permitir a criação de templates de configuração de túneis VPN IPSec a serem aplicados de maneira centralizada e padronizada em elementos concentradores VPN;
- 3.15. A solução deve permitir agendamento para a execução de configurações nos elementos administrados;
- 3.16. A solução deve permitir a criação e execução de scripts em elementos administrados de maneira programada;
- 3.17. A solução deve permitir a criação de templates de configuração a serem aplicados de maneira centralizada e padronizada em elementos da rede sem fio e switches;
- 3.18. As seguintes características do SSID devem ser configuradas nos pontos de acesso através dos templates: nome do SSID, endereçamento DHCP a ser entregue aos clientes wireless, métodos de autenticação e agendamento da disponibilidade do SSID;
- 3.19. As seguintes características devem ser configuradas nos pontos de acesso através dos templates: potência de transmissão Wi-Fi, escolha do canal, tamanho do canal, configuração do algoritmo de seleção automática de potência e canal, configuração de short guard interval, modo de operação e acesso administrativo ao ponto de acesso;
- 3.20. As seguintes características de segurança devem ser configuradas na rede sem fio através dos templates: configuração da detecção de Rogue Aps e configuração de assinaturas de wIDS ou wIPS;
- 3.21. As seguintes características de Bluetooth Low Energy (BLE) devem ser configuradas nos pontos de acesso através dos templates: configuração do UUID, Major ID, Minor ID, Beacon Interval e potência;
- 3.22. As seguintes características de VLAN devem ser configuradas nos switches através dos templates: VLAN, VLAN ID e endereçamento IP;
- 3.23. As seguintes características de segurança devem ser configuradas nos switches através dos templates: Autenticação 802.1X, Autenticação MAB e Guest VLAN;
- 3.24. As seguintes características de rede devem ser configuradas nos switches através dos templates: configuração das portas com respectivas VLANs tagged e untagged,

- configuração do protocolo LLDP e configurações de QoS;
- 3.25. A solução deve permitir que o administrador selecione em quais elementos os templates de configuração deverão ser aplicados;
- 3.26. A solução deve listar os elementos administrados e seu status de operação;
- 3.27. A solução deve listar todos os clientes conectados na rede sem fio, o nome do ponto de acesso ao qual o cliente está conectado, qualidade do sinal da conexão de cada cliente, tipo de dispositivo utilizado na conexão e nome do SSID;
- 3.28. A solução deve listar todos os Rogue APs na rede sem fio, nome do SSID do propagado, canal impactado, nível de sinal detectado e nome do ponto de acesso que detectou o Rogue AP;
- 3.29. A solução deve incorporar mapa mundi para visão unificada do status de operação dos elementos. Deve ainda permitir a adição de planta baixa de múltiplas localidades;
- 3.30. A solução deve garantir visão centralizada do status e estatísticas de uso das interfaces dos switches;
- 3.31. A solução deve apresentar a topologia da rede com status dos elementos e informações sobre a atuação do protocolo Spanning-Tree em interfaces;
- 3.32. A solução deve permitir a execução de testes remotos para identificação de problemas em cabos de rede conectados aos switches;
- 3.33. A solução deve permitir o agrupamento dos elementos administrados para aplicação de políticas ou templates de configuração;
- 3.34. A solução deverá realizar o backup automático das configurações dos elementos e permitir o retorno (rollback) de uma versão de configuração salva previamente;
- 3.35. A solução deverá possibilitar que o administrador visualize e compare diferentes versões de configurações dos elementos, sejam elas configurações vigentes, configurações anteriores e configurações antigas;
- 3.36. A solução deverá possuir sistema de backup e restauração de todas as configurações da própria ferramenta de administração centralizada;
- 3.37. A solução deverá identificar a versão de firmware em execução nos elementos administrados e garantir que quando houver novas versões de software para eles, que seja realizada a distribuição e instalação remota de maneira centralizada;
- 3.38. A solução deve permitir criar políticas/templates que definam a versão de firmware a ser distribuída e instalada em elementos administrados. Deve permitir ainda que o administrador da rede agende a atualização da versão de firmware de maneira automática

nos elementos administrados;

- 3.39. A solução deve garantir visão centralizada das estatísticas de uso da rede sem fio;
- 3.40. A solução deve garantir visão centralizada das aplicações mais acessadas na rede, com informações sobre o volume total de dados trafegados para cada aplicação e a identificação dos usuários que fizeram os acessos;
- 3.41. A solução deve garantir visão centralizada das categorias de websites mais acessados na rede, com informações sobre o volume total de dados trafegados para cada categoria e a identificação dos usuários que fizeram os acessos;
- 3.42. A solução deve garantir visão centralizada dos usuários que mais trafegaram dados na rede, com informações sobre os hosts aos quais o usuário estava conectado, volume de dados trafegados e os endereços de destino que foram acessados;
- 3.43. A solução deve garantir visão centralizada das estatísticas de uso dos túneis VPN, com informações sobre volume de dados trafegados, horário da conexão e identificação do usuário que conectou na VPN;
- 3.44. A solução deverá ser capaz de receber os logs dos elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede das unidades e apresentá-los de forma centralizada;
- 3.45. A solução deverá ser capaz de receber, no mínimo, 5GB de logs diários;
- 3.46. A solução deverá ser capaz de armazenar, no mínimo, 3TB de informação;
- 3.47. A solução deverá ser capaz de armazenar os logs por 12 meses;
- 3.48. A solução deverá possuir mecanismo para que logs antigos sejam removidos automaticamente;
- 3.49. A solução deverá permitir a exportação dos logs;
- 3.50. A solução deverá permitir que o administrador realize download de um determinado conjunto de logs em formato texto ou CSV;
- 3.51. A solução deverá garantir a geração de relatórios com mapas geográficos ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego;
- 3.52. A solução deverá permitir a extração de relatórios;
- 3.53. A solução deverá possuir relatórios pré-definidos;
- 3.54. A solução deverá possibilitar a duplicação de relatórios e gráficos existentes para edição dos mesmos logo em seguida;
- 3.55. A solução deverá permitir a personalização de capas para os relatórios
- 3.56. A solução deverá permitir a geração de relatórios de logs de tráfego de dados;

- 3.57. A solução deverá permitir a personalização dos relatórios para inserção de gráficos dos tipos barra, linha, tabela e pizza;
- 3.58. A solução deverá possibilitar o envio de relatórios por e-mail de maneira automática;
- 3.59. A solução deverá permitir a customização de quaisquer relatórios fornecidos pela solução, exclusivamente a critério da contratante, adaptando-o às suas necessidades;
- 3.60. A solução deverá permitir a definição de filtros nos relatórios;
- 3.61. A solução deverá ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros;
- 3.62. A solução deverá garantir a capacidade de criar consultas avançadas em sua base de dados que para as informações sejam utilizadas em gráficos e tabelas dentro dos relatórios;
- 3.63. A solução deverá implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;
- 3.64. A solução deverá permitir a criação de múltiplos perfis de usuários administradores com permissões granulares para limitar o acesso a determinadas funções e garantir privilégios de somente leitura e/ou leitura-escrita a outras;
- 3.65. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7. Durante o período de garantia deve ser possível a atualização do software para novas versões.
- 3.66. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução.
- 3.67. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.

4. Conectores Fibra Óptica

4.1. TRANSCEIVER 1000BASE-SX

- a) Transceiver SFP para conexão de fibras ópticas multimodo;
- b) Deve ser compatível com o padrão 1000BASE-SX para fibras ópticas de até 400 metros;
- c) Deve possuir conector LC duplex;
- d) Velocidade de 1GBe;
- e) Deve ser compatível com os switches deste processo;

4.2. TRANSCEIVER 10GBASE-SR 1.

- a) Transceiver SFP para conexão de fibras ópticas multimodo;
- b) Deve ser compatível com o padrão 10GBASE-SR para fibras ópticas de até 300 metros;
- c) Deve possuir conector LC duplex;
- d) Velocidade de 10GBE;
- e) Deve ser compatível com os switches deste processo;

5. SERVIÇO DE MONTAGEM, INSTALACAO, CONFIGURACAO E PADRONIZACAO DE SOFTWARE E EQUIPAMENTO DA SOLUCAO DE DATACENTER

5.1. SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE REDES E SEGURANÇA

- 5.1.1. A CONTRATADA será responsável Conectores Fibra Óptica pela instalação/configuração da solução apresentada no item 3 respeitando a quantidade adquirida.
- 5.1.2. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano.
- 5.1.3. Este serviço deverá incluir avaliação de pré-implantação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 3. Fases:
- 5.1.4. Avaliação de pré-implantação
 - a) O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas.
- 5.1.5. Cronograma do plano de implementação
 - a) Após a avaliação, o especialista contratado designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de

implementação não deve ser alterado depois de confirmado pelo cliente.

5.1.6. Garantia de qualidade

- a) A contratante deverá garantir a qualidade por meio de testes em laboratório da CONTRATADA com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real.

5.1.7. Execução

- a) A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas.
- b) A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir.

5.1.8. Monitoramento

- a) A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente.

5.1.9. Relatório de implementação

- a) O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados.

5.1.10. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes;

5.1.11. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento.

5.1.12. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial.

5.1.13. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para

o equipamento LAN da CONTRATADA e para os demais componentes que serão ofertados.

- 5.1.14. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento;
- 5.1.15. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação;
- 5.1.16. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE;
- 5.1.17. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação;
- 5.1.18. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas;

5.2.SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA

- 5.2.1. A CONTRATADA será responsável pela instalação/configuração da solução apresentada.
- 5.2.2. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano.
- 5.2.3. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório.
- 5.2.4. Avaliação de pré-implementação
 - a) O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na

implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas.

5.2.5. Cronograma do plano de implementação

- a) Após a avaliação, o especialista contratado designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente.

5.2.6. Garantia de qualidade

- a) A contratante deverá garantir a qualidade por meio de testes em laboratório da CONTRATADA com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real.

5.2.7. Execução

- a) A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas.
- b) A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir.

5.2.8. Monitoramento

- a) A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente.

5.2.9. Relatório de implementação

- a) O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados.

5.2.10. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas

nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes;

- 5.2.11. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento.
- 5.2.12. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial.
- 5.2.13. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da CONTRATADA e para os demais componentes que serão ofertados.
- 5.2.14. Será de responsabilidade do CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento;
- 5.2.15. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação;
- 5.2.16. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE;
- 5.2.17. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação;
- 5.2.18. A CONTRATADA deverá fazer a migração de regras do Firewall da CONTRATANTE para a nova solução.
- 5.2.19. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas;



ATA DE REGISTRO DE PREÇOS Nº 31105/2022
PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS
IFSC

Pregão Nº 31105/2022 – SRP

Processo nº 23292.030398/2022-96

O **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA**, CNPJ nº 11.402.887/0001-60, Rua 14 de Julho, 150 – Enseada dos Marinheiros – Coqueiros, Florianópolis/SC – CEP: 88.075-010, doravante denominado apenas CONTRATANTE, neste ato representado pelo seu Reitor, Sr. MAURÍCIO GARIBA JÚNIOR RG 986.743 CPF 464.505.729-49, realizou no site www.comprasnet.gov.br Pregão Eletrônico para Registro de Preços e, nos termos da Lei nº 10.520/02 e os Decretos nº 5.450/05, 7.892/13, 8.250/14, Instrução Normativa Nº 6, de 25 de julho de 2014, Lei nº 8.666/93 e das demais normas aplicáveis, em razão da classificação das propostas apresentadas no **Pregão Eletrônico de Registro de Preços nº 31105/2022**, Ata de Julgamento de Preços, divulgada no Comprasnet e homologada pelo Ordenador de Despesas deste IFSC, RESOLVE registrar os preços para a aquisição dos produtos, objeto do Pregão acima citado, que passa a fazer parte desta, tendo sido os referidos preços oferecidos pelas empresas cujas propostas foram classificadas em primeiro lugar no certame acima enumerado.

CLÁUSULA PRIMEIRA – DO OBJETO

A presente Ata tem por objeto assegurar o compromisso de possível contratação entre o IFSC e as empresas vencedoras do certame licitatório referente ao **Pregão Eletrônico nº 31105/2022**, cujo objeto é a contratação de pessoa jurídica PARA **AQUISIÇÃO DE EQUIPAMENTOS E SERVIÇOS PARA GERENCIAMENTO SEGURO DA REDE LAN/WLAN PARA OS CAMPUS DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA - IFSC**. Conforme descrito no Anexo I desta Ata e ratificado por todas as empresas vencedoras através das declarações anexas.

CLÁUSULA SEGUNDA – DA VALIDADE DA ATA

A presente Ata de registro de Preços terá a validade de 12 (Doze) meses, compreendendo o período de **24/01/2023 à 24/01/2024**.

Subcláusula Primeira – Durante o prazo de validade desta Ata de Registro de Preço, o IFSC não será obrigado a firmar as contratações que dela poderão advir, facultando-se-lhe a realização de licitação específica para a aquisição pretendida, sendo assegurado ao beneficiário do registro preferência de favorecimento em igualdade de condições.

Subcláusula Segunda – Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao órgão gerenciador promover as negociações junto aos fornecedores, observadas as disposições contidas na alínea “d” do inciso II do caput do art. 65 da Lei nº 8.666, de 1993.

Subcláusula Terceira – A Ata poderá sofrer alterações de preços de acordo com as condições estabelecidas no arts. 18 e 19 do Decreto nº 7.892, de 23 de janeiro de 2013.

CLÁUSULA TERCEIRA – DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

Instituto Federal de Santa Catarina – Reitoria

Rua: 14 de julho, 150 | Coqueiros | Florianópolis/SC | CEP: 88.075-010
Fone: (48) 3877-9000 | www.ifsc.edu.br | CNPJ 11.402.887/0001-60

1/165



A presente Ata de Registro de Preços poderá ser usada por todos os órgãos da Administração Pública Federal, desde que autorizados pelo IFSC.

Subcláusula Primeira - O preço ofertado pela(s) empresa(s) signatária(s) a presente Ata de Registro de Preços é especificado conforme o Anexo I.

Subcláusula Segunda - Em cada fornecedor decorrente desta Ata, serão observadas, quanto ao preço, as cláusulas e condições constantes do Edital referente a mesma.

Subcláusula Terceira - Em cada aquisição, o preço unitário a ser pago será o constante da proposta apresentada pela(s) empresa(s) detentora(s) da presente Ata, a(s) qual(is) também a integram.

CLÁUSULA QUARTA – DA CLASSIFICAÇÃO DAS PROPOSTAS

A relação do(s) item(ns) com a(s) respectiva(s) empresa(s) ofertante(s) do menor valor por item, a(s) qual(is) terá(ão) preferência de contratação constitui o Anexo I desta Ata.

CLÁUSULA QUINTA – DO LOCAL E PRAZO DE ENTREGA.

Em cada aquisição, o prazo de entrega do objeto desta licitação será aquele definido no edital do pregão eletrônico que originou esta Ata e os quantitativos serão os informados na Autorização de Fornecimento, conforme Anexo IV do Edital.

CLÁUSULA SEXTA – DO PAGAMENTO

Em todas as aquisições, o pagamento será feito por meio de ordem bancária transmitida ao Banco do Brasil, para crédito em banco, agência e conta-corrente indicados pelo contratado até 15 (quinze) dias do aceite na respectiva Nota Fiscal pelo órgão requisitante.

Subcláusula Primeira - Para os produtos com entregas diárias e semanais, o IFSC estimará o consumo mensal e emitirá uma Autorização de Fornecimento, sendo que o pagamento se dará após as entregas das quantidades previstas na referida autorização.

CLÁUSULA SÉTIMA – DA ENTREGA

A entrega dos produtos só estará caracterizada mediante o recebimento definitivo do mesmo, ou seja, o aceite na respectiva Nota Fiscal correspondente pelo fiscal do contrato.

Subcláusula Primeira - O fornecedor ficará obrigado a atender todos os pedidos efetuados durante a vigência desta Ata, mesmo que a entrega deles decorrente estiver prevista para data posterior à do seu vencimento.

Subcláusula Segunda - Os materiais deverão ser entregues acompanhados da Nota Fiscal ou Nota Fiscal Fatura correspondente.

CLÁUSULA OITAVA – DAS PENALIDADES

A licitante que ensejar o retardamento da execução do certame, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, garantido o direito de ampla defesa, ficará impedida de licitar e contratar com a União, e será descredenciada do SICAF, pelo prazo de até 05 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade sem prejuízo das multas previstas em edital e no contrato, e das demais cominações legais.

Subcláusula Única - A contratada ficará sujeita, ainda, as penalidades previstas no edital do Pregão que originou esta Ata.

CLÁUSULA NONA – DO REAJUSTE DE PREÇOS

Considerando o prazo de validade estabelecido na Cláusula Segunda da presente Ata, e em atendimento ao §1º, art.28, da Lei Federal 9.069 de 29.6.1995 e demais legislação, é vedado qualquer reajuste de preços.

Subcláusula Única - Fica ressalvada a possibilidade de Alteração das condições para a 03/12 concessão de reajuste em face da superveniência de normas federais aplicáveis à espécie.

CLÁUSULA DÉCIMA – DAS CONDIÇÕES DE RECEBIMENTO

Os materiais objetos desta Ata de Registro de preços serão recebidos pelo requisitante consoante o disposto no art. 73 da Lei 8.666/93 e demais normas pertinentes.

CLÁUSULA DÉCIMA PRIMEIRA – DO CANCELAMENTO DA ATA DE REGISTRO DE PREÇOS

Esta Ata de Registro de Preços poderá ser cancelada, de pleno direito:

I – Pela Administração, quando:

- a-** a detentora não cumprir as obrigações constantes desta Ata de Registro de Preços;
- b-** a detentora não assinar a Ata no prazo estabelecido e a Administração não aceitar a sua justificativa;
- c-** a detentora der causa a rescisão administrativa de contrato decorrente de registro de preços;
- d-** em qualquer das hipóteses de inexecução total ou parcial de contrato decorrente de registro de preços;
- e-** os preços registrados se apresentarem superiores aos praticados no mercado;
- f-** por razões de interesse público devidamente demonstradas e justificadas pela Administração;
- g-** a comunicação do cancelamento do preço registrado, nos casos previstos neste Edital, será feita pessoalmente ou por correspondência com aviso de recebimento, juntando-se o comprovante aos autos que deram origem ao registro de preços;
- h-** no caso de ser ignorado, incerto ou inacessível o endereço da detentora, a comunicação será feita por publicação no Diário Oficial da União, considerando-se cancelado o preço registrado após a publicação.

II- Pelas detentoras, quando:

- a-** mediante solicitação por escrito, comprovarem estar impossibilitadas de cumprir as exigências desta Ata de Registro de Preços;
- b-** o fornecedor poderá solicitar o cancelamento do seu registro de preços na ocorrência de fato superveniente que venha comprometer a perfeita execução contratual, decorrente de caso fortuito ou de força maior, devidamente comprovados;
- c-** à solicitação das detentoras para cancelamento dos preços registrados deverá ser formulada com a antecedência de 30 (trinta) dias, facultada à Administração a aplicação das penalidades previstas na Lei, caso não aceitas as razões do pedido.

CLÁUSULA DÉCIMA SEGUNDA – DA AUTORIZAÇÃO PARA AQUISIÇÃO E EMISSÃO

DAS AUTORIZAÇÕES DE FORNECIMENTO

As aquisições do objeto da presente Ata de Registro de Preço serão autorizadas, caso a caso, pelo Ordenador de Despesas do IFSC.

Subcláusula Primeira - A emissão das autorizações de fornecimento, sua retificação ou cancelamento, total ou parcial serão igualmente autorizados pelo órgão requisitante.

Subcláusula Segunda - Durante o prazo de validade do Registro de Preços, o IFSC poderá ou não contratar o objeto deste pregão.

CLÁUSULA DÉCIMA TERCEIRA – DAS DISPOSIÇÕES FINAIS E DO FORO

Integram esta Ata, o Anexo I (preços registrados) e as declarações de concordância das empresas vencedoras.

Esta Ata está vinculada ao Edital do **Pregão Eletrônico para Registro de Preços nº 31105/2022** e às propostas aceitas durante a sessão do referido certame pelas empresas relacionadas no Anexo I desta Ata.

Fica eleito o Foro da Justiça Federal, Seção Judiciária Florianópolis para dirimir quaisquer questões decorrentes da utilização da presente ata.

Os casos omissos serão resolvidos de acordo com a Lei 10.520/2002 e Decreto 5.450/2005, Lei 8.666/93 e demais normas aplicáveis.

Visando a eficiência nos processos, informamos que a partir de hoje (24/11/2022) o Pró-Reitor de Administração passará assinar os contratos e seus devidos termos, bem como as atas de registro de preço, conforme foi delegado pela Portaria do(a) Reitor(a) nº 1.452 de 19 de maio de 2021, que pode ser consultada através do link: <https://sig.ifsc.edu.br/sipac/VerInformativo?id=35281&imprimir=true>

Documento assinado digitalmente
 ALOISIO SILVA JUNIOR
Data: 24/01/2023 12:44:20-0300
Verifique em <https://verificador.iti.br>

Florianópolis, 24 de Janeiro de 2023.
Documento assinado de acordo com
Portaria do(a) Reitor(a) nº 1.452, de 19 de maio de 2021
MAURÍCIO GARIBA JÚNIOR
REITOR DO IFSC

OBS: A adesão das empresas vencedoras a esta Ata se dá pelas Declarações de Concordância anexas



ANEXO I - DA ATA DE REGISTRO DE PREÇOS

EMPRESAS E PREÇOS REGISTRADOS

Pregão Nº 31105 / 2022 – SRP

Processo nº 23292.030398/2022-96

Relação de empresas vencedoras, contendo a descrição dos itens e preços negociados na sessão do Pregão.

EMPRESA (1)			ADVANTA SISTEMAS DE TELECOMUNICACOES E SERVICOS DE INFORMATICA LTDA		
ENDEREÇO			AV. COPACABANA, 325 3 18º ANDAR 3 SALA 1810 A 1814. Bairro: DEZOITO DO FORTE EMPRESARIAL, BARUERI / SC CEP: 06472-001		
CNPJ			03.232.670/0001-21		
TELEFONE/FAX			11 4504 5900		
REPRESENTANTE LEGAL			Wilson Roberto Piedade		
CPF REPRESENTANTE			087.941.398-06		
Email			will.sebben@oakmontgroup.com.br		
ITEM	UNID.	QTD.	ESPECIFICAÇÃO	Preço Unitário (R\$)	Preço Total (R\$)
1	UNIDA DE	80.0	Código: 44905237001000077 INJETOR POE 3 SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Injetor PoE (power injector) para alimentação de dispositivos PoE onde não há switch com esta tecnologia; 2. Deve permitir o fornecimento de energia capaz de alimentar os pontos de acesso deste processo 3. Deve fornecer no mínimo 30 Watts para alimentação do dispositivo com suporte PoE atendendo ao padrão IEEE 802.3at; 4. Deve acompanhar cabos de energia e acessórios para o seu perfeito funcionamento; 5. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V ou 220V com comutação automática. Deve acompanhar o cabo de alimentação; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021	1.159,70	92.776,00



			(V o atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).***** Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012. Marca: FORTINET Fabricante: FORTINET		
2	UNIDA DE	90.0	Código: 44905237001000075 PONTO DE ACESSO INDOOR 1. Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede através dos wireless e que possua todas as suas configurações centralizadas na solução de gerenciamento de redes e segurança; 2. Deve suportar modo de operação centralizado, ou seja, sua operação depende da solução de gerenciamento de redes e segurança que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência; 3. Deve identificar automaticamente a solução de gerenciamento de redes e segurança ao qual se conectará; 4. Deve permitir ser gerenciado remotamente através de links WAN; 5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea; 6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio; 7. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal	6.173,44	555.609,60



		recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação; 8. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento; 9. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente; 10. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN; 11. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad; 12. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB; 13. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC; 14. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e a solução de gerenciamento de redes e segurança. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até a solução de gerenciamento de redes e segurança; 15. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o a solução de gerenciamento de redes e segurança através de túnel IPSec; 16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até a solução de gerenciamento de redes e segurança, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 17. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não		



		devem ser tunelados até a solução de gerenciamento de redes e segurança; 18. Deve permitir operação em modo Mesh; 19. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências; 20. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio; 21. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL); 22. Deve suportar OFDMA; 23. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax; 24. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID; 25. Deve suportar BSS Coloring; 26. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz; 27. Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20); 28. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz; 29. Em conjunto com a solução de gerenciamento de redes e segurança, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados; 30. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 31. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz; 32. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps; 33. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS); 34. Em conjunto com a solução de gerenciamento de redes e segurança, deve permitir a criação de múltiplos domínios de		



		mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea; 35. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 36. Em conjunto com a solução de gerenciamento de redes e segurança, deve ser compatível e implementar o método de autenticação WPA3; 37. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 38. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP; 39. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 40. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 41. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 42. Deve implementar o padrão IEEE 802.11e; 43. Deve implementar o padrão IEEE 802.11h; 44. Deve implementar o padrão IEEE 802.3az; 45. Deve suportar ser gerenciado via SNMP; 46. Deve suportar consultas via REST API; 47. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação; 48. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C; 49. Deve suportar sistema antifurto do tipo Kensington Security Lock ou similar; 50. Deve possuir indicadores luminosos (LED) para indicação de status; 51. O ponto de acesso deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 52. Quaisquer licenças e/ou softwares		



			necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 53. Deve possuir certificado emitido pela Wi-Fi Alliance; 54. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 55. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V $\propto$ atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 56. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 57. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo. Marca: FORTINET Fabricante: FORTINET		
3	LICENÇ A	2.0	Código: 44904005001000106 SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE REDE E SEGURANÇA 1. Solução que permita administrar de maneira centralizada todos os elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede dos campus e que garanta suporte a processos relativos à LGPD; 2. Deverá ser totalmente compatível com a solução proposta para gerenciamento da segurança e infraestrutura de rede dos campus; 3. A solução deverá estar devidamente licenciada para administrar todos os pontos de acesso, switches e elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede deste processo pelo período do contrato; 4. Quaisquer licenças e/ou softwares necessários para plena execução de todas as	67.511,02	135.022,04



		características descritas neste termo de referência deverão ser fornecidos; 5. A solução deverá ser composta por elemento ou elementos fornecido(s) na forma de appliance virtual (máquina virtual) compatível com Vmware ESXi, Microsoft Hyper-V ou Linux KVM; 6. A solução deverá garantir a integridade da configuração de um determinado item através de bloqueio de alterações quando ocorrer acesso simultâneo de dois ou mais administradores no mesmo ativo; 7. A solução deverá possibilitar a criação e administração de políticas de firewall, controle de aplicação e filtro de URL; 8. A solução deverá permitir criar, de forma centralizada, novos objetos que poderão ser utilizados nas políticas; 9. A solução deverá permitir que o administrador localize em quais regras um determinado objeto (ex: computador, serviço, etc.) está sendo utilizado; 10. A solução deverá atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS; 11. A solução deverá permitir a criação de regras de filtragem de tráfego que fiquem ativas apenas em horários pré-definidos; 12. A solução deverá permitir a criação de regras de filtragem de tráfego com data de expiração; 13. A solução deve possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem/conflitem com outras (shadowing) ou ainda garantir que esta exigência seja plenamente atendida por meio diverso; 14. A solução deve permitir a criação de templates de configuração de túneis VPN IPSec a serem aplicados de maneira centralizada e padronizada em elementos concentradores VPN; 15. A solução deve permitir agendamento para a execução de configurações nos elementos administrados; 16. A solução deve permitir a criação e execução de scripts em elementos administrados de maneira programada; 17. A solução deve permitir a criação de templates de configuração a serem aplicados de maneira centralizada e padronizada em elementos da rede sem fio e switches; 18. As seguintes características do SSID devem ser configuradas nos pontos de acesso através dos templates: nome do SSID, endereçamento DHCP a ser entregue aos		



		clientes wireless, métodos de autenticação e agendamento da disponibilidade do SSID; 19. As seguintes características devem ser configuradas nos pontos de acesso através dos templates: potência de transmissão Wi-Fi, escolha do canal, tamanho do canal, configuração do algoritmo de seleção automática de potência e canal, configuração de short guard interval, modo de operação e acesso administrativo ao ponto de acesso; 20. As seguintes características de segurança devem ser configuradas na rede sem fio através dos templates: configuração da detecção de Rogue Aps e configuração de assinaturas de WIDS ou WIPS; 21. As seguintes características de Bluetooth Low Energy (BLE) devem ser configuradas nos pontos de acesso através dos templates: configuração do UUID, Major ID, Minor ID, Beacon Interval e potência; 22. As seguintes características de VLAN devem ser configuradas nos switches através dos templates: VLAN, VLAN ID e endereçamento IP; 23. As seguintes características de segurança devem ser configuradas nos switches através dos templates: Autenticação 802.1X, Autenticação MAB e Guest VLAN; 24. As seguintes características de rede devem ser configuradas nos switches através dos templates: configuração das portas com respectivas VLANs tagged e untagged, configuração do protocolo LLDP e configurações de QoS; 25. A solução deve permitir que o administrador selecione em quais elementos os templates de configuração deverão ser aplicados; 26. A solução deve listar os elementos administrados e seu status de operação; 27. A solução deve listar todos os clientes conectados na rede sem fio, o nome do ponto de acesso ao qual o cliente está conectado, qualidade do sinal da conexão de cada cliente, tipo de dispositivo utilizado na conexão e nome do SSID; 28. A solução deve listar todos os Rogue APs na rede sem fio, nome do SSID do propagado, canal impactado, nível de sinal detectado e nome do ponto de acesso que detectou o Rogue AP; 29. A solução deve incorporar mapa mundi para visão unificada do status de operação dos elementos. Deve ainda permitir a adição de planta baixa de múltiplas localidades; 30. A solução deve garantir visão centralizada		



		do status e estatísticas de uso das interfaces dos switches; 31. A solução deve apresentar a topologia da rede com status dos elementos e informações sobre a atuação do protocolo Spanning-Tree em interfaces; 32. A solução deve permitir a execução de testes remotos para identificação de problemas em cabos de rede conectados aos switches; 33. A solução deve permitir o agrupamento dos elementos administrados para aplicação de políticas ou templates de configuração; 34. A solução deverá realizar o backup automático das configurações dos elementos e permitir o retorno (rollback) de uma versão de configuração salva previamente; 35. A solução deverá possibilitar que o administrador visualize e compare diferentes versões de configurações dos elementos, sejam elas configurações vigentes, configurações anteriores e configurações antigas; 36. A solução deverá possuir sistema de backup e restauração de todas as configurações da própria ferramenta de administração centralizada; 37. A solução deverá identificar a versão de firmware em execução nos elementos administrados e garantir que quando houver novas versões de software para eles, que seja realizada a distribuição e instalação remota de maneira centralizada; 38. A solução deve permitir criar políticas/templates que definam a versão de firmware a ser distribuída e instalada em elementos administrados. Deve permitir ainda que o administrador da rede agende a atualização da versão de firmware de maneira automática nos elementos administrados; 39. A solução deve garantir visão centralizada das estatísticas de uso da rede sem fio; 40. A solução deve garantir visão centralizada das aplicações mais acessadas na rede, com informações sobre o volume total de dados trafegados para cada aplicação e a identificação dos usuários que fizeram os acessos; 41. A solução deve garantir visão centralizada das categorias de websites mais acessados na rede, com informações sobre o volume total de dados trafegados para cada categoria e a identificação dos usuários que fizeram os acessos; 42. A solução deve garantir visão centralizada dos usuários que mais trafegaram dados na		



		rede, com informações sobre os hosts aos quais o usuário estava conectado, volume de dados trafegados e os endereços de destino que foram acessados; 43. A solução deve garantir visão centralizada das estatísticas de uso dos túneis VPN, com informações sobre volume de dados trafegados, horário da conexão e identificação do usuário que conectou na VPN; 44. A solução deverá ser capaz de receber os logs dos elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede das unidades e apresentá-los de forma centralizada; 45. A solução deverá ser capaz de receber, no mínimo, 5GB de logs diários; 46. A solução deverá ser capaz de armazenar, no mínimo, 3TB de informação; 47. A solução deverá ser capaz de armazenar os logs por 12 meses; 48. A solução deverá possuir mecanismo para que logs antigos sejam removidos automaticamente; 49. A solução deverá permitir a exportação dos logs; 50. A solução deverá permitir que o administrador realize download de um determinado conjunto de logs em formato texto ou CSV; 51. A solução deverá garantir a geração de relatórios com mapas geográficos ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego; 52. A solução deverá permitir a extração de relatórios; 53. A solução deverá possuir relatórios pré-definidos; 54. A solução deverá possibilitar a duplicação de relatórios e gráficos existentes para edição dos mesmos logo em seguida; 55. A solução deverá permitir a personalização de capas para os relatórios 56. A solução deverá permitir a geração de relatórios de logs de tráfego de dados; 57. A solução deverá permitir a personalização dos relatórios para inserção de gráficos dos tipos barra, linha, tabela e pizza; 58. A solução deverá possibilitar o envio de relatórios por e-mail de maneira automática; 59. A solução deverá permitir a customização de quaisquer relatórios fornecidos pela solução, exclusivamente a critério da contratante, adaptando-o às suas necessidades; 60. A solução deverá permitir a definição de filtros nos relatórios;		



			61. A solução deverá ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros; 62. A solução deverá garantir a capacidade de criar consultas avançadas em sua base de dados que para as informações sejam utilizadas em gráficos e tabelas dentro dos relatórios; 63. A solução deverá implementar autenticação administrativa através dos protocolos RADIUS ou TACACS; 64. A solução deverá permitir a criação de múltiplos perfis de usuários administradores com permissões granulares para limitar o acesso a determinadas funções e garantir privilégios de somente leitura e/ou leitura-escrita a outras; 65. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7. Durante o período de garantia deve ser possível a atualização do software para novas versões. 66. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 67. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo. Marca: SEM MARCA Fabricante: -		
4	LICENÇA	400.0	Código: 44904005001000125 LICENÇAS PARA TELEFONE - SOFTPHONE 1. O softphone deve ser um aplicativo com capacidade de se registrar no controlador de chamadas existente neste órgão e atender os seguintes requisitos: 1.1. Deve possuir versões para os sistemas operacionais Windows, MacOS, iOS e Android; 1.2. Deve possuir login por usuário e senha; 1.3. Deve ser homologado para funcionar em conjunto com o Controlador de Chamadas fornecido neste grupo; 2. Deve suportar no mínimo os seguintes codecs: 2.1. G.711u; 2.2. G.711a; 2.3. G.729a; 2.4. G.722;	289,47	115.788,00



			3. Deve possuir a funcionalidade de ●Não perturbe●, com o objetivo de não ser notificado de se uma ligação esta entrando; 4. Deve suportar funcionalidades como chamada em espera, transferência, alternancia entre chamadas recebidas e conferência entre as chamadas recebidas; 5. Deve permitir a gravação de uma chamada 6. Deve permitir chamadas simultâneas e alternar entre elas; 7. Deve possuir indicador de mensagem no correio de voz; 8. Deve possuir o histórico de chamadas com no mínimo a identificação do número recebido e discado, data e hora; 9. Softfone para Windows e MACOS devem suportar: 9.1. Deve suportar o envie e recebimento de FAX; 9.2. Deve suportar a conexão com STUN (Session Traversal Utilities for NAT) server; 9.3. Deve suportar chamadas de video usando no mínimo os codecs H.264, VP9 e VP8; 10. Deve ser garantida atualização de software/firmware durante período de garantia. Marca: SEM MARCA Fabricante: -		
5	UNIDA DE	20.0	Código: 44905237001000076 PONTO DE ACESSO OUTDOOR 1. Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede através da wireless e que possua todas as suas configurações centralizadas na solução de gerenciamento de redes e segurança; 2. Deve suportar modo de operação centralizado, ou seja, sua operação depende da solução de gerenciamento de redes e segurança que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência; 3. Deve identificar automaticamente a solução de gerenciamento de redes e segurança ao qual se conectará; 4. Deve permitir ser gerenciado remotamente através de links WAN; 5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea; 6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio; 7. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para	11.668,79	233.375,80



		funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (WIDS/WIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação; 8. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento; 9. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente; 10. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T, ou superior, com conector RJ-45 para permitir a conexão com a rede LAN; 11. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad; 12. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB; 13. Deve permitir sua alimentação através de Power Over Ethernet (PoE). Deve acompanhar injetor PoE para alimentação do equipamento; 14. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e a solução de gerenciamento de redes e segurança. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até a solução de gerenciamento de redes e segurança; 15. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o a solução de gerenciamento de redes e segurança através de túnel IPSec; 16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até a solução de gerenciamento de redes e segurança, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 17. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego		



		conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até a solução de gerenciamento de redes e segurança; 18. Deve permitir operação em modo Mesh; 19. Deve possuir potência de irradiação de 25dBm em 2.4GHz e 5GHz; 20. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1.2 Gbps em um único rádio; 21. Deve suportar MUMIMO com operações em Downlink (DL) e Uplink (UL); 22. Deve suportar OFDMA com operações em Downlink (DL) e Uplink (UL); 23. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax; 24. Deve implementar recurso de Target Wake Time (TWT) configurado por SSID; 25. Deve suportar BSS Coloring; 26. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz; 27. Deve possuir sensibilidade mínima de -91dBm quando operando em 5GHz com MCS0 (HT20); 28. Deve possuir antenas internas ao equipamento com ganho mínimo de 6dBi em 2.4GHz e 6dBi em 5GHz; 29. Em conjunto com a solução de gerenciamento de redes e segurança, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados; 30. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos nãoWiFi e que operem nas frequências de 2.4GHz ou 5GHz; 31. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps; 32. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS); 33. Em conjunto com a solução de gerenciamento de redes e segurança, deve permitir a criação de múltiplos domínios de		



		mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 8 (oito) SSIDs com operação simultânea; 34. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 35. Em conjunto com a solução de gerenciamento de redes e segurança, deve ser compatível e implementar o método de autenticação WPA3 com 802.1X; 36. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 37. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 38. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 39. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 40. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 41. Deve implementar o padrão IEEE 802.11e; 42. Deve implementar o padrão IEEE 802.11h; 43. Deve implementar o padrão IEEE 802.3az; 44. Deve suportar consultas SNMP diretamente no ponto de acesso; 45. Deve suportar consultas REST API diretamente no ponto de acesso; 46. Deve possuir estrutura robusta para operação em ambientes externos e permitir ser instalado em paredes e postes. Deve acompanhar os acessórios para fixação em paredes e postes; 47. Deve ser capaz de operar em ambientes com temperaturas entre -10 e 60° C; 48. O equipamento deve possuir grau de proteção IP67. Não serão aceitos equipamentos instalados em acessórios, por exemplo caixas herméticas, para que alcancem		



			este grau de proteção; 49. Deve possuir indicadores luminosos (LED) para indicação de status das interfaces físicas e dos rádios WiFi; 50. O ponto de acesso deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 51. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 52. Deve possuir certificado emitido pela Wi-Fi Alliance; 53. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 54. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V $\propto$ atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 55. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 56. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo. Marca: FORTINET Fabricante: FORTINET		
6	SERVIÇO	10.0	Código: 33904021006000177 SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 1 1. A PROPONENTE será responsável pela conexão física do Equipamento do item 20 conforme tabela acima respeitando a quantidade adquirida em ATA. 2. As instalações, que ocorrerão em etapas: 2.1. O serviço de implantação será fornecido para implementar a implantação do dispositivo	16.656,42	166.564,20



		no ambiente de rede da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano. 2.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 3. Fases: 3.1. Avaliação de pré-implementação 3.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 3.2. Cronograma do plano de implementação 3.2.1. Após a avaliação, o especialista contratado designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 3.3. Garantia de qualidade 3.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real. 3.4. Execução 3.4.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 3.4.2. A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 3.5. Monitoramento 3.5.1. A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente. 3.6. Relatório de implementação 3.6.1. O Relatório de Implantação de		



		Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 9. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 10. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução		



			implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas; Marca: SEM MARCA Fabricante: -		
7	SERVIÇO	4.0	Código: 33904021006000178 SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 2 1. A PROPONENTE será responsável pela conexão física do Equipamento do item 21 conforme tabela acima respeitando a quantidade adquirida em ATA. 2. As instalações, que ocorrerão em etapas: 2.1. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano. 2.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 3. Fases: 3.1. Avaliação de pré-implementação 3.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 3.2. Cronograma do plano de implementação 3.2.1. Após a avaliação, o especialista contratado designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 3.3. Garantia de qualidade 3.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real.	25.466,10	101.864,40



		3.4. Execução 3.4.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 3.4.2. A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 3.5. Monitoramento 3.5.1. A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente. 3.6. Relatório de implementação 3.6.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 9. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 10. A CONTRATADA, depois de concluído o		



			serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas; Marca: SEM MARCA Fabricante: -		
8	SERVIÇO	15.0	Código: 33904021006000179 SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 3 1. A PROPONENTE será responsável pela conexão física do Equipamento do item 22 conforme tabela acima respeitando a quantidade adquirida em ATA. 2. As instalações, que ocorrerão em etapas: 2.1. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano. 2.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 3. Fases: 3.1. Avaliação de pré-implementação 3.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 3.2. Cronograma do plano de implementação 3.2.1. Após a avaliação, o especialista contratada designado deverá desenvolver o	4.279,45	64.191,75



		plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 3.3. Garantia de qualidade 3.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real. 3.4. Execução 3.4.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 3.4.2. A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 3.5. Monitoramento 3.5.1. A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente. 3.6. Relatório de implementação 3.6.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento.		



			6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 9. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 10. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas; Marca: SEM MARCA Fabricante: -		
9	SERVIÇO	5.0	Código: 33904021006000180 SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 4 1. A PROPONENTE será responsável pela conexão física do Equipamento do item 23 conforme tabela acima respeitando a quantidade adquirida em ATA. 2. As instalações, que ocorrerão em etapas: 2.1. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano.	6.559,68	32.798,40



		2.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 3. Fases: 3.1. Avaliação de pré-implementação 3.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 3.2. Cronograma do plano de implementação 3.2.1. Após a avaliação, o especialista contratado designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 3.3. Garantia de qualidade 3.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real. 3.4. Execução 3.4.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 3.4.2. A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 3.5. Monitoramento 3.5.1. A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente. 3.6. Relatório de implementação 3.6.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns		



			recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 9. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 10. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas; Marca: SEM MARCA Fabricante: -		
10	SERVIÇ	2.0	Código: 33904021006000181 SERVIÇO DE	17.214,32	34.428,64



	O	CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 5 1. A PROPONENTE será responsável pela conexão física do Equipamento do item 24 conforme tabela acima respeitando a quantidade adquirida em ATA. 2. As instalações, que ocorrerão em etapas: 2.1. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano. 2.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 3. Fases: 3.1. Avaliação de pré-implementação 3.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 3.2. Cronograma do plano de implementação 3.2.1. Após a avaliação, o especialista contratada designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 3.3. Garantia de qualidade 3.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real. 3.4. Execução 3.4.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas.		



		3.4.2. A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 3.5. Monitoramento 3.5.1. A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente. 3.6. Relatório de implementação 3.6.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 9. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 10. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente		



			instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas; Marca: SEM MARCA Fabricante: -		
11	SERVIÇO	2.0	Código: 33904021006000182 SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 6 1. A PROPONENTE será responsável pela conexão física do Equipamento do item 25 conforme tabela acima respeitando a quantidade adquirida em ATA. 2. As instalações, que ocorrerão em etapas: 2.1. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano. 2.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 3. Fases: 3.1. Avaliação de pré-implementação 3.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 3.2. Cronograma do plano de implementação 3.2.1. Após a avaliação, o especialista contratada designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a	5.188,57	10.377,14



		aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 3.3. Garantia de qualidade 3.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real. 3.4. Execução 3.4.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 3.4.2. A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 3.5. Monitoramento 3.5.1. A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente. 3.6. Relatório de implementação 3.6.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os		



			demais componentes que serão ofertados. 8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 9. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 10. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas; Marca: SEM MARCA Fabricante: -		
12	SERVIÇO	2.0	Código: 33904021006000175 SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE REDES E SEGURANÇA 1. A PROPONENTE será responsável pela instalação/configuração da solução apresentada no item 03 respeitando a quantidade adquirida em ATA. 2. As instalações, que ocorrerão em etapas: 2.1. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano. 2.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório.	15.663,53	31.327,06



		3. Fases: 3.1. Avaliação de pré-implementação 3.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 3.2. Cronograma do plano de implementação 3.2.1. Após a avaliação, o especialista contratado designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 3.3. Garantia de qualidade 3.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real. 3.4. Execução 3.4.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 3.4.2. A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 3.5. Monitoramento 3.5.1. A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente. 3.6. Relatório de implementação 3.6.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo,		



			eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 9. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 10. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas; Marca: SEM MARCA Fabricante: -		
13	SERVIÇO	2.0	Código: 33904021006000195 SERVIÇO DE INSTALAÇÃO/CONFIGURAÇÃO - TELEFONIA TIPO 1 1. Este serviço deve englobar o serviço de instalação, configuração e customização dos	23.371,70	46.743,40



		seguintes itens deste grupo: 1.1. Sistema de Voz $\propto$ Tipo I - VM 2. Este serviço será executado on-site, em cada um dos campus deste órgão; 3. Deve ser instalado nos locais definidos por este órgão; 4. Os serviços devem ser realizados por técnico com certificação técnica emitida pelo fabricante dos equipamentos; 5. No mínimo as seguintes configurações devem ser realizadas: 5.1. Instalação, configuração e testes do Controlador e Gateway de Voz; 5.2. Configurações para integração com o Controlador de Chamadas; 5.3. Plano de discagem; 5.4. Rota de Menor Custo; 5.5. Grupos de Captura; 5.6. Recurso de conferência; 5.7. Música em espera local; 5.8. Criptografia das Chamadas; 5.9. Configuração do entroncamento E1; 5.10. Configuração de entroncamento SIP; 5.11. Configuração de integração com serviço fone@RNP; 5.12. Configuração e testes do modo de emergência; 5.13. Instalação e configuração dos Terminais de Comunicação; 5.14. Demais parâmetros que forem alinhados na reunião de pré-projeto 6. Ao final da instalação deverá ser realizado, para cada equipamento instalado, um repasse de informações hands-on com pelo menos 2 horas de duração, demonstrando o correto funcionamento das funcionalidades solicitadas e apresentando as configurações realizadas nos equipamentos; 7. Este órgão irá fornecer pontos elétricos e lógicos necessários para a instalação dos equipamentos, assim como a configuração dos ativos de rede para o pleno funcionamento da solução; 8. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, reunião esta que pode ser por telefone ou webconferência, devendo a contratada sugerir as configurações de acordo com normas e boas práticas, cabendo a contratante a aceitação ou não; 9. Esta reunião de pré-projeto deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho) elaborado pela CONTRATADA. Neste documento devem conter o objetivo dos serviços, as atividades que serão realizadas, os prazos estimados para		



			cada atividade, as diretrizes dos serviços que serão realizados, os locais de execução, as informações necessárias, os padrões que serão aplicados, o nome do(s) gerente(s) de projetos responsável e do(s) técnico(s) responsável(is) pela execução dos serviços. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes; 10. Os preços devem refletir a instalação, configuração e customização de todos os equipamentos descritos neste item; 11. Devem estar incluídas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços; Ao término do serviço deve ser fornecido um relatório contendo todas as configurações realizadas de modo a facilitar a administração da solução por este órgão e permitir a continuidade do funcionamento da solução. Marca: SEM MARCA Fabricante: -		
14	SERVIÇO	10.0	Código: 33904021006000196 SERVIÇO DE INSTALAÇÃO/CONFIGURAÇÃO - TELEFONIA TIPO 2 1. Este serviço deve englobar o serviço de instalação, configuração e customização dos seguintes itens deste grupo: 1.1. Sistema de Voz $\propto$ Tipo II - VM 2. Este serviço será executado on-site, em cada um dos campus deste órgão; 3. Deve ser instalado nos locais definidos por este órgão; 4. Os serviços devem ser realizados por técnico com certificação técnica emitida pelo fabricante dos equipamentos; 5. No mínimo as seguintes configurações devem ser realizadas: 5.1. Instalação, configuração e testes do Controlador e Gateway de Voz; 5.2. Configurações para integração com o Controlador de Chamadas; 5.3. Plano de discagem; 5.4. Rota de Menor Custo; 5.5. Grupos de Captura; 5.6. Recurso de conferência; 5.7. Música em espera local; 5.8. Criptografia das Chamadas; 5.9. Configuração do entroncamento E1; 5.10. Configuração de entroncamento SIP; 5.11. Configuração de integração com serviço fone@RNP; 5.12. Configuração e testes do modo de emergência; 5.13. Instalação e configuração dos Terminais	12.953,24	129.532,40



			de Comunicação; 5.14. Demais parâmetros que forem alinhados na reunião de pré-projeto 6. Ao final da instalação deverá ser realizado, para cada equipamento instalado, um repasse de informações hands-on com pelo menos 2 horas de duração, demonstrando o correto funcionamento das funcionalidades solicitadas e apresentando as configurações realizadas nos equipamentos; 7. Este órgão irá fornecer pontos elétricos e lógicos necessários para a instalação dos equipamentos, assim como a configuração dos ativos de rede para o pleno funcionamento da solução; 8. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, reunião esta que pode ser por telefone ou webconferência, devendo a contratada sugerir as configurações de acordo com normas e boas práticas, cabendo a contratante a aceitação ou não; 9. Esta reunião de pré-projeto deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho) elaborado pela CONTRATADA. Neste documento devem conter o objetivo dos serviços, as atividades que serão realizadas, os prazos estimados para cada atividade, as diretrizes dos serviços que serão realizados, os locais de execução, as informações necessárias, os padrões que serão aplicados, o nome do(s) gerente(s) de projetos responsável e do(s) técnico(s) responsável(is) pela execução dos serviços. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes; 10. Os preços devem refletir a instalação, configuração e customização de todos os equipamentos descritos neste item; 11. Devem estar incluídas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços; Ao término do serviço deve ser fornecido um relatório contendo todas as configurações realizadas de modo a facilitar a administração da solução por este órgão e permitir a continuidade do funcionamento da solução. Marca: SEM MARCA Fabricante: -		
15	SERVIÇO	5.0	Código: 33904021006000176 SERVIÇO TÉCNICO PARA SITE SURVEY 1. O serviço de Site Survey será utilizado para análise técnica do ambiente real dos campus do IFSC em todas as localidades do estado de	22.723,01	113.615,05



		Santa Catarina de forma presencial nos respectivos endereços, apoiada por ferramentas e softwares adequados, que indiquem: 1.1. O melhor posicionamento dos dispositivos pontos de acesso de rede sem fio para a maximização da cobertura do sinal de RF; 1.2. A quantidade exata de pontos de acesso a serem instalados por prédio; 1.3. Fontes e zonas de interferência; 1.4. O canal de frequência a ser utilizado por cada ponto de acesso; 1.5. As áreas de cobertura e as taxas de transmissão ou faixas de nível de recepção de sinal de RF em desenho colorido; 2. A unidade de serviço deve contemplar um campus independente da sua localidade; 3. Será de responsabilidade da CONTRATANTE a disponibilização de planta arquitetônica em CAD (*.dwg) para realização de predição teórica e confecção de as-built; 4. Será de responsabilidade da CONTRATADA os seguintes serviços abaixo: 4.1. A disponibilização de um ou mais técnicos para realização de testes em campos para determinar a melhor disposição dos pontos de acesso de rede sem fio; 4.2. Relatório técnico de vistoria resultante da predição teórica das plantas fornecidas pela CONTRATANTE com as seguintes informações: 4.2.1. As possíveis limitações físicas ou dificuldades de implementação detectados nos locais e restrições da construção, obstáculos, etc.; 4.2.2. Melhor posicionamento dos dispositivos em cada andar das localidades visando a maximização da cobertura do sinal de RF; 4.2.3. A quantidade exata de pontos de acesso a ser instalados em cada andar e locais previstos no projeto; 4.2.4. As zonas e faixas de interferência detectadas durante o mapeamento de rádio frequência; 4.2.5. As faixas de frequência a serem utilizadas para cada ponto de acesso; 4.2.6. As áreas de cobertura e as taxas de transmissão ou faixas de nível de recepção de sinal de RF avaliados durante o mapeamento; 5. O relatório técnico deverá ser emitido com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA; 6. Todos os instrumentos/equipamentos e softwares necessários para a execução do serviço serão fornecidos pela CONTRATADA; 7. O relatório técnico de vistoria com o		



			resultado do estudo de site survey deverá ser entregue ao analista ou técnico de TI lotados no câmpus em avaliação, em via impressa ou em meio digital em até 30 (trinta) dias úteis após assinatura do contrato para os itens acima citados. Marca: SEM MARCA Fabricante: -		
16	UNIDA DE	2.0	Código: 44905237001000085 SISTEMA DE VOZ - TIPO I - VM CARACTERÍSTICAS GERAIS: ----- Administração do Sistema 1. O sistema proposto deve ter pelo menos dois métodos de configuração através de uma interface Web e através de uma linha de comando acessível através de um console serial, telnet ou SSH. 2. O equipamento proposto deve possuir um endereço IP padrão em uma de suas interfaces para poder iniciar a instalação e configuração diretamente na interface Web. 3. O sistema proposto deve ter um assistente de configuração para poder realizar os passos iniciais da configuração até a realização de chamadas telefônicas. 4. Deve ter uma página web para que os usuários possam gerenciar suas extensões incluindo as seguintes funcionalidades: 5. Verificação do correio de voz, incluindo reproduzir, excluir ou salvar mensagens de correio de voz 6. Usar o operador de console para processar chamadas da empresa. 7. Verificar o registro de chamadas para chamadas discadas, recebidas e não atendidas ou armazene correios de voz 8. Revisar o diretório corporativo 9. Gerenciar chamadas 10. Configurar perfil de telefone 11. Personalizar arquivos de som. 12. Para acessar esta página da web, o usuário deve inserir seu número de ramal e um PIN na página. Monitoramento do Sistema 13. O sistema proposto deve ter um dashboard para verificar o estado geral do equipamento incluindo o número de série, o tempo de operação, a disponibilidade de recursos de memória, CPU e largura de banda de rede utilizada, a versão do sistema operacional, bem como um histórico de estatísticas de chamadas. 14. Esta Interface deve ser personalizável para poder selecionar as informações mais relevantes e até mesmo entrar na linha de	32.576,76	65.153,52



		comando por este meio. 15. O sistema de monitoramento dos equipamentos propostos deve permitir a visualização de chamadas de saída, chamadas em espera, chamadas em conferência, ramais, troncos, filas de chamadas, clientes DHCP e telefones não atribuídos. 16. Para chamadas ativas, o sistema deve mostrar em tempo real, incluindo os números que estão sendo chamados e de onde as chamadas estão sendo feitas, bem como os troncos que estão sendo usados 203;203;naquele momento, o status da chamada e sua duração 17. Deve mostrar os detalhes das chamadas de conferência incluindo o nome da conferência, o número dos ramais na conferência e a duração da conferência. 18. Deve apresentar a informação de todos os ramais incluindo o estado, seu identificador, o número, o nome do usuário, o tipo de ramal e o tipo de telefone conectado. 19. Para o status dos troncos, o sistema deve mostrar em tempo real incluindo os nomes, endereços IP, tipo de tronco e se estiver conectado e cadastrado na operadora, o status deve mostrar se está em serviço, se está não disponível, se estiver em alarme ou se estiver desabilitado. 20. Exibir o status dos faxes. 21. O sistema deve ter um serviço de relatórios e entregá-los em HTML ou PDF 22. Deve ter um sistema de logs acessível diretamente da página web que deve permitir pesquisas com critérios personalizados e poder exportá-los para uma tabela. Configuração do sistema 23. O sistema proposto deve suportar IPv4 e IPv6 24. Deve suportar a criação de VLANs e a criação de interfaces redundantes combinando duas ou mais interfaces físicas para fornecer redundância. 25. Deve conter pelo menos 4 portas Ethernet 10/100/1000 BaseT. 26. Deve permitir a criação de rotas estáticas 27. Deve funcionar como servidor DHCP 28. Deve permitir a captura de pacotes e armazenar essas informações em um arquivo 3.pcap9 para análise posterior. 29. Suportar a criação de diferentes contas de administrador e poder limitar o acesso de endereços IP específicos. 30. A autenticação deve ser feita localmente ou por meio de um servidor LDAP		



		31. Suporte a diferentes perfis de administração, como contas de monitor, onde você só tem direitos de leitura do sistema 32. Suporta um esquema de alta disponibilidade com um dispositivo ativo e um dispositivo passivo, fazendo alterações no dispositivo ativo e replicando automaticamente a configuração no dispositivo passivo. 33. Selecione o fuso horário em que o equipamento vai funcionar bem como o uso de servidores NTP para garantir o horário dentro do equipamento. 34. Suporte a políticas de senha, como a escolha do número mínimo de caracteres solicitados na senha, bem como o uso de letras maiúsculas ou minúsculas e caracteres especiais. 35. Suporte SNMPv3 36. Configure pelo menos um servidor de correio para enviar mensagens de alerta do sistema. 37. Interface gráfica personalizável 38. Suportar uma pré-autorização para integrar o sistema através do uso de certificados digitais para fazer uma conexão segura. Configuração do sistema telefônico 39. Seleção do país onde será colocado o equipamento proposto. 40. Suporte à configuração do número de emergência 41. Configuração de prefixos para atender chamadas externas, interurbanas e internacionais. 42. Configurando padrões para planos de discagem para ramais 43. Configuração de templates para envio de emails e relatórios. 44. Configuração SIP para a seleção das portas RTP, TCP e UDP a serem utilizadas 45. Suporte ao provisionamento automático da configuração SIP do telefone 46. Suporte para uso de diferentes arquivos de áudio para atendedores automáticos e música em espera. 47. Configuração de diferentes perfis para ramais que incluem diferentes serviços como seleção de codec para telefones. 48. Suporte a fax sobre IP 49. Suporte à modificação do identificador de chamadas e possibilidade de mapeá-lo para um grupo de ramais 50. Configuração de atendimento de chamadas dependendo do agendamento 51. Configuração remota de teclas		



		programáveis &#8203;&#8203;em telefones SIP 52. Quando apenas a conectividade SIP está disponível, o sistema também pode ser instalado em uma instância virtual no vSphere, HyperV, KVM e XEN Server. 53. Você deve poder contar com um módulo para hotéis Configurações das extensões 54. Configuração remota de teclas programáveis &#8203;&#8203;em telefones SIP 55. Configuração de ramais IP locais e remotos onde o usuário discará apenas o número do ramal e o sistema proposto discará um número local ou celular. 56. O sistema proposto deve ser capaz de gerar automaticamente senhas e PINs para cada ramal ou ser definido pelo administrador. 57. Deve ter a facilidade de importar e exportar a lista de extensões para um arquivo no formato CSV 58. Reinicializar o telefone remotamente 59. Deve ser fácil aplicar a mesma alteração ou modificação para variar as extensões ao mesmo tempo. 60. O sistema proposto deve detectar o tipo de telefone IP que cada um dos ramais possui. 61. Deve ser possível selecionar um perfil SIP para cada um dos ramais IP. 62. Deve ser possível conceder diferentes privilégios aos usuários dos ramais IP. 63. Cada ramal IP deve ter uma caixa postal de voz e os telefones IP devem ter um LED que permaneça aceso para notificar o usuário de que há uma entrada em sua caixa postal. 64. O sistema deve ser capaz de auditar ramais para determinar se há senhas fracas. 65. Deve possuir um sistema que permita a localização de ramais repetidos, em conflito ou sem número. 66. Suportará a importação de uma lista de extensões de um arquivo CSV 67. Suporta o protocolo T38 para manipulação de Fax sobre VoIP. 68. Definir após quantas vezes o ramal toca para ser enviado ao correio de voz 69. Enviar um e-mail com a mensagem do correio de voz como anexo. 70. Deve ser possível configurar o gerenciamento de chamadas de acordo com o calendário e qual ação deve ser seguida se o ramal estiver ocupado, não atender ou estiver em modo Ⓜ não perturbeⓂ. 71. Deve ser possível criar grupos de ramais,		



		para que uma chamada de entrada toque da mesma forma em todos os ramais pertencentes a este grupo ou faça-o sequencialmente onde tocará em cada ramal separadamente dentro do grupo. 72. O sistema proposto deve ter um sistema de anúncio (paging) 73. Adicionalmente, deve ser possível criar grupos de trabalho onde um usuário possa atender uma chamada que esteja tocando em outro ramal pertencente ao seu grupo. 74. Você deve ter uma caixa postal geral. 75. Apoiar a criação de ramais virtuais que não serão fixos em um único telefone IP. Configuração de tronco 76. O sistema deve suportar vários tipos de troncos como E1, troncos SIP e linhas analógicas tradicionais. 77. Deve exibir o status de cada um dos troncos configurados 78. O sistema proposto deve ser capaz de configurar escritórios remotos para fazer chamadas entre escritórios como se fossem ramais IP. 79. Obter a lista telefônica do site remoto. Atendimento de chamadas 80. Deve ser possível programar diferentes planos de discagem para lidar com chamadas recebidas e efetuadas. 81. No caso de chamadas de entrada, deve ser possível configurar mapeamentos diretos (DIDs) para um ou vários ramais. 82. Para chamadas de saída, deve ser possível criar um plano de discagem que, dependendo dos dígitos selecionados, determine como o sistema irá canalizar aquela chamada. 83. Deve ter atendentes automáticos para atender as chamadas. 84. Cada atendedor automático deve ter opções e gravações diferentes. 85. Os ramais IP devem poder ser configurados para limitar chamadas internacionais ou de longa distância. 86. Apoiar a configuração de chamadas em conferência. 87. Suporte à configuração de discagem rápida 88. O sistema deve ser capaz de gravar chamadas recebidas e efetuadas sem a necessidade de qualquer software ou dispositivo adicional. 89. Suporte para configuração de filas de chamadas, podendo limitar o número de chamadas na fila e o tempo que a chamada		



		permanecerá na fila. 90. Suporte a música em espera com possibilidade de upload de um arquivo de áudio para o sistema proposto. 91. Suporte para estacionar a chamada para poder colocá-la em espera e recuperá-la de outro ramal. Relatórios e registros 92. O sistema proposto deve armazenar em seu log todos os eventos relacionados ao sistema, como alterações na configuração, login e logout do administrador e os eventos relacionados às chamadas. 93. Deve ser possível selecionar o nível de gravidade do evento para determinar se ele está armazenado ou não. 94. O sistema proposto deve ser capaz de armazenar os logs em seu disco rígido ou utilizar um servidor Syslog. 95. Ser capaz de usar os logs como base do sistema de relatórios integrados. 96. Deve ser possível selecionar que tipo de logs serão armazenados. 97. Deve ter um perfil para configurar relatórios. 98. Deve possuir relatórios para detalhamento dos atendimentos e pode ser agendado para que o sistema os gere a cada determinado momento. 99. Os relatórios de chamadas devem ser enviados por e-mail. 100. O sistema proposto deve ter um relatório de cobrança de chamadas. 101. CDRs podem ser agendados e gerar um relatório em formato CSV. ESPECIFICAÇÕES TÉCNICAS----- Especificações de Hardware 1. A arquitetura da plataforma de comunicação corporativa deverá ser instalação em ambiente de virtualização compatível com VMware versão 6.0 ou superior fornecido pela Contratante. 2. O sistema deverá ser integrado a rede de dados corporativa da CONTRATANTE 3. Deve possuir no mínimo 02 vCPU 4. Deve possuir, no mínimo, 4GB de memória RAM 5. Deve possuir, no mínimo, 04 (quatro) interfaces de Rede RJ-45 10/100/1000 BASE-T 6. Deve possuir capacidade de armazenamento de até 8 TB. 7. Capacidade 8. Deve possuir, no mínimo, capacidade para suportar 24 (vinte e quatro) troncos VoIP		



			9. Deve possuir, no mínimo, capacidade para suportar 200 (duzentos) ramais IP 10. Deve possuir, no mínimo, capacidade para suportar até 36 (trinta e seis) chamadas simultaneamente. 11. Deve possuir, no mínimo, capacidade para suportar 10 (dez) chamadas de auto-atendimento. 12. Deve possuir, no mínimo, capacidade para suportar 10 (dez) Bridges de conferência. 13. Deve possuir, no mínimo, capacidade para suportar até 12 (doze) chamadas por Bridge de conferência. 14. Deve possuir, no mínimo, capacidade para suportar até 20 (vinte) agentes de Call Center. Marca: FORTINET Fabricante: FORTINET		
17	UNIDA DE	10.0	Código: 44905237001000086 SISTEMA DE VOZ - TIPO II - VM CARACTERÍSTICAS GERAIS Administração do Sistema 1. O sistema proposto deve ter pelo menos dois métodos de configuração através de uma interface Web e através de uma linha de comando acessível através de um console serial, telnet ou SSH. 2. O equipamento proposto deve possuir um endereço IP padrão em uma de suas interfaces para poder iniciar a instalação e configuração diretamente na interface Web. 3. O sistema proposto deve ter um assistente de configuração para poder realizar os passos iniciais da configuração até a realização de chamadas telefônicas. 4. Deve ter uma página web para que os usuários possam gerenciar suas extensões incluindo as seguintes funcionalidades: 5. Verificação do correio de voz, incluindo reproduzir, excluir ou salvar mensagens de correio de voz 6. Usar o operador de console para processar chamadas da empresa. 7. Verificar o registro de chamadas para chamadas discadas, recebidas e não atendidas ou armazene correios de voz 8. Revisar o diretório corporativo 9. Gerenciar chamadas 10. Configurar perfil de telefone 11. Personalizar arquivos de som. 12. Para acessar esta página da web, o usuário deve inserir seu número de ramal e um PIN na página. Monitoramento do Sistema 13. O sistema proposto deve ter um	25.559,55	255.595,50



		dashboard para verificar o estado geral do equipamento incluindo o número de série, o tempo de operação, a disponibilidade de recursos de memória, CPU e largura de banda de rede utilizada, a versão do sistema operacional, bem como um histórico de estatísticas de chamadas. 14. Esta Interface deve ser personalizável para poder selecionar as informações mais relevantes e até mesmo entrar na linha de comando por este meio. 15. O sistema de monitoramento dos equipamentos propostos deve permitir a visualização de chamadas de saída, chamadas em espera, chamadas em conferência, ramais, troncos, filas de chamadas, clientes DHCP e telefones não atribuídos. 16. Para chamadas ativas, o sistema deve mostrar em tempo real, incluindo os números que estão sendo chamados e de onde as chamadas estão sendo feitas, bem como os troncos que estão sendo usados &#8203;&#8203;naquele momento, o status da chamada e sua duração 17. Deve mostrar os detalhes das chamadas de conferência incluindo o nome da conferência, o número dos ramais na conferência e a duração da conferência. 18. Deve apresentar a informação de todos os ramais incluindo o estado, seu identificador, o número, o nome do usuário, o tipo de ramal e o tipo de telefone conectado. 19. Para o status dos troncos, o sistema deve mostrar em tempo real incluindo os nomes, endereços IP, tipo de tronco e se estiver conectado e cadastrado na operadora, o status deve mostrar se está em serviço, se está não disponível, se estiver em alarme ou se estiver desabilitado. 20. Exibir o status dos faxes. 21. O sistema deve ter um serviço de relatórios e entregá-los em HTML ou PDF 22. Deve ter um sistema de logs acessível diretamente da página web que deve permitir pesquisas com critérios personalizados e poder exportá-los para uma tabela. Configuração do sistema 23. O sistema proposto deve suportar IPv4 e IPv6 24. Deve suportar a criação de VLANs e a criação de interfaces redundantes combinando duas ou mais interfaces físicas para fornecer redundância. 25. Deve conter pelo menos 4 portas Ethernet 10/100/1000 BaseT.		



		26. Deve permitir a criação de rotas estáticas 27. Deve funcionar como servidor DHCP 28. Deve permitir a captura de pacotes e armazenar essas informações em um arquivo ®.pcap® para análise posterior. 29. Suportar a criação de diferentes contas de administrador e poder limitar o acesso de endereços IP específicos. 30. A autenticação deve ser feita localmente ou por meio de um servidor LDAP 31. Suporte a diferentes perfis de administração, como contas de monitor, onde você só tem direitos de leitura do sistema 32. Suporta um esquema de alta disponibilidade com um dispositivo ativo e um dispositivo passivo, fazendo alterações no dispositivo ativo e replicando automaticamente a configuração no dispositivo passivo. 33. Selecione o fuso horário em que o equipamento vai funcionar bem como o uso de servidores NTP para garantir o horário dentro do equipamento. 34. Suporte a políticas de senha, como a escolha do número mínimo de caracteres solicitados na senha, bem como o uso de letras maiúsculas ou minúsculas e caracteres especiais. 35. Suporte SNMPv3 36. Configure pelo menos um servidor de correio para enviar mensagens de alerta do sistema. 37. Interface gráfica personalizável 38. Suportar uma pré-autorização para integrar o sistema através do uso de certificados digitais para fazer uma conexão segura. Configuração do sistema telefônico 39. Seleção do país onde será colocado o equipamento proposto. 40. Suporte à configuração do número de emergência 41. Configuração de prefixos para atender chamadas externas, interurbanas e internacionais. 42. Configurando padrões para planos de discagem para ramais 43. Configuração de templates para envio de emails e relatórios. 44. Configuração SIP para a seleção das portas RTP, TCP e UDP a serem utilizadas 45. Suporte ao provisionamento automático da configuração SIP do telefone 46. Suporte para uso de diferentes arquivos de áudio para atendedores automáticos e música em espera.		



		47. Configuração de diferentes perfis para ramais que incluem diferentes serviços como seleção de codec para telefones. 48. Suporte a fax sobre IP 49. Suporte à modificação do identificador de chamadas e possibilidade de mapeá-lo para um grupo de ramais 50. Configuração de atendimento de chamadas dependendo do agendamento 51. Configuração remota de teclas programáveis &#8203;&#8203;em telefones SIP 52. Quando apenas a conectividade SIP está disponível, o sistema também pode ser instalado em uma instância virtual no vSphere, HyperV, KVM e XEN Server. 53. Você deve poder contar com um módulo para hotéis Configurações das extensões 54. Configuração remota de teclas programáveis &#8203;&#8203;em telefones SIP 55. Configuração de ramais IP locais e remotos onde o usuário discará apenas o número do ramal e o sistema proposto discará um número local ou celular. 56. O sistema proposto deve ser capaz de gerar automaticamente senhas e PINs para cada ramal ou ser definido pelo administrador. 57. Deve ter a facilidade de importar e exportar a lista de extensões para um arquivo no formato CSV 58. Reinicializar o telefone remotamente 59. Deve ser fácil aplicar a mesma alteração ou modificação para variar as extensões ao mesmo tempo. 60. O sistema proposto deve detectar o tipo de telefone IP que cada um dos ramais possui. 61. Deve ser possível selecionar um perfil SIP para cada um dos ramais IP. 62. Deve ser possível conceder diferentes privilégios aos usuários dos ramais IP. 63. Cada ramal IP deve ter uma caixa postal de voz e os telefones IP devem ter um LED que permaneça aceso para notificar o usuário de que há uma entrada em sua caixa postal. 64. O sistema deve ser capaz de auditar ramais para determinar se há senhas fracas. 65. Deve possuir um sistema que permita a localização de ramais repetidos, em conflito ou sem número. 66. Suportará a importação de uma lista de extensões de um arquivo CSV 67. Suporta o protocolo T38 para manipulação de Fax sobre VoIP.		



		68. Definir após quantas vezes o ramal toca para ser enviado ao correio de voz 69. Enviar um e-mail com a mensagem do correio de voz como anexo. 70. Deve ser possível configurar o gerenciamento de chamadas de acordo com o calendário e qual ação deve ser seguida se o ramal estiver ocupado, não atender ou estiver em modo "não perturbe". 71. Deve ser possível criar grupos de ramais, para que uma chamada de entrada toque da mesma forma em todos os ramais pertencentes a este grupo ou faça-o sequencialmente onde tocará em cada ramal separadamente dentro do grupo. 72. O sistema proposto deve ter um sistema de anúncio (paging) 73. Adicionalmente, deve ser possível criar grupos de trabalho onde um usuário possa atender uma chamada que esteja tocando em outro ramal pertencente ao seu grupo. 74. Você deve ter uma caixa postal geral. 75. Apoiar a criação de ramais virtuais que não serão fixos em um único telefone IP. Configuração de tronco 76. O sistema deve suportar vários tipos de troncos como E1, troncos SIP e linhas analógicas tradicionais. 77. Deve exibir o status de cada um dos troncos configurados 78. O sistema proposto deve ser capaz de configurar escritórios remotos para fazer chamadas entre escritórios como se fossem ramais IP. 79. Obter a lista telefônica do site remoto. Atendimento de chamadas 80. Deve ser possível programar diferentes planos de discagem para lidar com chamadas recebidas e efetuadas. 81. No caso de chamadas de entrada, deve ser possível configurar mapeamentos diretos (DIDs) para um ou vários ramais. 82. Para chamadas de saída, deve ser possível criar um plano de discagem que, dependendo dos dígitos selecionados, determine como o sistema irá canalizar aquela chamada. 83. Deve ter atendentes automáticos para atender as chamadas. 84. Cada atendedor automático deve ter opções e gravações diferentes. 85. Os ramais IP devem poder ser configurados para limitar chamadas internacionais ou de longa distância. 86. Apoiar a configuração de chamadas em		



		conferência. 87. Suporte à configuração de discagem rápida 88. O sistema deve ser capaz de gravar chamadas recebidas e efetuadas sem a necessidade de qualquer software ou dispositivo adicional. 89. Suporte para configuração de filas de chamadas, podendo limitar o número de chamadas na fila e o tempo que a chamada permanecerá na fila. 90. Suporte a música em espera com possibilidade de upload de um arquivo de áudio para o sistema proposto. 91. Suporte para estacionar a chamada para poder colocá-la em espera e recuperá-la de outro ramal. Relatórios e registros 92. O sistema proposto deve armazenar em seu log todos os eventos relacionados ao sistema, como alterações na configuração, login e logout do administrador e os eventos relacionados às chamadas. 93. Deve ser possível selecionar o nível de gravidade do evento para determinar se ele está armazenado ou não. 94. O sistema proposto deve ser capaz de armazenar os logs em seu disco rígido ou utilizar um servidor Syslog. 95. Ser capaz de usar os logs como base do sistema de relatórios integrados. 96. Deve ser possível selecionar que tipo de logs serão armazenados. 97. Deve ter um perfil para configurar relatórios. 98. Deve possuir relatórios para detalhamento dos atendimentos e pode ser agendado para que o sistema os gere a cada determinado momento. 99. Os relatórios de chamadas devem ser enviados por e-mail. 100. O sistema proposto deve ter um relatório de cobrança de chamadas. 101. CDRs podem ser agendados e gerar um relatório em formato CSV. ESPECIFICAÇÕES TÉCNICAS 1. A arquitetura da plataforma de comunicação corporativa deverá ser instalação em ambiente de virtualização compatível com VMware versão 6.0 ou superior fornecido pela Contratante. 2. O sistema deverá ser integrado a rede de dados corporativa da CONTRATANTE		



			3. Deve possuir no mínimo 01 vCPU 4. Deve possuir, no mínimo, 2GB de memória RAM 5. Deve possuir, no mínimo, 04 (quatro) interfaces de Rede RJ-45 10/100/1000 BASE-T 6. Deve possuir capacidade de armazenamento de até 8 TB. 7. Capacidade 8. Deve possuir, no mínimo, capacidade para suportar 16 (dezesesseis) troncos VoIP 9. Deve possuir, no mínimo, capacidade para suportar 100 (cem) ramais IP 10. Deve possuir, no mínimo, capacidade para suportar até 30 (trinta) chamadas simultaneamente. 11. Deve possuir, no mínimo, capacidade para suportar 10 (dez) chamadas de auto-atendimento. 12. Deve possuir, no mínimo, capacidade para suportar 08 (oito) Bridges de conferência. 13. Deve possuir, no mínimo, capacidade para suportar até 12 (doze) chamadas por Bridge de conferência. 14. Deve possuir, no mínimo, capacidade para suportar até 10 (dez) agentes de Call Center. Marca: FORTINET Fabricante: FORTINET		
18	UNIDA DE	10.0	Código: 44905237001000087 SISTEMA DE VOZ GATEWAY - TIPO I APPLIANCE 1. Equipamento do tipo appliance, ou seja, equipamento e software do mesmo fabricante. Não serão aceitos computadores ou equipamentos baseados em computadores; 2. Os Gateways de voz devem fazer parte do sistema de comunicação corporativa, serão os equipamentos controlados pelo servidor principal de telefonia IP e exclusivamente utilizados para conectividade dos seguintes elementos: 2.1. Interfaces para suportar os protocolos PRI T1, PRI E1 e R2 em configurações de porta única e dupla. 2.2. Interfaces para entroncamento GSM com o SMP e o SME (Conversão SIP/GSM). 3. Deve possuir funcionalidade de operar como central IP com capacidade de registro e gerenciamento local para situações de emergência caso haja problemas na conectividade com a solução de comunicação central, suprimindo no mínimo as seguintes funcionalidades: registro dos telefones, chamadas entre os ramais registrados neste gateway, chamadas de/e para RTPC, colocar chamada em espera, captura, correio de voz (pela RTPC), transferência e geração de	34.858,58	348.585,80



		bilhetes local (CDR); 4. Deve entrar e sair deste modo de emergência (perda de conexão com a solução de comunicação central) automaticamente, sem intervenção humana; 5. Deve implementar, no mínimo, os Codecs de voz G711 e G729; 6. Deve possuir conectividade com a rede IP através de porta RJ-45 10/100/1000 (Gigabit Ethernet); 7. Deve possuir porta de console para gerenciamento local do equipamento; 8. Deve possuir entregue com pelo menos 2 (duas) interfaces E1; 9. Deve implementar IPv4 e IPv6; 10. Deve ser baseado no protocolo IP, com implementação do protocolo SIP (RFC3261); 11. Deve implementar o protocolo cRTP; 12. Deve implementar Qualidade de Serviço (QoS), utilizando DiffServ (CoS), IP Precedence (ToS) ou Differentiated Services Code Point (DSCP); 13. Deve ser compatível para instalação em racks padrão 19. Deverá vir acompanhado de kits de fixação, cabos, acessórios e demais materiais necessários à sua instalação, configuração e operação; 14. Deve implementar buffer dinâmico e programável para controle de jitter; 15. Deve implementar cancelamento de eco, segundo o padrão G.165 ou G.168; 16. Deverá se comunicar com o sistema central via protocolo SIP; 17. Deverá possuir áudio seguro, com SRTP, onde todas as chamadas são criptografadas para máxima segurança; 18. As configurações devem ser armazenadas em memória tipo não volátil; 19. Deve suportar transmissão de fax, segundo padrão T.38; 20. Deverá permitir múltiplos usuários para administração, com níveis de acesso distintos; 21. Deve implementar criptografia para tráfego de sinalização e de voz além da criptografia IPSEC solicitada para tráfego entre os gateways e com os aparelhos telefônicos, esta criptografia não deverá ser perdida quando estiver em modo de emergência (perda de conexão com a solução de comunicação central); 22. Deve permitir a execução local de música em espera; 23. Deve implementar SNMP com criptografia; 24. Fonte de alimentação interna que opere de 110V a 220V automaticamente; 25. Deve ser garantida atualização de		



			software/firmware do equipamento pelo período de garantia sem custos para este órgão; 26. A empresa deve possuir, após a assinatura do contrato, pelo menos 1 (um) profissional com certificação técnica emitida pelo fabricante do equipamento ofertado, capaz de prestar suporte de primeiro nível aos produtos em garantia, e escalar o suporte ao fabricante conforme necessidade; 27. Garantia de 36 (trinta e seis) meses; Marca: FORTINET Fabricante: FORTINET		
19	UNIDA DE	10.0	Código: 44905237001000088 SISTEMA DE VOZ GATEWAY - TIPO II APPLIANCE 1. Equipamento do tipo appliance, ou seja, equipamento e software do mesmo fabricante. Não serão aceitos computadores ou equipamentos baseados em computadores; 2. Os Gateways de voz devem fazer parte do sistema de comunicação corporativa, serão os equipamentos controlados pelo servidor principal de telefonia IP e exclusivamente utilizados para conectividade dos seguintes elementos: 2.1. Interfaces para suportar os protocolos PRI T1, PRI E1 e R2 em configurações de porta única e dupla. 2.2. Interfaces para entroncamento GSM com o SMP e o SME (Conversão SIP/GSM). 3. Deve possuir funcionalidade de operar como central IP com capacidade de registro e gerenciamento local para situações de emergência caso haja problemas na conectividade com a solução de comunicação central, suprimindo no mínimo as seguintes funcionalidades: registro dos telefones, chamadas entre os ramais registrados neste gateway, chamadas de/e para RTPC, colocar chamada em espera, captura, correio de voz (pela RTPC), transferência e geração de bilhetes local (CDR); 4. Deve entrar e sair deste modo de ⑧emergência⑨ (perda de conexão com a solução de comunicação central) automaticamente, sem intervenção humana; 5. Deve implementar, no mínimo, os Codecs de voz G711 e G729; 6. Deve possuir conectividade com a rede IP através de porta RJ-45 10/100/1000 (Gigabit Ethernet); 7. Deve possuir porta de console para gerenciamento local do equipamento; 8. Deve possuir entregue com pelo menos 1 (uma) interfaces E1; 9. Deve implementar IPv4 e IPv6;	25.556,78	255.567,80



			10. Deve ser baseado no protocolo IP, com implementação do protocolo SIP (RFC3261); 11. Deve implementar o protocolo cRTP; 12. Deve implementar Qualidade de Serviço (QoS), utilizando DiffServ (CoS), IP Precedence (ToS) ou Differentiated Services Code Point (DSCP); 13. Deve ser compatível para instalação em racks padrão 19". Deverá vir acompanhado de kits de fixação, cabos, acessórios e demais materiais necessários à sua instalação, configuração e operação; 14. Deve implementar buffer dinâmico e programável para controle de jitter; 15. Deve implementar cancelamento de eco, segundo o padrão G.165 ou G.168; 16. Deverá se comunicar com o sistema central via protocolo SIP; 17. Deverá possuir áudio seguro, com SRTP, onde todas as chamadas são criptografadas para máxima segurança; 18. As configurações devem ser armazenadas em memória tipo não volátil; 19. Deve suportar transmissão de fax, segundo padrão T.38; 20. Deverá permitir múltiplos usuários para administração, com níveis de acesso distintos; 21. Deve implementar criptografia para tráfego de sinalização e de voz além da criptografia IPSEC solicitada para tráfego entre os gateways e com os aparelhos telefônicos, esta criptografia não deverá ser perdida quando estiver em modo de emergência (perda de conexão com a solução de comunicação central); 22. Deve permitir a execução local de música em espera; 23. Deve implementar SNMP com criptografia; 24. Fonte de alimentação interna que opere de 110V a 220V automaticamente; 25. Deve ser garantida atualização de software/firmware do equipamento pelo período de garantia sem custos para este órgão; 26. A empresa deve possuir, após a assinatura do contrato, pelo menos 1 (um) profissional com certificação técnica emitida pelo fabricante do equipamento ofertado, capaz de prestar suporte de primeiro nível aos produtos em garantia, e escalar o suporte ao fabricante conforme necessidade; 27. Garantia de 36 (trinta e seis) meses; Marca: FORTINET Fabricante: FORTINET		
20	UNIDA DE	8.0	Código: 44905237001000078 SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA	62.302,30	498.418,40



		PARA CÂMPUS TIPO 1 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de virtual, ou seja, cada elemento deverá ser composto software do respectivo fabricante; 3. Deve suportar compatibilidade com Hypervisors abaixo: a. VMware ESXi v5.5 / v6.0 / v6.5 / v6.7 / v7.0 b. VMware NSX-T* v2.3 / v2.4 / v2.5 c. Microsoft Hyper-V Server 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 d. Microsoft AzureStack e. Citrix XenServer v5.6 sp2, v6.0, v6.2 and later f. Open source Xen v3.4.3, v4.1 and later g. KVM qemu 0.12.1 & libvirt 0.10.2 and later for Red Hat Enterprise Linux / CentOS 6.4 and later / Ubuntu 16.04 LTS (generic kernel) h. KVM qemu 2.3.1 for SuSE Linux Enterprise Server 12 SP1 LTSS i. Nutanix AHV (AOS 5.10, Prism Central 5.10) j. Cisco Cloud Services Platform 2100 k. Cisco ENCS (NFVIS 3.12.3) 4. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 5. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 6. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 7. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 8. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 9. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem		



		utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 10. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 11. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 12. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 96 (novecentos e seis) pontos de acesso		



		wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 25. 25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo		



		todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPsec e SSL com elementos externos; 36. A solução deverá ser capaz de encaminhar 4.5 Gbps de tráfego encapsulado via VPN IPsec; 37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 38. A VPN IPsec deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 39. A VPN IPsec deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPsec; 42. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN ou tecnologia similar; 46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 47. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas		



		frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 48. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 56. A solução deve permitir restringir o		



		número máximo de dispositivos conectados por ponto de acesso e por rádio; 57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à		



		infraestrutura wireless, melhorando assim o consumo de Airtime; 67. A solução deve permitir a configuração dos parâmetros BLE (Blueooth Low Energy) nos pontos de acesso; 68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); b. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; c. ASLEAP; d. Null Probe Response or Null SSID Probe Response; e. Long Duration; f. Ataques contra Wireless Bridges; g. Weak WEP; h. Invalid MAC OUI.		



		75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 84. A solução deverá suportar Single-Sign-On (SSO); 85. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web		



		HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 91. A solução deve permitir a configuração do captive portal com endereço IPv6; 92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 99. A solução deverá ser capaz de inspecionar 3.5 Gbps de tráfego SSL; 100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir		



		notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo continuar; 103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 113. A solução deverá ser capaz de tratar 4		



		(quatro) Gbps de tráfego por meio do filtro de aplicações; 114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 117. A solução deverá permitir a criação manual de novos padrões de aplicações; 118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 126. A solução deverá ser capaz de tratar 20 (vinte) Gbps de tráfego por meio das regras de firewall stateful; 127. A solução deverá ser capaz de suportar 270.000 (duzentos e setenta) novas sessões por segundo; 128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos ↔ NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um,		



		vários para um, NAT64, NAT66, NAT46 e PAT; 129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 130. A solução deverá suportar PBR ou Policy Based Routing; 131. A solução deverá suportar roteamento multicast; 132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 133. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323; 134. A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN		



		IPSec; 143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 152. A solução deverá suportar Netflow ou sFlow; 153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 157. A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap; 158. A solução deve possuir ferramentas de		



			diagnósticos e debug 159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 161. A solução deve suportar comunicação com elementos externos através de REST API; 162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V <i>o</i> atendimento aos princípios: a. da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 164. A A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 165. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo. Marca: SEM MARCA Fabricante: -		
21	UNIDA DE	3.0	Código: 44905237001000079 SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 2 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de virtual, ou seja, cada elemento deverá ser composto software do respectivo fabricante;	187.774,7 1	563.324,13



		3. Deve suportar compatibilidade com Hypervisors abaixo: a) VMware ESXi v5.5 / v6.0 / v6.5 / v6.7 / v7.0 b) VMware NSX-T* v2.3 / v2.4 / v2.5 c) Microsoft Hyper-V Server 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 d) Microsoft AzureStack e) Citrix Xen XenServer v5.6 sp2, v6.0, v6.2 and later f) Open source Xen v3.4.3, v4.1 and later g) KVM qemu 0.12.1 & libvirt 0.10.2 and later for Red Hat Enterprise Linux / CentOS 6.4 and later / Ubuntu 16.04 LTS (generic kernel) h) KVM qemu 2.3.1 for SuSE Linux Enterprise Server 12 SP1 LTSS i) Nutanix AHV (AOS 5.10, Prism Central 5.10) j) Cisco Cloud Services Platform 2100 k) Cisco ENCS (NFVIS 3.12.3) 4. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 5. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 6. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 7. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 8. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 9. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 10. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 11. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 12. A solução deve monitorar a rede e		



		apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 96 (noventa e seis) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 26. A solução deve permitir a adição de planta		



		baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;		



		34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPsec e SSL com elementos externos; 36. A solução deverá ser capaz de encaminhar 9.4 Gbps de tráfego encapsulado via VPN IPsec; 37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 38. A VPN IPsec deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 39. A VPN IPsec deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPsec; 42. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN ou ADVPN ou tecnologia similar; 46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 47. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 48. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção		



		humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as		



		decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 67. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os		



		clientes sejam desconectados; 70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); b. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; c. ASLEAP; d. Null Probe Response or Null SSID Probe Response; e. Long Duration; f. Ataques contra Wireless Bridges; g. Weak WEP; h. Invalid MAC OUI. 75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes		



		métodos de autenticação: WPA (TKIP) e WPA2 (AES); 79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 84. A solução deverá suportar Single-Sign-On (SSO); 85. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 91. A solução deve permitir a configuração do captive portal com endereço IPv6;		



		92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 99. A solução deverá ser capaz de inspecionar 6.2 Gbps de tráfego SSL; 100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo continuar; 103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução;		



		106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 113. A solução deverá ser capaz de tratar 6 (seis) Gbps de tráfego por meio do filtro de aplicações; 114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 117. A solução deverá permitir a criação manual de novos padrões de aplicações;		



		118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 126. A solução deverá ser capaz de tratar 27 (vinte e sete) Gbps de tráfego por meio das regras de firewall stateful; 127. A solução deverá ser capaz de suportar 450.000 (quatrocentos e cinquenta) novas sessões por segundo; 128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos ↔ NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 130. A solução deverá suportar PBR ↔ Policy Based Routing; 131. A solução deverá suportar roteamento multicast; 132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 133. A solução deverá possuir mecanismo de tratamento para aplicações multimídia		



		(session-helpers ou ALGs) tipo SIP e H323; 134. A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado		



		em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 152. A solução deverá suportar Netflow ou sFlow; 153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 157. A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap; 158. A solução deve possuir ferramentas de diagnósticos e debug 159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 161. A solução deve suportar comunicação com elementos externos através de REST API; 162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo;		



			163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V <i>o</i> atendimento aos princípios: 164. 165. da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 166. 167. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 168. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo. Marca: SEM MARCA Fabricante: -		
22	UNIDA DE	15.0	Código: 44905237001000080 SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 3 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 6 (seis) interfaces 1000Base-T e 2 (duas) interfaces 1 Gigabit Ethernet padrão 1GBase-LX para permitir a conexão com a rede; 4. Deve possuir interface console com conector RJ-45 ou USB para gerenciamento local; 5. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar	29.986,20	449.793,00



		os cabos de alimentação; 6. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 7. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 8. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 9. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 10. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 11. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 12. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 13. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 14. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 15. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 768 (setecentos e sessenta e oito) portas de switch ou um total de 16 (dezesesseis) switches; 16. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 17. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 18. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas		



		interfaces dos switches; 19. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 21. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 22. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 23. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 24. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 25. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 26. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 96 (noventa e seis) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 27. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 28. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 29. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 30. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 31. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda		



		desabilitar o ajuste automático de potência e canais quando necessário; 32. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 33. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 34. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 35. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 36. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 37. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 38. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 39. A solução deverá ser capaz de encaminhar 6.5 Gbps de tráfego encapsulado via VPN IPSec; 40. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES;		



		41. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 42. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 43. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 44. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSEc; 45. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 46. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 47. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 48. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN ou ADVPN ou tecnologia similar; 49. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 50. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 51. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 52. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 53. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 54. A solução deve identificar automaticamente pontos de acesso intrusos		



		que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 55. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 56. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 57. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 58. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 59. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 60. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 61. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 62. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 63. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 64. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 65. A solução deve implementar técnicas de Call Admission Control para limitar o número		



		de chamadas simultâneas na rede sem fio; 66. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 67. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 68. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 69. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 70. A solução deve permitir a configuração dos parâmetros BLE (Blueooth Low Energy) nos pontos de acesso; 71. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 72. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 73. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 74. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 75. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar		



		serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 76. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 77. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: 77.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); 77.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; 77.3. ASLEAP; 77.4. Null Probe Response or Null SSID Probe Response; 77.5. Long Duration; 77.6. Ataques contra Wireless Bridges; 77.7. Weak WEP; 77.8. Invalid MAC OUI. 78. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 79. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 80. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 81. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 82. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 83. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 84. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 85. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos		



		de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 86. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 87. A solução deverá suportar Single-Sign-On (SSO); 88. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 89. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 90. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 91. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 92. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 93. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 94. A solução deve permitir a configuração do captive portal com endereço IPv6; 95. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 96. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 97. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 98. A solução deve implementar recurso para controle de URLs acessadas na rede através de		



		análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 99. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 100. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 101. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 102. A solução deverá ser capaz de inspecionar 950 (novecentos e cinquenta) Mbps de tráfego SSL; 103. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 104. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 105. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 106. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 107. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 108. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 109. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios préconfigurados em sua base de conhecimento; 110. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 111. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos		



		acessos aos websites/domínios que passaram pelo filtro de DNS; 112. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 113. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 114. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 115. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 116. A solução deverá ser capaz de tratar 1 (um) Gbps de tráfego por meio do filtro de aplicações; 117. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 118. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 119. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 120. A solução deverá permitir a criação manual de novos padrões de aplicações; 121. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 122. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 123. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 124. A solução deve monitorar e classificar o		



		risco das aplicações acessadas pelos clientes na rede; 125. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 126. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 127. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 128. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 129. A solução deverá ser capaz de tratar 7 (sete) Gbps de tráfego por meio das regras de firewall stateful; 130. A solução deverá ser capaz de suportar 1.500.000 (um milhão e quinhentos mil) de sessões simultâneas/concorrentes e 45.000 (quarenta e cinco) novas sessões por segundo; 131. A solução deverá possuir a funcionalidade de tradução de endereços estáticos ↔ NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 132. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 133. A solução deverá suportar PBR ↔ Policy Based Routing; 134. A solução deverá suportar roteamento multicast; 135. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 136. A solução deverá possuir mecanismo de tratamento para aplicações multimedial (session-helpers ou ALGs) tipo SIP e H323; 137. A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 138. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego;		



		139. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 140. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 141. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 142. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 143. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 144. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 145. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 146. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 147. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 148. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 149. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 150. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 151. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão		



		apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 152. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 153. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 154. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 155. A solução deverá suportar Netflow ou sFlow; 156. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 157. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 158. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 159. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 160. A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap; 161. A solução deve possuir ferramentas de diagnósticos e debug 162. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 163. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 164. A solução deve suportar comunicação com elementos externos através de REST API; 165. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 166. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V <i>o</i> atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia,		



			deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 167. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 168. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo. Marca: SEM MARCA Fabricante: -		
23	UNIDA DE	5.0	Código: 44905237001000081 SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 4 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 16 (dezesseis) interfaces 1 Gigabit Ethernet padrão 1000Base-T ou 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Caso sejam ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX; 4. Deve possuir interface console com conector RJ-45 ou USB para gerenciamento local; 5. Cada appliance físico deve possuir fonte de alimentação redundante com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 6. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 7. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;	67.352,08	336.760,40



		8. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 9. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 10. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 11. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 12. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 13. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 14. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 15. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 288 (duzentos e oitenta e oito) portas de switch ou um total de 64 (sessenta e quatro) switches; 16. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 17. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 18. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 19. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 21. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;		



		22. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 23. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 24. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 25. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 26. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 8 (oito) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 27. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 28. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 29. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 30. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 31. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 32. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 33. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos		



		de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 34. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 35. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 36. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 37. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 38. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPsec e SSL com elementos externos; 39. A solução deverá ser capaz de encaminhar 13 Gbps de tráfego encapsulado via VPN IPsec; 40. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 41. A VPN IPsec deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 42. A VPN IPsec deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 43. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 44. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPsec;		



		45. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 46. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 47. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 48. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN ~~ou~~ ADVPN ou tecnologia similar; 49. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 50. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 51. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 52. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 53. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 54. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 55. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças		



		na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 56. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 57. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 58. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 59. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 60. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 61. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 62. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 63. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 64. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 65. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 66. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em		



		Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 67. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 68. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 69. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 70. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 71. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 72. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 73. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 74. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 75. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 76. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do		



		tipo outdoor; 77. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: 77.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); 77.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; 77.3. ASLEAP; 77.4. Null Probe Response or Null SSID Probe Response; 77.5. Long Duration; 77.6. Ataques contra Wireless Bridges; 77.7. Weak WEP; 77.8. Invalid MAC OUI. 78. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 79. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 80. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 81. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 82. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 83. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 84. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 85. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 86. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 87. A solução deverá suportar SingleSign-On (SSO); 88. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando		



		automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 89. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 90. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 91. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 92. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 93. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 94. A solução deve permitir a configuração do captive portal com endereço IPv6; 95. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 96. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 97. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 98. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 99. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários;		



		100. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 101. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 102. A solução deverá ser capaz de inspecionar 500 (quinhentos) Mbps de tráfego SSL; 103. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 104. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 105. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 106. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 107. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 108. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 109. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 110. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 111. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 112. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo		



		nslookup e/ou dig; 113. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 114. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 115. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 116. A solução deverá ser capaz de tratar 3.5 Gbps de tráfego por meio do filtro de aplicações; 117. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 118. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 119. A solução deverá permitir a criação manual de novos padrões de aplicações; 120. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 121. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 122. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 123. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 124. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 125. A solução deve permitir a configuração		



		de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 126. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 127. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 128. A solução deverá ser capaz de tratar 11 Gbps de tráfego por meio das regras de firewall stateful; 129. A solução deverá ser capaz de suportar 3.000.000 (três milhões) de sessões simultâneas/concorrentes e 280.000 (duzentos e oitenta) novas sessões por segundo; 130. A solução deverá possuir a funcionalidade de tradução de endereços estáticos ↔ NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 131. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 132. A solução deverá suportar PBR ↔ Policy Based Routing; 133. A solução deverá suportar roteamento multicast; 134. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 135. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323; 136. A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 137. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 138. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 139. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 140. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada;		



		141. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 142. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 143. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 144. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 145. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 146. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 147. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 148. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 149. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 150. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 151. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 152. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de		



		firmwares diferentes; 153. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 154. A solução deverá suportar Netflow ou sFlow; 155. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 156. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 157. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 158. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 159. A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap; 160. A solução deve possuir ferramentas de diagnósticos e debug 161. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 162. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 163. A solução deve suportar comunicação com elementos externos através de REST API; 164. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 165. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 166. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V $\propto$ atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 167. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução.		



			168. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo. Marca: SEM MARCA Fabricante: -		
24	UNIDA DE	2.0	Código: 44905237001000082 SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 5 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 8 (oito) interfaces 1 Gigabit Ethernet padrão 1000Base-T e 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Adicionalmente devem ser fornecidos 2 (dois) transceivers SFP+ conforme padrão 10GBase-SR; 4. Deve possuir interface console com conector RJ-45 ou USB para gerenciamento local; 5. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 6. Deve suportar a instalação de fonte de alimentação redundante; 7. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 8. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 9. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 10. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda	209.102,8 2	418.205,64



		desabilitar o ajuste automático de potência e canais quando necessário; 11. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 12. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 13. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 14. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 15. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 16. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 4608 (quatro mil e seiscentos e oito) portas de switch ou um total de 96 (noventa e seis) switches; 17. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 18. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 19. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 20. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 21. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 22. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 23. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 24. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e		



		BPDU Guard; 25. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 26. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 27. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de, no mínimo, 500 (quinhentos) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 28. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 29. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 30. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 31. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 32. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 33. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 34. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 35. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes		



		enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 36. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 37. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 38. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 39. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPsec e SSL com elementos externos; 40. A solução deverá ser capaz de encaminhar 20 Gbps de tráfego encapsulado via VPN IPsec; 41. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 42. A VPN IPsec deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 43. A VPN IPsec deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 44. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 45. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPsec; 46. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 47. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 48. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 49. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN  ADVPN		



		ou tecnologia similar; 50. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 51. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 52. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 53. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 54. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 55. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 56. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 57. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 58. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com		



		configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 59. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 60. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 61. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 62. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 63. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 64. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 65. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 66. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 67. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 68. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente		



		em 5GHz através do recurso conhecido como Band Steering; 69. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 70. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 71. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 72. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 73. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 74. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 75. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 76. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 77. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 78. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); b. Os seguintes ataques de negação de serviço: Association Flood, Authentication		



		Flood, Broadcast Deauthentication e Spoofed Deauthentication; c. ASLEAP; d. Null Probe Response or Null SSID Probe Response; e. Long Duration; f. Ataques contra Wireless Bridges; g. Weak WEP; h. Invalid MAC OUI. 79. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 80. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 81. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 82. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 83. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 84. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 85. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 86. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 87. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 88. A solução deverá suportar SingleSign-On (SSO); 89. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 90. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos		



		pelos servidores RADIUS; 91. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 92. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 93. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 94. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 95. A solução deve permitir a configuração do captive portal com endereço IPv6; 96. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 97. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 98. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 99. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 100. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 101. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 102. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 103. A solução deverá ser capaz de inspecionar 8 Gbps de tráfego SSL;		



		104. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 105. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 106. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 107. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 109. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 110. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios préconfigurados em sua base de conhecimento; 111. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 112. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 113. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 114. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 115. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6.		



		Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 116. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 117. A solução deverá ser capaz de tratar 9.5 Gbps de tráfego por meio do filtro de aplicações; 118. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 119. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 120. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 121. A solução deverá permitir a criação manual de novos padrões de aplicações; 122. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 123. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 124. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 125. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 126. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 127. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 128. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 129. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 130. A solução deverá ser capaz de tratar 27		



		Gbps de tráfego por meio das regras de firewall stateful; 131. A solução deverá ser capaz de suportar 8.000.000 (oito milhões) de sessões simultâneas/concorrentes e 450.000 (quatrocentos e cinquenta mil) novas sessões por segundo; 132. A solução deverá possuir a funcionalidade de tradução de endereços estáticos ↔ NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 133. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 134. A solução deverá suportar PBR ↔ Policy Based Routing; 135. A solução deverá suportar roteamento multicast; 136. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 137. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323; 138. A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 139. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 140. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 141. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 142. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 143. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 144. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de		



		Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 145. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 146. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 147. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 148. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 149. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 150. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 151. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 152. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 153. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 154. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 155. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 156. A solução deverá suportar Netflow ou sFlow; 157. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 158. Deve implementar autenticação		



			administrativa através do protocolo RADIUS ou TACACS; 159. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 160. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 161. A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap; 162. A solução deve possuir ferramentas de diagnósticos e debug 163. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 164. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 165. A solução deve suportar comunicação com elementos externos através de REST API; 166. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 167. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V o atendimento aos princípios: a. da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 168. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 169. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo. Marca: SEM MARCA Fabricante: -		
25	UNIDA DE	2.0	Código: 44905237001000083 SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 6	343.861,9 1	687.723,82



		Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 16 (dezesesseis) interfaces 1 Gigabit Ethernet padrão 1000Base-T, 4 (quatro) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede e 4 (quatro) interfaces 25 Gigabit Ethernet padrão 25GBase-LR. Caso sejam ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX; 4. Deve possuir interface console com conector RJ-45 ou USB para gerenciamento local; 5. Cada appliance físico deve suportar fonte de alimentação redundante (Hot Swappable) com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 6. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 7. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 8. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 9. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 10. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 11. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 12. Permitir agendar dia e horário em que		



		ocorrerá a otimização do provisionamento automático de canais nos Access Points; 13. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 14. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 15. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 4.608 (quatro mil e seiscentos e oito) portas de switch ou um total de 96 (noventa e seis) switches; 16. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 17. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 18. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 19. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 21. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 22. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 23. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 24. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 25. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 26. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de		



		1000 (um mil) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 27. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 28. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 29. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 30. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 31. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 32. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 33. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 34. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 35. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo		



		todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 36. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 37. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 38. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 39. A solução deverá ser capaz de encaminhar 48 Gbps de tráfego encapsulado via VPN IPSec; 40. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 41. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 42. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 43. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 44. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 45. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 46. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 47. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 48. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN ou ADVPN ou tecnologia similar; 49. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 50. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas		



		frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 51. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 52. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 53. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 54. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 55. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 56. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 57. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 58. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 59. A solução deve permitir restringir o		



		número máximo de dispositivos conectados por ponto de acesso e por rádio; 60. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 61. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 62. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 63. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 64. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 65. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 66. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 67. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 68. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 69. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à		



		infraestrutura wireless, melhorando assim o consumo de Airtime; 70. A solução deve permitir a configuração dos parâmetros BLE (Blueooth Low Energy) nos pontos de acesso; 71. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 72. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 73. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 74. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 75. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 76. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 3. 77. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); b. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; c. ASLEAP; d. Null Probe Response or Null SSID Probe Response; e. Long Duration; f. Ataques contra Wireless Bridges; g. Weak WEP; h. Invalid MAC OUI.		



		78. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 79. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 80. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 81. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 82. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 83. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 84. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 85. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 86. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 87. A solução deverá suportar SingleSign-On (SSO); 88. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 89. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 90. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 91. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web		



		HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 92. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 93. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 94. A solução deve permitir a configuração do captive portal com endereço IPv6; 95. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 96. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 97. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 98. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 99. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 100. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 101. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 102. A solução deverá ser capaz de inspecionar 8.4 Gbps de tráfego SSL; 103. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 104. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 105. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir		



		notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo continuar; 106. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 107. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 108. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 109. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios préconfigurados em sua base de conhecimento; 110. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 111. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 112. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 113. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 114. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 115. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 116. A solução deverá ser capaz de tratar 9.8		



		Gbps de tráfego por meio do filtro de aplicações; 117. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 118. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 119. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 120. A solução deverá permitir a criação manual de novos padrões de aplicações; 121. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 122. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 123. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 124. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 125. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 126. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 127. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 128. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 129. A solução deverá ser capaz de tratar 27(vinte e sete) Gbps de tráfego por meio das regras de firewall stateful; 130. A solução deverá ser capaz de suportar 8.000.000 (oito milhões) de sessões simultâneas/concorrentes e 500.000 (quinhentos mil) novas sessões por segundo; 131. A solução deverá possuir a funcionalidade de tradução de endereços estáticos e NAT (Network Address Translation)		



		dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 132. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 133. A solução deverá suportar PBR ou Policy Based Routing; 134. A solução deverá suportar roteamento multicast; 135. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 136. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323; 137. A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 138. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 139. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 140. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 141. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 142. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 143. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 144. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 145. A solução deverá implementar método de		



		correção de erros de pacotes em túneis de VPN IPSec; 146. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 147. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 148. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 149. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 150. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 151. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 152. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 153. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 154. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 155. A solução deverá suportar Netflow ou sFlow; 156. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 157. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 158. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 159. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 160. A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap;		



			161. A solução deve possuir ferramentas de diagnósticos e debug 162. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 163. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 164. A solução deve suportar comunicação com elementos externos através de REST API; 165. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 166. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V <i>o</i> atendimento aos princípios: a. da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 1. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 2. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo. Marca: SEM MARCA Fabricante: -		
26	UNIDA DE	30.0	Código: 44905237001000067 SWITCH TIPO 1 <i>o</i> SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA Características Mínimas: 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a autonegociação de velocidade e	8.127,65	243.829,50



		duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 5. Deve possuir 1 (uma) interface USB; 6. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 32.000 endereços; 9. Deve operar com latência igual ou inferior à 1us (microsegundo); 10. 8. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 11. 9. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol $\propto$ LACP); 12. 10. Deve suportar a comutação de Jumbo Frames; 13. 11. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 14. 12. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 15. 10.13. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 16. 14. Deve implementar serviço de DHCP Relay; 17. 15. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (um mil) entradas na tabela; 18. 16. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 19. 17. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 20. 18. Deve implementar recurso conhecido		



		como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 21. 19. Deve implementar mecanismo de proteção da root bridge do algoritmo Spanning-Tree para prover defesa contra ataques do tipo Denial of Service no ambiente nível 2; 22. 20. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo fast forwarding (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 23. 21. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 24. 22. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 25. 23. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 26. 24. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 27. 25. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 28. 26. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 29. 27. Deverá implementar priorização de tráfego baseada nos valores do campo Differentiated Services Code Point (DSCP) do cabeçalho IP, conforme definições do IETF; 28. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que		



		não estejam autorizados na rede; 32. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 35. Deve suportar MAC Authentication Bypass (MAB); 36. Deve implementar RADIUS CoA (Change of Authorization); 37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 38. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 40. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 43. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 44. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 45. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces,		



		quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 47. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 50. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 52. Deve permitir ser gerenciado através de IPv6; 53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 55. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 58. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 59. Deverá suportar ser configurado e monitorado através de REST API; 60. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 61. Deve suportar temperatura de operação de até 45º Celsius; 62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 63. Deve ser fornecido com fonte de alimentação interna com capacidade para		



			operar em tensões de 110V e 220V; 64. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 65. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 66. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 67. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 68. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V $\propto$ atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 69. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 70. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo. Marca: FORTINET Fabricante: FORTINET		
27	UNIDA DE	30.0	Código: 44905237001000068 SWITCH TIPO 3 $\propto$ SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA Características Mínimas: 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar	17.187,19	515.615,70



		automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet $\propto$ PoE) e IEEE 802.3at (Power over Ethernet Plus $\propto$ PoE+) com PoE budget de 370W a serem alocados em qualquer uma das portas 1000Base-T; 5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 6. Deve possuir 1 (uma) interface USB; 7. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo); 8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 9. Deve possuir tabela MAC com suporte a 32.000 endereços; 10. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 11. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol $\propto$ LACP); 12. Deve suportar a comutação de Jumbo Frames; 13. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 14. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 15. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 16. Deve implementar serviço de DHCP Relay; 17. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (quinhentas) entradas na tabela; 18. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 19. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;		



		20. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 21. Deve implementar mecanismo de proteção da root bridge do algoritmo Spanning-Tree para prover defesa contra ataques do tipo Denial of Service no ambiente nível 2; 22. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo fast forwarding (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 23. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 24. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 25. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 26. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 27. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 28. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 29. Deverá implementar priorização de tráfego baseada nos valores do campo Differentiated Services Code Point (DSCP) do cabeçalho IP, conforme definições do IETF; 30. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 31. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 32. Deve implementar DHCP Snooping para		



		mitigar problemas com servidores DHCP que não estejam autorizados na rede; 33. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 34. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 35. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 36. Deve suportar MAC Authentication Bypass (MAB); 37. Deve implementar RADIUS CoA (Change of Authorization); 38. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 39. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 40. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 41. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 42. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 43. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 44. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 45. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 46. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for		



		aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 47. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 48. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 49. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 50. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 51. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 52. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 53. Deve permitir ser gerenciado através de IPv6; 54. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 55. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 56. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 57. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 58. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 59. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 60. Deverá suportar ser configurado e monitorado através de REST API; 61. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 62. Deve suportar temperatura de operação de até 45º Celsius; 63. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 64. Deve ser fornecido com fonte de		



			alimentação interna com capacidade para operar em tensões de 110V e 220V; 65. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 66. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 67. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 68. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 69. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V <i>o</i> atendimento aos princípios: a. da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 70. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 71. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo. Marca: FORTINET Fabricante: FORTINET		
28	UNIDA DE	15.0	Código: 44905237001000069 SWITCH TIPO 4 <i>o</i> SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA Características Mínimas: 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade	12.908,60	193.629,00



		e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 1000Base-SR operando em 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 1. Deve possuir 1 (uma) interface USB; 5. Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo); 6. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 7. Deve possuir tabela MAC com suporte a 32.000 endereços; 2. Deve operar com latência igual ou inferior a 1us (microsegundo); 8. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 9. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol ou LACP); 10. Deve suportar a comutação de Jumbo Frames; 11. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 12. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 13. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 14. Deve implementar serviço de DHCP Relay; 15. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela; 16. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 17. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 18. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma		



		porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 19. Deve implementar mecanismo de proteção da ③root bridge③ do algoritmo Spanning-Tree para prover defesa contra ataques do tipo ③Denial of Service③ no ambiente nível 2; 20. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo ③fast forwarding③ (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 21. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 22. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 23. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 24. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 25. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 26. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 27. Deverá implementar priorização de tráfego baseada nos valores do campo ③Differentiated Services Code Point③ (DSCP) do cabeçalho IP, conforme definições do IETF; 28. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 29. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 30. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;		



		31. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 32. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 33. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 34. Deve suportar MAC Authentication Bypass (MAB); 35. Deve implementar RADIUS CoA (Change of Authorization); 36. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 37. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 38. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 39. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 40. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 41. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 42. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 43. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 44. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces		



		do mesmo switch e quando o MAC Address for removido da interface; 45. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 46. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 47. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 48. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 49. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 50. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 51. Deve permitir ser gerenciado através de IPv6; 52. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 53. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 54. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 55. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 56. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 57. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 58. Deverá suportar ser configurado e monitorado através de REST API; 59. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 60. Deve suportar temperatura de operação de até 45º Celsius; 61. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 62. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;		



			63. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 64. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 65. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 66. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 67. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V $\propto$ atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET		
29	UNIDA DE	20.0	Código: 44905237001000070 SWITCH TIPO 5 $\propto$ SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA Características Mínimas: 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10000Base-SR operando em 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet $\propto$ PoE) e IEEE 802.3at (Power over Ethernet Plus $\propto$ PoE+) com PoE budget de 370W; 5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do	21.569,23	431.384,60



		equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 1. Deve possuir 1 (uma) interface USB; 6. Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 32.000 endereços; 2. Deve operar com latência igual ou inferior à 1us (microsegundo); 9. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 10. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol ~~vs~~ LACP); 11. Deve suportar a comutação de Jumbo Frames; 12. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 13. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 14. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 15. Deve implementar serviço de DHCP Relay; 16. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela; 17. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 18. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 19. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 20. Deve implementar mecanismo de proteção da 3root bridge9 do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo 3Denial of Service9 no ambiente nível 2; 21. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo 3fast		



		forwarding® (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 22. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 23. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 24. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 25. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 26. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 27. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 28. Deverá implementar priorização de tráfego baseada nos valores do campo ③Differentiated Services Code Point③ (DSCP) do cabeçalho IP, conforme definições do IETF; 29. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 32. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 34. Deve suportar a autenticação simultânea		



		de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 35. Deve suportar MAC Authentication Bypass (MAB); 36. Deve implementar RADIUS CoA (Change of Authorization); 37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 38. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 40. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 43. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 44. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 45. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 47. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;		



		49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 50. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 52. Deve permitir ser gerenciado através de IPv6; 53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 55. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 58. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 59. Deverá suportar ser configurado e monitorado através de REST API; 60. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 61. Deve suportar temperatura de operação de até 45º Celsius; 62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 64. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 65. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 66. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;		



			67. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 68. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V $\propto$ atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 69. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 70. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo. Marca: FORTINET Fabricante: FORTINET		
30	LICENÇA A	10.0	Código: 44904005001000126 TARIFADOR - TELEFONIA VOIP 1. O sistema de tarifação deverá operar em sistema operacional Windows 2016 Server ou superior. 2. O Sistema Automático de Tarifação e Bilhetagem deverá armazenar suas informações em banco de dados relacional que deve ser entregue junto com a solução; 3. Funcionalidade WEB: acesso disponível, a partir de qualquer ponto da rede, às consultas gráficas e relatórios via browser; 4. O Sistema deverá seguir a filosofia baseada no controle por USUÁRIO, os quais poderão acessar os relatórios e/ou gráficos a partir de qualquer estação (windows ou linux) na rede Intranet, via Web-Browser, através do uso de senha de autenticação, segundo o PERFIL que será estabelecido pela CONTRATANTE para os usuários. Para maior segurança das estações e servidor não será permitida a instalação de aplicativos ou componentes necessários para emular o ambiente web, como Active-X, por exemplo. O sistema deverá permitir a associação do usuário a um ou mais ramais	3.385,06	33.850,60



		e /ou uma ou mais senhas. 5. O sistema deverá permitir a criação de perfis diferenciados de acesso, com permissões 5.1. por usuário. 6. Tarifação on-line: o Sistema Automático de Tarifação e Bilhetagem deverá atribuir valor monetário imediatamente, ao receber as informações dos bilhetes telefônicos, conforme as tabelas das operadoras. 7. Retarifação automática: a retarifação deverá ser automática e imediata, ou seja, recalculada imediatamente a partir do momento em que uma alteração diretamente relacionada com o custo da ligação ocorra. 8. Relatórios via Intranet: o Sistema Automático de Tarifação e Bilhetagem deverá possibilitar o acesso a qualquer informação via browser. 9. Os relatórios deverão permitir a geração nos formatos HTML, TXT, Excel, Word e PDF. 10. Agendamento de Tarefas: O sistema deverá permitir o agendamento de emissão de 10.1. relatórios periódicos, exportação dos dados das ligações, fechamento da tarifação, ou seja, no momento definido o próprio sistema se incumbirá de executar a atividade previamente agendada. 11. Cópia de segurança compacta e programável: o sistema deverá ter uma rotina interna de backup automática, cuja periodicidade pode ser programada. 12. O sistema deverá controlar o histórico de utilização de cada ramal por usuário. 13. O sistema deverá efetuar a coleta dos bilhetes gerados pelos PABXs e/ou equipamentos IP e os tarifar e processar de forma centralizada. 14. O sistema deverá possuir um recurso de Controle de Gastos, onde poderão ser definidos valores de gastos por usuário e/ou departamentos e o sistema deverá enviar notificações periódicas indicando se o usuário está dentro ou fora de sua meta (budget), seja essa notificação por uma porcentagem de consumo ou por uma tendência de consumo. 15. O sistema deverá possuir um recurso que permita a monitoração do andamento do 15.1. sistema. Esta janela deverá alertar o usuário de eventuais falhas em alguma aplicação ou serviço da solução. Paralelamente, a solução de gerenciamento de falhas deverá enviar alertas por email ou visuais para os responsáveis, por cada evento defeituoso. O próprio recurso de monitoramento deverá tentar restabelecer os serviços que		



		caírem. 16. A coleta dos bilhetes deverá ser efetuada através da rede, de forma automática, com a geração de alarmes quando da falha na coleta dos bilhetes, com envio de mensagem eletrônica. 17. O sistema deverá possuir no mínimo os seguintes relatórios: Relatórios flexíveis, com 17.1. informações de identificação de usuários, ramais (origem e destino), tempo e data de cada chamada, centro de custo, Grupos de Usuários, custo da ligação, relatórios de tráfego (tráfego de entrada ou de saída, tráfego de por rota ou por ramal), etc.; 18. O Sistema deverá permitir a observação de dados de tráfego, de tal forma que possibilite a 18.1. medição e registros diários, relatório de tráfego na Hora e Dia de Maior Movimento, em forma de relatórios específicos para análise de custos, ocupação de troncos e ramais, duração de chamadas e avaliação do nível de serviço em períodos pré-determinados. 19. O Sistema deverá permitir a simulação de Tráfego em cima das informações fornecidas pela observação citada anteriormente e indicar o número ideal de Troncos e/ou links necessários para correto dimensionamento da central. 20. O Sistema deverá permitir a geração de Gráficos comparativos entre os centros de custo do órgão, mostrando a evolução dos últimos 13 meses. Essa evolução deverá ser apresentada 20.1. por: Custo das ligações, Quantidade de ligações e Duração das ligações e também Usuário por Plano de Serviço e Centro de Custo por Planos de Serviço. 21. O Sistema deverá possuir recurso para permitir que o próprio usuário valide as ligações particulares via Web Browser e que as mesmas sejam cadastradas automaticamente no banco de dados. 22. O sistema deve incluir a atualização automática mensal via Internet das tarifas, prefixos, localidades e novos planos praticados e publicados pelas operadoras e homologadas pela ANATEL. 23. Tabela de tarifas flexível e configurável. 24. Deve estar dimensionado e licenciado para 1100 ramais; 25. Deve ser compatível com o ③Controlador de Chamadas④ fornecido neste grupo; 26. Garantia de 36 (trinta e seis) meses; Marca: SEM MARCA Fabricante: -		



31	UNIDA DE	50.0	Código: 44905237001000089 TERMINAL DE COMUNICAÇÃO - TIPO I 1. Terminal de comunicação IP composto por telefone, monofone e acessórios para pleno funcionamento; 2. O conjunto deve ser nativo no protocolo IP. Não serão aceitos equipamentos híbridos com telefonia analógica ou que necessitem de adaptadores externos para o funcionamento; 3. Deve possuir display com resolução mínima de 320x240 pontos. Este display deve prover informações de data e hora, correio de voz, ícone de chamadas perdidas, detalhes da chamada durante uma ligação, histórico de chamadas efetuadas e recebidas e configurações do aparelho; 4. Deve permitir a alimentação de energia através de PoE, com consumo máximo de 4W para redução do consumo de energia; 5. Deve implementar protocolo SIP nativamente; 6. Deve possuir duas interfaces Ethernet RJ-45 10/100, sendo uma para conexão a LAN e outro para ligar um computador. Deve funcionar como "Ethernet Switch", permitindo ligar a rede de um computador no telefone compartilhando entre o PC e o telefone um único cabo e uma única porta no switch da rede; 7. Deve suportar LLDP; 8. Deve suportar o protocolo TFTP; 9. Deve suportar DSCP; 10. Deve possuir uma interface RJ-22 para conexão do monofone, de forma que seja fácil a sua substituição em caso de defeito do monofone ou do próprio cabo; 11. Deve permitir a fixação do aparelho na parede. Caso tal recurso não seja nativo no hardware do aparelho, os acessórios para fixação em parede devem ser fornecidos; 12. Deve suportar o idioma Português (Brasil); 13. Deve permitir duas chamadas simultâneas; 14. Deve suportar música em espera; 15. Deve possuir indicador de mensagem em espera no correio de voz; 16. Deve suportar conferência e captura de chamadas; 17. Deve possuir no mínimo 4 teclas físicas de atalhos específicas para as funcionalidades mais utilizadas: colocar chamada em espera, rediscar, mudo, volume (mais/menos); 18. Deve possuir a funcionalidade de "viva-voz" (microfone e alto-falante), sendo esta funcionalidade ativada/desativada por uma	1.405,57	70.278,50



			tecla física específica para este fim. Deve ser possível desabilitar o ⑧viva-voz⑨ no menu de configurações; 19. Deve possuir teclado numérico físico; 20. Deve ser compatível com os codecs G711 e G729a; 21. Deve possuir cliente DHCP, permitindo configuração automática de endereçamento IP. 22. Deve suportar também a configuração manual de endereçamento IP; 23. Deve possuir a funcionalidade de ⑨Não pertube⑩, com o objetivo de não ser notificado de se uma ligação esta entrando. 24. Deve ser gerenciável através de interface web; 25. Deve ser fornecido em cor neutra (preta ou cinza); 26. Garantia de 36 (trinta e seis) meses; Marca: FORTINET Fabricante: FORTINET		
32	UNIDA DE	20.0	Código: 44905237001000071 TRANSCEIVER 1000BASE-LX (2023) 1. Transceiver SFP para conexão de fibras ópticas monomodo; 2. Deve ser compatível com o padrão 1000BASE-X para fibras ópticas de até 10 quilômetros; 3. Deve possuir conector LC duplex; 4. Velocidade de 1GBe; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V <i>o</i> atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET	967,31	19.346,20
33	UNIDA DE	20.0	Código: 44905237001000073 TRANSCEIVER 10GBASE-LR (2023) 1. Transceiver SFP para conexão de fibras ópticas monomodo; 2. Deve ser compatível com o padrão 10GBASE-LR para fibras ópticas de até 10 quilômetros; 3. Deve possuir conector LC duplex; 4. Velocidade de 10GBe; 5. Deve ser compatível com os switches deste processo;	2.475,83	49.516,60



			6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V $\propto$ atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET		
34	UNIDA DE	20.0	Código: 44905237001000084 TRANSCEIVER 1000BASE-SX (2023) 1. Transceiver SFP para conexão de fibras ópticas multimodo; 2. Deve ser compatível com o padrão 1000BASE-SX para fibras ópticas de até 400 metros; 3. Deve possuir conector LC duplex; 4. Velocidade de 1GBe; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V $\propto$ atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET	487,04	9.740,80
35	UNIDA DE	20.0	Código: 44905237001000072 TRANSCEIVER 10GBASE-SR 1. Transceiver SFP para conexão de fibras ópticas multimodo; 2. Deve ser compatível com o padrão 10GBASE-SR para fibras ópticas de até 300 metros; 3. Deve possuir conector LC duplex; 4. Velocidade de 10GBe; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V $\propto$ atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET	946,23	18.924,60



Total	R\$ 7.329.257, 99

VALOR TOTAL DA ATA	R\$ 7.329.257,99

Ofício 03/2023

CONCORDÂNCIA EM FORNECIMENTO

À

DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS

Prezados,

A empresa **Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA**, inscrita no CNPJ/MF sob o nº 03.232.670/0001-21, situada na v. Copacabana, 325 – 18º Andar – Sala 1810 a 1814 – Dezoito do Forte Empresarial/Alphaville, Barueri-SP, CEP 06472-001, declara sob as penas da Lei que concorda em fornecer os equipamentos abaixo descritos, contidos **Ata de Registro de Preços nº 31105/2022 do Pregão eletrônico nº 31105/2022**, sem comprometer o acordo firmado com o Instituto Federal de Santa Catarina.

Item/Ata	Descrição	QTD	VLr Unit. R\$	Total R\$
25	Código: 44905237001000083 SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 6	1	343.861,91	343.861,91
3	Código: 44904005001000106 SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE REDE E SEGURANÇA	1	67.511,02	67.511,02
35	Código: 44905237001000072 TRANSCEIVER 10GBASE-SR	8	946,23	7.569,84
34	Código: 44905237001000084 TRANSCEIVER 1000BASE-SX (2023)	8	487,04	3.896,32
12	Código: 33904021006000175 SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE REDES E SEGURANÇA	1	15.663,53	15.663,53
7	Código: 33904021006000178 SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 2	1	25.466,10	25.466,10
Total Geral R\$				463.968,72

Observação: esta carta de concordância é válida apenas nos casos de adesão total do item e quantidades descritos acima.

Prazo de entrega dos equipamentos: Conforme anexo I item 5.2.3. e 5.2.4, do referido edital.

Barueri, SP 13 de abril de 2023.

Atenciosamente,

RAFAEL ALVES DE SOUZA:32628082888
Assinado de forma digital por RAFAEL ALVES DE SOUZA:32628082888
Dados: 2023.04.17 15:50:37 -03'00'

Rafael Alves de Souza
Diretor Executivo

De: siasgnet-atasrp@planejamento.gov.br
Para: [Thais Moisés](#)
Assunto: [SIASGnet-AtaSRP] Solicitação de Adesão Autorizada para a Ata do(a) Pregão Eletrônico 158516-31105/2022
Data: terça-feira, 11 de abril de 2023 14:31:14

Prezado Gestor,

O Gestor da Ata do(a) Pregão Eletrônico 158516-31105/2022 autorizou a adesão para o item Nº 12 da solicitação de adesão 927304-00001/2023.

Esta mensagem foi gerada automaticamente pelo sistema SIASGnet e não deve ser respondida.

De: siasgnet-atasrp@planejamento.gov.br
Para: [Thais Moisés](#)
Assunto: [SIASGnet-AtaSRP] Solicitação de Adesão Autorizada para a Ata do(a) Pregão Eletrônico 158516-31105/2022
Data: terça-feira, 11 de abril de 2023 14:30:49

Prezado Gestor,

O Gestor da Ata do(a) Pregão Eletrônico 158516-31105/2022 autorizou a adesão para o item Nº 7 da solicitação de adesão 927304-00001/2023.

Esta mensagem foi gerada automaticamente pelo sistema SIASGnet e não deve ser respondida.

De: siasgnet-atasrp@planejamento.gov.br
Para: [Thais Moisés](#)
Assunto: [SIASGnet-AtaSRP] Solicitação de Adesão Autorizada para a Ata do(a) Pregão Eletrônico 158516-31105/2022
Data: terça-feira, 11 de abril de 2023 14:30:46

Prezado Gestor,

O Gestor da Ata do(a) Pregão Eletrônico 158516-31105/2022 autorizou a adesão para o item Nº 3 da solicitação de adesão 927304-00001/2023.

Esta mensagem foi gerada automaticamente pelo sistema SIASGnet e não deve ser respondida.

De: siasgnet-atasrp@planejamento.gov.br
Para: [Thais Moisés](#)
Assunto: [SIASGnet-AtaSRP] Solicitação de Adesão Autorizada para a Ata do(a) Pregão Eletrônico 158516-31105/2022
Data: terça-feira, 11 de abril de 2023 14:30:45

Prezado Gestor,

O Gestor da Ata do(a) Pregão Eletrônico 158516-31105/2022 autorizou a adesão para o item Nº 35 da solicitação de adesão 927304-00001/2023.

Esta mensagem foi gerada automaticamente pelo sistema SIASGnet e não deve ser respondida.

De: siasgnet-atasrp@planejamento.gov.br
Para: [Thais Moisés](#)
Assunto: [SIASGnet-AtaSRP] Solicitação de Adesão Autorizada para a Ata do(a) Pregão Eletrônico 158516-31105/2022
Data: terça-feira, 11 de abril de 2023 14:30:20

Prezado Gestor,

O Gestor da Ata do(a) Pregão Eletrônico 158516-31105/2022 autorizou a adesão para o item Nº 34 da solicitação de adesão 927304-00001/2023.

Esta mensagem foi gerada automaticamente pelo sistema SIASGnet e não deve ser respondida.

De: siasgnet-atasrp@planejamento.gov.br
Para: [Thais Moisés](#)
Assunto: [SIASGnet-AtaSRP] Solicitação de Adesão Autorizada para a Ata do(a) Pregão Eletrônico 158516-31105/2022
Data: terça-feira, 11 de abril de 2023 14:31:17

Prezado Gestor,

O Gestor da Ata do(a) Pregão Eletrônico 158516-31105/2022 autorizou a adesão para o item Nº 25 da solicitação de adesão 927304-00001/2023.

Esta mensagem foi gerada automaticamente pelo sistema SIASGnet e não deve ser respondida.



Editais **31105/2022**

REGISTRO DE PREÇOS PARA AQUISIÇÃO DE EQUIPAMENTOS E SERVIÇOS PARA GERENCIAMENTO SEGURO DA REDE LAN/WLAN DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA.



PREGÃO ELETRÔNICO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA PREGÃO ELETRÔNICO Nº 31105/2022 (Processo Administrativo n.º 23292.030398/2022-96)

Torna-se público que o(a) Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, por meio do Departamento de Compras, sediado à rua 14 de Julho, 150, Coqueiros, CEP: 88075-010, Florianópolis-SC, realizará licitação, **para registro de preços**, na modalidade PREGÃO, na forma ELETRÔNICA, sob a forma de execução indireta, nos termos da Lei nº 10.520, de 17 de julho de 2002, da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 10.024, de 20 de setembro de 2019, do Decreto 9.507, de 21 de setembro de 2018, do Decreto nº 7.746, de 05 de junho de 2012, do Decreto nº 7.174, de 12 de maio de 2010, do Decreto nº 7.892, de 23 de janeiro de 2013, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, das Instruções Normativas SEGES/MP nº 05, de 26 de maio de 2017 e nº 03, de 26 de abril de 2018 e da Instrução Normativa SLTI/MPOG nº 01, de 19 de janeiro de 2010, da Lei Complementar nº 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto nº 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993 e as exigências estabelecidas neste Edital.

Data da sessão: 19/01/2023
Horário: 09h00min

Local: Portal de Compras do Governo Federal – <https://www.gov.br/compras/pt-br>
Critério de Julgamento: menor preço/ por item/por grupo
Regime de Execução: Empreitada por Preço Unitário

1 DO OBJETO

- 1.1 O objeto da presente licitação é a escolha da proposta mais vantajosa para a **AQUISIÇÃO DE EQUIPAMENTOS E SERVIÇOS PARA GERENCIAMENTO SEGURO DA REDE LAN/WLAN DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA**, conforme condições, quantidades e exigências estabelecidas neste edital e seus anexos.
- 1.2 A licitação será realizada em grupo único, formado por 35 itens, conforme tabela constante no Termo de Referência e Quadro de Especificações Mínimas, devendo o licitante oferecer proposta para todos os itens que o compõem.
- 1.3 O critério de julgamento adotado será o menor preço global do grupo, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.
- 1.4 Cada serviço ou produto do lote deverá estar discriminado em itens separados nas propostas de preços, de modo a permitir a identificação do seu preço individual na composição do preço global, e a eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam às Normas Técnicas Brasileiras - NTB
- 1.5 Os produtos listados neste grupo deverão ser do mesmo fabricante e compatíveis com a solução em implantação no IFSC - solução de rede sem fio e segurança FORTINET.
- 1.6 Os itens deste processo compõem solução única de tecnologia da informação e comunicação. São equipamentos para complementação da solução de rede sem fio e segurança em implantação no IFSC. O detalhamento encontra-se no Estudo Técnico Preliminar (ETP) e Termo de Referência (TR).
- 1.7 Aquisição de bens e serviços comuns.



2 DO REGISTRO DE PREÇOS

- 2.1 As regras referentes aos órgãos gerenciador e participantes, bem como a eventuais adesões são as que constam da minuta de Ata de Registro de Preços

3 DO CREDENCIAMENTO

- 3.1 O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.
- 3.2 O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio <https://www.gov.br/compras/pt-br/>, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.
- 3.3 O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.
- 3.4 O licitante responsabilizar-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.
- 3.5 É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles que se tornem desatualizados.
- 3.5.1 A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação

4 DA PARTICIPAÇÃO NO PREGÃO.

- 4.1 Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.
- 4.1.1 Os licitantes deverão utilizar o certificado digital para acesso ao Sistema.
- 4.1.2 Não há itens para participação exclusiva de microempresas e empresas de pequeno porte, nos termos do art. 48 da Lei Complementar nº 123, de 14 de dezembro de 2006.
- 4.1.3 Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 34 da Lei nº 11.488, de 2007, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006, bem como para bens e serviços produzidos no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010.
- 4.2 Não poderão participar desta licitação os interessados:
- 4.2.1 proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;
- 4.2.2 que não atendam às condições deste Edital e seu(s) anexo(s);
- 4.2.3 estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;
- 4.2.4 que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;
- 4.2.5 que estejam sob falência, concurso de credores ou insolvência, em processo de dissolução ou liquidação;



- 4.2.6 entidades empresariais que estejam reunidas em consórcio;
 - 4.2.7 organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário);
 - 4.2.8 sociedades *cooperativas*, considerando a vedação contida no art. 10 da Instrução Normativa SEGES/MP nº 5, de 2017.
- 4.3 Nos termos do art. 5º do Decreto nº 9.507, de 2018, é vedada a contratação de pessoa jurídica na qual haja administrador ou sócio com poder de direção, familiar de:
- a) detentor de cargo em comissão ou função de confiança que atue na área responsável pela demanda ou contratação; ou
 - b) de autoridade hierarquicamente superior no âmbito do órgão contratante.
- 4.4.1 Para os fins do disposto neste item, considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau (Súmula Vinculante/STF nº 13, art. 5º, inciso V, da Lei nº 12.813, de 16 de maio de 2013 e art. 2º, inciso III, do Decreto nº 7.203, de 04 de junho de 2010);
- 4.4 Nos termos do art. 7º do Decreto nº 7.203, de 2010, é vedada, ainda, a utilização, na execução dos serviços contratados, de empregado da futura Contratada que seja familiar de agente público ocupante de cargo em comissão ou função de confiança neste órgão contratante.
- 4.5 É vedada a contratação de uma mesma empresa para dois ou mais serviços licitados, quando, por sua natureza, esses serviços exigirem a segregação de funções, tais como serviços de execução e de avaliação, mensuração ou apoio à fiscalização.
- 4.6 Como condição para participação no Pregão, o licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:
- 4.6.1 que cumpre os requisitos estabelecidos no artigo 3º da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49.
 - 4.6.1.1 nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;
 - 4.6.1.2 nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.
 - 4.6.2 que está ciente e concorda com as condições contidas no Edital e seus anexos;
 - 4.6.3 que cumpre plenamente os requisitos de habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;
 - 4.6.4 que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;
 - 4.6.5 que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição;
 - 4.6.6 que a proposta foi elaborada de forma independente.
 - 4.6.7 que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;



- 4.6.8 que os equipamentos e serviços são fornecidos por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.
- 4.6.9 que cumpre os requisitos do Decreto n. 7.174, de 2010, estando apto a usufruir dos critérios de preferência.
- 4.6.9.1 A assinatura do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto no Decreto nº 7.174, de 2010.
- 4.7. A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

5 DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

- 5.1 Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para a abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio desse documento.
- 5.2 O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.
- 5.3 Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurando aos demais licitantes o direito de acesso aos dados constantes dos sistemas.
- 5.4 As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, §1º, da LC nº 123, de 2006.
- 5.5 Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.
- 5.6 Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;
- 5.7 Não será estabelecida, nesta etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.
- 5.8 Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

6 PREENCHIMENTO DA PROPOSTA

- 6.1 O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:
- 6.1.1 valor unitário e total do item;
- 6.1.2 Descrição do objeto, contendo as informações similares à especificação do Termo de Referência, além da marca e modelo no caso de aquisição de bens;
- 6.2 Todas as especificações do objeto contidas na proposta vinculam a Contratada.
- 6.3 Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos equipamentos e serviços;



- 6.3.1 A Contratada deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1º do artigo 57 da Lei nº 8.666, de 1993.
- 6.3.2 Caso o eventual equívoco no dimensionamento dos quantitativos se revele superior às necessidades da contratante, a Administração deverá efetuar o pagamento seguindo estritamente as regras contratuais de faturamento do quanto demandado e executado, concomitantemente com a realização, se necessário e cabível, de adequação contratual do quantitativo necessário, com base na alínea "b" do inciso I do art. 65 da Lei n. 8.666/93 e nos termos do art. 63, §2º da IN SEGES/MPDG n. 5/2017.
- 6.4 A empresa é a única responsável pela cotação correta dos encargos tributários. Em caso de erro ou cotação incompatível com o regime tributário a que se submete, serão adotadas as orientações a seguir:
- 6.4.1 cotação de percentual menor que o adequado: o percentual será mantido durante toda a execução contratual;
- 6.4.2 Cotação de percentual maior que o adequado: o excesso será suprimido, unilateralmente, da proposta e haverá glosa, quando do pagamento, e/ou redução, quando da repactuação, para fins de total ressarcimento do débito.
- 6.5 Se o regime tributário da empresa implica o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses, devendo o licitante ou contratada apresentar ao pregoeiro ou à fiscalização, a qualquer tempo, comprovação da adequação dos recolhimentos, para os fins do previsto no subitem anterior.
- 6.6 Independentemente do percentual de tributo inserido na proposta, no pagamento dos serviços, serão retidos na fonte os percentuais estabelecidos na legislação vigente.
- 6.7 A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de fornecer os equipamentos e serviços nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.
- 6.8 Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.
- 6.9 O prazo de validade da proposta não será inferior a 100 (cem) dias, a contar da data de sua apresentação.
- 6.10 Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;
- 6.10.1 O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato



7 DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

- 7.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.
- 7.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis, ilegalidades, ou não apresentem as especificações exigidas no Termo de Referência.
 - 7.2.1. Também será desclassificada a proposta que **identifique o licitante**.
 - 7.2.2. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.
 - 7.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.
- 7.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.
- 7.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.
- 7.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.
 - 7.5.1. O lance deverá ser ofertado pelo valor unitário do item/lote.
- 7.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.
- 7.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.
- 7.9. Será adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.
- 7.10. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de tempo de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.
- 7.11. Encerrado o prazo previsto no item anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até dez por cento superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o que será sigiloso até o encerramento deste prazo.
 - 7.11.1. Não havendo, pelo menos, três ofertas nas condições definidas neste item poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado até cinco minutos, o qual será sigiloso até o encerramento deste prazo.
- 7.12. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará os lances segundo a ordem crescente de valores.
 - 7.12.1. Não havendo lance final fechado e classificado na forma estabelecida nos itens anteriores, haverá o reinício da etapa fechada para que os demais licitantes, até no máximo de três, na ordem de classificação, possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo, observando-se, após, o item anterior.



- 7.13. Poderá o pregoeiro, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fechada, caso nenhum licitante classificado na etapa de lance fechado atender as exigências de habilitação
- 7.14. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.
- 7.15. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.
- 7.16. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.
- 7.17. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempos superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas após a comunicação do fato aos participantes no sítio eletrônico utilizado para divulgação.
- 7.18. O critério de julgamento adotado será o menor preço/menor desconto, conforme definido neste Edital e seus anexos.
- 7.19. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.
- 7.20. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.
- 7.21. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.
- 7.22. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.
- 7.23. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.
- 7.24. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.
- 7.25. Será assegurado o direito de preferência previsto no artigo 3º da Lei nº 8.248, de 1991, conforme procedimento estabelecido nos artigos 5º e 8º do Decreto nº 7.174, de 2010, nos seguintes termos:
- 7.25.1. Após a aplicação das regras de preferência para microempresas e empresas de pequeno porte, caberá a aplicação das regras de preferência, sucessivamente, para:
- 7.25.1.1. bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;**



7.25.1.2. bens e serviços com tecnologia desenvolvida no País; e

7.25.1.3. bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal, nos termos do art. 5º e 8º do Decreto 7.174, de 2010 e art. 3º da Lei nº 8.248, de 1991.

7.25.2. Os licitantes classificados que estejam enquadrados no item 7.25.1.1, na ordem de classificação, serão convocados para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame.

7.25.3. Caso a preferência não seja exercida na forma do item 7.25.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 7.25.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 7.25.1.3 caso esse direito não seja exercido.

7.25.4. As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

7.26. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

7.27. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se à preferência, sucessivamente, ao objeto executado:

7.27.1. por empresas brasileiras;

7.27.2. por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.27.3. por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

7.28. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas ou os lances empatados.

7.29. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital..

7.29.1. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

7.29.2. O pregoeiro solicitará ao licitante melhor classificado que, no prazo de, no mínimo, duas horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

7.29.3. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

7.30. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.



8 DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

- 8.1. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade de preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no §9º do art. 26 do Decreto nº 10.024/2019.
- 8.2. Será desclassificada a proposta ou o lance vencedor, nos termos do item 9.1 do Anexo VII-A da In SEGES/MPDG n. 5/2017, que:
 - 8.2.1. não estiver em conformidade com os requisitos estabelecidos neste edital;
 - 8.2.2. contenha vício insanável ou ilegalidade;
 - 8.2.3. não apresente as especificações técnicas exigidas pelo Termo de Referência;
 - 8.2.4. apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018-TCU – Plenário), desconto menor do que o mínimo exigido, ou que apresentar preço manifestamente inexequível.
 - 8.2.4.1. Quando o licitante não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:
 - 8.2.4.1.1. for insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.
- 8.3. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3º do artigo 43 da Lei nº 8.666, de 1993 e a exemplo das enumeradas no item 9.4 do Anexo VII-A da IN SEGES/MPDG N. 5, de 2017, para que a empresa comprove a exequibilidade da proposta.
- 8.4. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, e a inexequibilidade da proposta não for flagrante e evidente pela sua análise, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.
- 8.5. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.
 - 8.5.1. Na hipótese de necessidade de suspensão de sessão pública para a realização de diligências, com vista ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata.
- 8.6. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo de 2 horas, sob pena de não aceitação da proposta.
 - 8.6.1. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo;
- 8.7. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante da solução ou da área especializada no objeto.



- 8.8. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.
- 8.9. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a sua continuidade.
- 8.10. Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.
- 8.11. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.
- 8.12. O Pregoeiro solicitará ao licitante provisoriamente classificado em primeiro lugar que apresente ou envie juntamente com a proposta, sob pena de não-aceitação, certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012, conforme exigido no Termo de Referência.
- 8.13. O Pregoeiro solicitará ao licitante provisoriamente classificado em primeiro lugar que apresente ou envie juntamente com a proposta, sob pena de não-aceitação, comprovação de que os bens de informática e/ou automação ofertados não contêm substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil-polibromados (PBDEs). b.1) A comprovação poderá ser feita mediante apresentação de certificação emitida por instituição pública oficial ou instituição credenciada, ou por qualquer outro meio de prova, em especial laudo pericial, que ateste que o bem fornecido cumpre com as exigências do edital.

9. DA HABILITAÇÃO

- 9.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:
- a) SICAF;
 - b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);
 - c) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php);
 - d) Lista de Inidôneos mantida pelo Tribunal de Contas da União - TCU;
- 9.1.1. Para a consulta de licitantes pessoa jurídica poderá haver a substituição das consultas das alíneas “b”, “c” e “d” acima pela Consulta Consolidada de Pessoa Jurídica do TCU (<https://certidoesapf.apps.tcu.gov.br/>)
- 9.1.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei nº 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.



- 9.1.2.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.
- 9.1.2.2. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.
- 9.1.2.2.1. O Licitante será convocado para manifestação previamente à sua desclassificação.
- 9.2. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.
- 9.2.1. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.
- 9.3. Caso atendidas as condições de participação, a habilitação dos licitantes será verificada por meio do SICAF, nos documentos por ele abrangidos, em relação à habilitação jurídica, à regularidade fiscal e trabalhista, à qualificação econômica financeira e habilitação técnica, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.
- 9.3.1. O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF até o terceiro dia útil anterior à data prevista para recebimento das propostas;
- 9.3.2. É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.
- 9.3.3. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.
- 9.4. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de 2 horas sob pena de inabilitação.
- 9.5. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante a apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.
- 9.6. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.
- 9.7. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.
- 9.7.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferentes números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.
- 9.8. Ressalvado o disposto do item 5.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação.
- 9.9. **Habilitação jurídica:**



- 9.9.1. No caso de empresário individual, inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;
- 9.9.2. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;
- 9.9.3. Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;
- 9.9.4. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;
- 9.9.5. decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;
- 9.10. Regularidade fiscal e trabalhista:**
 - 9.10.1. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;
 - 9.10.2. prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.
 - 9.10.3. prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);
 - 9.10.4. prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;
 - 9.10.5. prova de inscrição no cadastro de contribuintes *estadual*, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
 - 9.10.6. prova de regularidade com a Fazenda Estadual do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;
 - 9.10.7. caso o licitante seja considerado isento dos tributos *estaduais* relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda *Estadual* do seu domicílio ou sede, ou outra equivalente, na forma da lei;
- 9.11. Qualificação Técnica:**
 - 9.11.1. As licitantes deverão apresentar Atestados de Capacidade Técnica para comprovação de aptidão para o fornecimento de bens em características e quantidades compatíveis com o objeto desta licitação, ou com o item pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.
 - 9.11.2. Os atestados deverão referir-se a produtos fornecidos no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;



- 9.11.3. Os atestados de capacidade técnica podem ser apresentados em nome da matriz ou da filial da empresa licitante;
- 9.12. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.
- 9.12.1. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.
- 9.13. Caso a proposta mais vantajosa seja ofertada por microempresa, empresa de pequeno porte ou sociedade cooperativa equiparada, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.
- 9.14. A não-regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.
- 9.15. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.
- 9.16. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.
- 9.17. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.
- 9.18. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

10 DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

- 10.1. A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de duas horas, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:
- 10.1.1. ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.
- 10.1.2. conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.
- 10.1.3. **A proposta final deverá ser datada, terá validade de 100 dias**, deverá conter, no mínimo: Nome da empresa, CNPJ, Representante legal, CPF do mesmo, Número de telefone válido, e endereço eletrônico (e-mail) válido, além da descrição do item ofertado, seu valor unitário e total, sua quantidade e sua unidade de fornecimento;
- 10.2. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.



- 10.2.1. Todas as especificações do objeto contidas na proposta vinculam a Contratada.
- 10.3. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).
- 10.3.1. Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.
- 10.4. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.
- 10.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.
- 10.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

11 DOS RECURSOS

- 11.1. O Pregoeiro declarará o vencedor e, depois de decorrida a fase de regularização fiscal e trabalhista de microempresa ou empresa de pequeno porte, se for o caso, concederá o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.
- 11.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.
- 11.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.
- 11.2.2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.
- 11.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três dias, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.
- 11.3. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.
- 11.4. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

12 DA REABERTURA DA SESSÃO PÚBLICA

- 12.1. A sessão pública poderá ser reaberta:
- 12.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.



12.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

12.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

12.2.1. A convocação se dará por meio do sistema eletrônico ("chat"), e-mail, de acordo com a fase do procedimento licitatório.

12.2.2. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

13 DA ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

13.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

14 DA GARANTIA DE EXECUÇÃO

Não haverá exigência de garantia de execução para a presente contratação, pois tratando-se de um serviço e aquisição comum de baixa complexidade, entende-se que a exigência garantia pode onerar a contratação.



15 DA ATA DE REGISTRO DE PREÇOS

- 15.1. Homologado o resultado da licitação, terá o adjudicatário o prazo de 5 (cinco) dias, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.
- 15.2. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura da Ata de Registro de Preços, a Administração poderá encaminhá-la para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinada e devolvida no prazo de 5 (cinco) dias, a contar da data de seu recebimento.
- 15.3. O prazo estabelecido no subitem anterior para assinatura da Ata de Registro de Preços poderá ser prorrogado uma única vez, por igual período, quando solicitado pelo(s) licitante(s) vencedor(s), durante o seu transcurso, e desde que devidamente aceito.
- 15.4. Serão formalizadas tantas Atas de Registro de Preços quanto necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.
 - 15.4.1. Será incluído na ata, sob a forma de anexo, o registro dos licitantes que aceitarem fornecer a solução com preços iguais aos do licitante vencedor na sequência da classificação do certame, quando o objeto não atender aos requisitos previstos no art. 3º da Lei nº 8.666, de 1993;

16 DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

- 16.1. Será dispensada a celebração do instrumento formal de contrato, substituído nesta aquisição por:
 - 16.1.1. O edital e seus anexos;
 - 16.1.2. A proposta final do fornecedor;
 - 16.1.3. A ata de registro de preços;
 - 16.1.4. A nota de empenho e autorização de fornecimento do serviço;
 - 16.1.5. A nota fiscal.
- 16.2. O adjudicatário terá o prazo de 3 (três) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou para aceitar a nota de empenho, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.
- 16.3. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.
- 16.4. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:
 - 16.4.1. referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;
 - 16.4.2. A contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;
 - 16.4.3. A contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.
- 16.5. O prazo de vigência da Ata de Registro de Preços é de 12 meses.



16.6. Previamente à contratação a Administração realizará consulta ao Sicaf para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

16.6.1. Nos casos em que houver necessidade de assinatura do instrumento de contrato, e o fornecedor não estiver inscrito no SICAF, este deverá proceder ao seu cadastramento, sem ônus, antes da contratação.

16.6.2. Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias úteis, sob pena de aplicação das penalidades previstas no edital e anexos.

16.7. Na assinatura do contrato ou da ata de registro de preços, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da ata de registro de preços.

16.8. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato ou a ata de registro de preços, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato ou a ata de registro de preços.

17 DO REAJUSTAMENTO EM SENTIDO GERAL

17.1. As regras acerca do reajustamento em sentido geral do valor contratual são as estabelecidas no Termo de Referência, anexo a este Edital.

18 DO MODELO DE EXECUÇÃO DO CONTRATO

18.1. O modelo de execução do contrato, contemplando os critérios de recebimento e aceitação do objeto estão previstos no Termo de Referência.

19 DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

19.1. As obrigações (deveres e responsabilidades) da Contratante e da Contratada e do órgão gerenciador da ata de registro de preços são as estabelecidas no Termo de Referência.

20 DO PAGAMENTO

20.1. As regras acerca do pagamento são as estabelecidas no Termo de Referência, anexo a este Edital.

20.2. É admitida a cessão de crédito decorrente da contratação de que trata este Instrumento Convocatório, nos termos do previsto na minuta contratual anexa a este Edital.

21 DAS SANÇÕES ADMINISTRATIVAS.

21.1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

21.1.1. não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

21.1.2. não assinar a ata de registro de preços, quando cabível;

21.1.3. apresentar documentação falsa;



- 21.1.4. deixar de entregar os documentos exigidos no certame;
- 21.1.5. ensejar o retardamento da execução do objeto;
- 21.1.6. não manter a proposta;
- 21.1.7. cometer fraude fiscal;
- 21.1.8. comportar-se de modo inidôneo;
- 21.2. As sanções do item acima também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente.
- 21.3. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.
- 21.4. O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, e quando não houver disposição específica no Termo de Referência, às seguintes sanções:
 - 21.4.1. Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;
 - 21.4.2. Multa de 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;
 - 21.4.3. Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;
 - 21.4.4. Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;
 - 21.4.4.1. A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa neste Edital.
 - 21.4.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;
- 21.5. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.
- 21.6. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.
- 21.7. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.
- 21.8. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à



Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

- 21.9. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.
- 21.10. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.
- 21.11. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.
- 21.12. As penalidades serão obrigatoriamente registradas no SICAF.
- 21.13. As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência.

22 A FORMAÇÃO DO CADASTRO DE RESERVA

- 22.1. Após o encerramento da etapa competitiva, os licitantes poderão reduzir seus preços ao valor da proposta do licitante mais bem classificado.
- 22.2. A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante melhor classificado.
- 22.3. Havendo um ou mais licitantes que aceitarem cotar suas propostas em valor igual ao do licitante vencedor, estes serão classificados segundo a ordem da última proposta individual apresentada durante a fase competitiva.
- 22.4. Esta ordem de classificação dos licitantes registrados deverá ser respeitada nas contratações e somente será utilizada acaso o melhor colocado no certame não assine a ata ou tenha seu registro cancelado nas hipóteses previstas nos artigos 20 e 21 do Decreto nº 7.892/213.

23 DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

- 23.1. Até 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.
- 23.2. A impugnação poderá ser realizada por forma eletrônica, pelo e-mail: licitacoes@ifsc.edu.br ou por petição dirigida ou protocolada no endereço da Reitoria do IFSC, rua 14 de Julho, 150, Coqueiros, Fpolis/SC - 88075-010 - Setor de PROTOCOLO.
- 23.3. Caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração deste Edital e seus anexos, decidir sobre a impugnação no prazo de até dois dias úteis contados da data de recebimento da impugnação.
- 23.4. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.
- 23.5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, no endereço indicado no Edital.



- 23.6. O pregoeiro responderá aos pedidos de esclarecimentos no prazo de dois dias úteis, contados da data do recebimento do pedido e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital e dos anexos
- 23.7. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.
- 23.7.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.
- 23.8. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.

24 DAS DISPOSIÇÕES GERAIS

- 24.1. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.
- 24.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.
- 24.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.
- 24.4. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.
- 24.5. A homologação do resultado desta licitação não implicará direito à contratação.
- 24.6. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.
- 24.7. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.
- 24.8. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.
- 24.9. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.
- 24.10. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.
- 24.11. O Edital está disponibilizado, na íntegra, no endereço eletrônico <https://www.gov.br/compras/pt-br/>, <https://sig.ifsc.edu.br/public/listaEditais.do?tipo=1&aba=p-comunicados> e também poderá ser lido e/ou obtido no endereço Rua 14 de Julho, 150, Coqueiros, Fpolis/SC 88075-010 (Departamento de Compras do IFSC), nos dias úteis, no horário das 08 horas às 17 horas, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados mediante prévio agendamento pelo e-mail licitacoes@ifsc.edu.br.



24.12. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

- ANEXO I – Termo de Referência;
- ANEXO II – Minuta de Ata de Registro de Preços;
- ANEXO III – Modelo de Termo de Compromisso de Manutenção de Sigilo;
- ANEXO IV – Modelo de Termo de Ciência;
- ANEXO V – Cadastramento da Empresa;
- ANEXO VI – Estudo Técnico Preliminar;
- ANEXO VII – Quadro de Especificações Mínimas.

Florianópolis, 06 de dezembro de 2022.

Aloisio Silva Junior
Pró-Reitor de Administração do IFSC

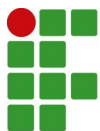
Anexo I
Edital 31105/2022

TERMO DE REFERÊNCIA

Processo Administrativo nº 23292.030398/2022-96

**REGISTRO DE PREÇOS PARA AQUISIÇÃO DE EQUIPAMENTOS E
SERVIÇOS PARA GERENCIAMENTO SEGURO DA REDE LAN/WLAN DO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE
SANTA CATARINA.**

Florianópolis, novembro/2022



Histórico de Revisões

Data	Versão	Descrição	Autor
21/09/2022	1.0	Início da primeira versão do documento.	Equipe de Planejamento
24/10/2022	1.1	Finalização da primeira versão do documento.	Equipe de Planejamento

TERMO DE REFERÊNCIA

Referência: Arts. 12 a 24 IN SGD/ME Nº 1/2019.

1 – OBJETO DA CONTRATAÇÃO

- 1.1. Expansão da solução de segurança para rede LAN/WLAN do IFSC.
- 1.2. Solução de segurança para rede LAN/WLAN com implantação em 2022 a partir da execução do processo 23292.10214/2021-24 - PE 32/2021.
- 1.3. O objeto principal deste processo licitatório é a solução única de TIC. Os serviços que compõem a solução são inerentes à instalação/configuração dos equipamentos a serem adquiridos, não sendo abrangidos pelo Art. 1º, § 3º da IN 01/SGD/2019 e suas alterações:
- 1.4. “...§ 3º Os órgãos e entidades deverão observar a necessidade de aprovação prévia dos processos que ensejaram a formação de atas de registro de preços de serviços de TIC passíveis de adesão por parte de órgãos ou entidades não participantes, para efeito do disposto no art. 22, § 10, inciso II do Decreto nº 7.892, de 23 de janeiro de 2013, regulamentado pela Instrução Normativa SGD/ME nº 5, de 2021. (Incluído pela Instrução Normativa nº 31, de 23 de março de 2021)...”
- 1.5. Os itens deste processo contemplam o quantitativo de materiais necessários para atendimento da demanda apresentada, bem como são identificados pelo código do Catálogo de Materiais, disponível no Portal de Compras do Governo Federal (art. 12, II e 14 da IN SGD/ME nº 1/2019).

2 – DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. Bens e serviços que compõem a solução

Item	Descrição	CATSER CATMAT
LOTE/GRUPO 1: Solução de Gerenciamento de Rede, Telefonia e Segurança		
1	INJETOR POE – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Injetor PoE (power injector) para alimentação de dispositivos PoE onde não há switch com esta tecnologia; 2. Deve permitir o fornecimento de energia capaz de alimentar os pontos de acesso deste processo; 3. Deve fornecer no mínimo 30 Watts para alimentação do dispositivo com suporte PoE atendendo ao padrão IEEE 802.3at; 4. Deve acompanhar cabos de energia e acessórios para o seu perfeito funcionamento; 5. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V ou 220V com comutação automática. Deve acompanhar o cabo de alimentação; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). ***** Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012.	426731
2	PONTO DE ACESSO INDOOR 1. Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede através dos wireless e que possua todas as suas configurações centralizadas na solução de gerenciamento de redes e	393277



segurança; 2. Deve suportar modo de operação centralizado, ou seja, sua operação depende da solução de gerenciamento de redes e segurança que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência; 3. Deve identificar automaticamente a solução de gerenciamento de redes e segurança ao qual se conectará; 4. Deve permitir ser gerenciado remotamente através de links WAN; 5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea; 6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio; 7. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação; 8. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento; 9. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente; 10. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN; 11. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad; 12. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB; 13. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC; 14. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e a solução de gerenciamento de redes e segurança. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até a solução de gerenciamento de redes e segurança; 15. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o a solução de gerenciamento de redes e segurança através de túnel IPSec; 16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até a solução de gerenciamento de redes e segurança, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 17. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até a solução de gerenciamento de redes e segurança; 18. Deve permitir operação em modo Mesh; 19. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências; 20. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio; 21. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL); 22. Deve suportar OFDMA; 23. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax; 24. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID; 25. Deve suportar BSS Coloring; 26. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz; 27. Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20); 28. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz; 29. Em conjunto com a solução de gerenciamento de redes e segurança, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados; 30. Em conjunto com a solução de gerenciamento de redes e segurança,



	deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 31. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz; 32. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps; 33. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS); 34. Em conjunto com a solução de gerenciamento de redes e segurança, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea; 35. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 36. Em conjunto com a solução de gerenciamento de redes e segurança, deve ser compatível e implementar o método de autenticação WPA3; 37. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 38. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP; 39. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 40. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 41. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 42. Deve implementar o padrão IEEE 802.11e; 43. Deve implementar o padrão IEEE 802.11h; 44. Deve implementar o padrão IEEE 802.3az; 45. Deve suportar ser gerenciado via SNMP; 46. Deve suportar consultas via REST API; 47. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação; 48. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45° C; 49. Deve suportar sistema antifurto do tipo Kensington Security Lock ou similar; 50. Deve possuir indicadores luminosos (LED) para indicação de status; 51. O ponto de acesso deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 52. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 53. Deve possuir certificado emitido pela Wi-Fi Alliance; 54. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 55. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 56. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 57. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.	
3	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE REDE E SEGURANÇA 1. Solução que permita administrar de maneira centralizada todos os elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede dos campus e	27456



que garanta suporte a processos relativos à LGPD; 2. Deverá ser totalmente compatível com a solução proposta para gerenciamento da segurança e infraestrutura de rede dos campus; 3. A solução deverá estar devidamente licenciada para administrar todos os pontos de acesso, switches e elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede deste processo pelo período do contrato; 4. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 5. A solução deverá ser composta por elemento ou elementos fornecido(s) na forma de appliance virtual (máquina virtual) compatível com Vmware ESXi, Microsoft Hyper-V ou Linux KVM; 6. A solução deverá garantir a integridade da configuração de um determinado item através de bloqueio de alterações quando ocorrer acesso simultâneo de dois ou mais administradores no mesmo ativo; 7. A solução deverá possibilitar a criação e administração de políticas de firewall, controle de aplicação e filtro de URL; 8. A solução deverá permitir criar, de forma centralizada, novos objetos que poderão ser utilizados nas políticas; 9. A solução deverá permitir que o administrador localize em quais regras um determinado objeto (ex: computador, serviço, etc.) está sendo utilizado; 10. A solução deverá atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS; 11. A solução deverá permitir a criação de regras de filtragem de tráfego que fiquem ativas apenas em horários pré-definidos; 12. A solução deverá permitir a criação de regras de filtragem de tráfego com data de expiração; 13. A solução deve possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem/conflitem com outras (shadowing) ou ainda garantir que esta exigência seja plenamente atendida por meio diverso; 14. A solução deve permitir a criação de templates de configuração de túneis VPN IPSec a serem aplicados de maneira centralizada e padronizada em elementos concentradores VPN; 15. A solução deve permitir agendamento para a execução de configurações nos elementos administrados; 16. A solução deve permitir a criação e execução de scripts em elementos administrados de maneira programada; 17. A solução deve permitir a criação de templates de configuração a serem aplicados de maneira centralizada e padronizada em elementos da rede sem fio e switches; 18. As seguintes características do SSID devem ser configuradas nos pontos de acesso através dos templates: nome do SSID, endereçamento DHCP a ser entregue aos clientes wireless, métodos de autenticação e agendamento da disponibilidade do SSID; 19. As seguintes características devem ser configuradas nos pontos de acesso através dos templates: potência de transmissão Wi-Fi, escolha do canal, tamanho do canal, configuração do algoritmo de seleção automática de potência e canal, configuração de short guard interval, modo de operação e acesso administrativo ao ponto de acesso; 20. As seguintes características de segurança devem ser configuradas na rede sem fio através dos templates: configuração da detecção de Rogue Aps e configuração de assinaturas de wIDS ou wIPS; 21. As seguintes características de Bluetooth Low Energy (BLE) devem ser configuradas nos pontos de acesso através dos templates: configuração do UUID, Major ID, Minor ID, Beacon Interval e potência; 22. As seguintes características de VLAN devem ser configuradas nos switches através dos templates: VLAN, VLAN ID e endereçamento IP; 23. As seguintes características de segurança devem ser configuradas nos switches através dos templates: Autenticação 802.1X, Autenticação MAB e Guest VLAN; 24. As seguintes características de rede devem ser configuradas nos switches através dos templates: configuração das portas com respectivas VLANs tagged e untagged, configuração do protocolo LLDP e configurações de QoS; 25. A solução deve permitir que o administrador selecione em quais elementos os templates de configuração deverão ser aplicados; 26. A solução deve listar os elementos administrados e seu status de operação; 27. A solução deve listar todos os clientes conectados na rede sem fio, o nome do ponto de acesso ao qual o cliente está conectado, qualidade do sinal da conexão de cada cliente, tipo de dispositivo utilizado na conexão e nome do SSID; 28. A solução deve listar todos os Rogue APs na rede sem fio, nome do SSID do propagado, canal impactado, nível de sinal detectado e nome do ponto de acesso



que detectou o Rogue AP; 29. A solução deve incorporar mapa mundi para visão unificada do status de operação dos elementos. Deve ainda permitir a adição de planta baixa de múltiplas localidades; 30. A solução deve garantir visão centralizada do status e estatísticas de uso das interfaces dos switches; 31. A solução deve apresentar a topologia da rede com status dos elementos e informações sobre a atuação do protocolo Spanning-Tree em interfaces; 32. A solução deve permitir a execução de testes remotos para identificação de problemas em cabos de rede conectados aos switches; 33. A solução deve permitir o agrupamento dos elementos administrados para aplicação de políticas ou templates de configuração; 34. A solução deverá realizar o backup automático das configurações dos elementos e permitir o retorno (rollback) de uma versão de configuração salva previamente; 35. A solução deverá possibilitar que o administrador visualize e compare diferentes versões de configurações dos elementos, sejam elas configurações vigentes, configurações anteriores e configurações antigas; 36. A solução deverá possuir sistema de backup e restauração de todas as configurações da própria ferramenta de administração centralizada; 37. A solução deverá identificar a versão de firmware em execução nos elementos administrados e garantir que quando houver novas versões de software para eles, que seja realizada a distribuição e instalação remota de maneira centralizada; 38. A solução deve permitir criar políticas/templates que definam a versão de firmware a ser distribuída e instalada em elementos administrados. Deve permitir ainda que o administrador da rede agende a atualização da versão de firmware de maneira automática nos elementos administrados; 39. A solução deve garantir visão centralizada das estatísticas de uso da rede sem fio; 40. A solução deve garantir visão centralizada das aplicações mais acessadas na rede, com informações sobre o volume total de dados trafegados para cada aplicação e a identificação dos usuários que fizeram os acessos; 41. A solução deve garantir visão centralizada das categorias de websites mais acessados na rede, com informações sobre o volume total de dados trafegados para cada categoria e a identificação dos usuários que fizeram os acessos; 42. A solução deve garantir visão centralizada dos usuários que mais trafegaram dados na rede, com informações sobre os hosts aos quais o usuário estava conectado, volume de dados trafegados e os endereços de destino que foram acessados; 43. A solução deve garantir visão centralizada das estatísticas de uso dos túneis VPN, com informações sobre volume de dados trafegados, horário da conexão e identificação do usuário que conectou na VPN; 44. A solução deverá ser capaz de receber os logs dos elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede das unidades e apresentá-los de forma centralizada; 45. A solução deverá ser capaz de receber, no mínimo, 5GB de logs diários; 46. A solução deverá ser capaz de armazenar, no mínimo, 3TB de informação; 47. A solução deverá ser capaz de armazenar os logs por 12 meses; 48. A solução deverá possuir mecanismo para que logs antigos sejam removidos automaticamente; 49. A solução deverá permitir a exportação dos logs; 50. A solução deverá permitir que o administrador realize download de um determinado conjunto de logs em formato texto ou CSV; 51. A solução deverá garantir a geração de relatórios com mapas geográficos ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego; 52. A solução deverá permitir a extração de relatórios; 53. A solução deverá possuir relatórios pré-definidos; 54. A solução deverá possibilitar a duplicação de relatórios e gráficos existentes para edição dos mesmos logo em seguida; 55. A solução deverá permitir a personalização de capas para os relatórios; 56. A solução deverá permitir a geração de relatórios de logs de tráfego de dados; 57. A solução deverá permitir a personalização dos relatórios para inserção de gráficos dos tipos barra, linha, tabela e pizza; 58. A solução deverá possibilitar o envio de relatórios por e-mail de maneira automática; 59. A solução deverá permitir a customização de quaisquer relatórios fornecidos pela solução, exclusivamente a critério da contratante, adaptando-o às suas necessidades; 60. A solução deverá permitir a definição de filtros nos relatórios; 61. A solução deverá ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes,



	cores, entre outros; 62. A solução deverá garantir a capacidade de criar consultas avançadas em sua base de dados que para as informações sejam utilizadas em gráficos e tabelas dentro dos relatórios; 63. A solução deverá implementar autenticação administrativa através dos protocolos RADIUS ou TACACS; 64. A solução deverá permitir a criação de múltiplos perfis de usuários administradores com permissões granulares para limitar o acesso a determinadas funções e garantir privilégios de somente leitura e/ou leitura-escrita a outras; 65. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7. Durante o período de garantia deve ser possível a atualização do software para novas versões. 66. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 67. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.	
4	LICENÇAS PARA TELEFONE - SOFTPHONE 1. O softphone deve ser um aplicativo com capacidade de se registrar no controlador de chamadas existente neste órgão e atender os seguintes requisitos: 1.1. Deve possuir versões para os sistemas operacionais Windows, MacOS, iOS e Android; 1.2. Deve possuir login por usuário e senha; 1.3. Deve ser homologado para funcionar em conjunto com o Controlador de Chamadas fornecido neste grupo; 2. Deve suportar no mínimo os seguintes codecs: 2.1. G.711u; 2.2. G.711a; 2.3. G.729a; 2.4. G.722; 3. Deve possuir a funcionalidade de "Não perturbe", com o objetivo de não ser notificado de se uma ligação está entrando; 4. Deve suportar funcionalidades como chamada em espera, transferência, alternância entre chamadas recebidas e conferência entre as chamadas recebidas; 5. Deve permitir a gravação de uma chamada 6. Deve permitir chamadas simultâneas e alternar entre elas; 7. Deve possuir indicador de mensagem no correio de voz; 8. Deve possuir o histórico de chamadas com no mínimo a identificação do número recebido e discado, data e hora; 9. Softphone para Windows e MACOS devem suportar: 9.1. Deve suportar o envio e recebimento de FAX; 9.2. Deve suportar a conexão com STUN (Session Traversal Utilities for NAT) server; 9.3. Deve suportar chamadas de vídeo usando no mínimo os codecs H.264, VP9 e VP8; 10. Deve ser garantida atualização de software/firmware durante o período de garantia.	27456
5	PONTO DE ACESSO OUTDOOR 1. Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede através da wireless e que possua todas as suas configurações centralizadas na solução de gerenciamento de redes e segurança; 2. Deve suportar modo de operação centralizado, ou seja, sua operação depende da solução de gerenciamento de redes e segurança que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência; 3. Deve identificar automaticamente a solução de gerenciamento de redes e segurança ao qual se conectará; 4. Deve permitir ser gerenciado remotamente através de links WAN; 5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea; 6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio; 7. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação; 8. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento; 9. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente; 10. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T, ou superior, com conector RJ-45 para permitir a conexão com a rede LAN; 11. Deve implementar link	393277



aggregation de acordo com o padrão IEEE 802.3ad; 12. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB; 13. Deve permitir sua alimentação através de Power Over Ethernet (PoE). Deve acompanhar injetor PoE para alimentação do equipamento; 14. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e a solução de gerenciamento de redes e segurança. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até a solução de gerenciamento de redes e segurança; 15. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para a solução de gerenciamento de redes e segurança através de túnel IPSec; 16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até a solução de gerenciamento de redes e segurança, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 17. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até a solução de gerenciamento de redes e segurança; 18. Deve permitir operação em modo Mesh; 19. Deve possuir potência de irradiação de 25dBm em 2.4GHz e 5GHz; 20. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1.2 Gbps em um único rádio; 21. Deve suportar MUMIMO com operações em Downlink (DL) e Uplink (UL); 22. Deve suportar OFDMA com operações em Downlink (DL) e Uplink (UL); 23. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax; 24. Deve implementar recurso de Target Wake Time (TWT) configurado por SSID; 25. Deve suportar BSS Coloring; 26. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz; 27. Deve possuir sensibilidade mínima de -91dBm quando operando em 5GHz com MCS0 (HT20); 28. Deve possuir antenas internas ao equipamento com ganho mínimo de 6dBi em 2.4GHz e 6dBi em 5GHz; 29. Em conjunto com a solução de gerenciamento de redes e segurança, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados; 30. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não WiFi e que operem nas frequências de 2.4GHz ou 5GHz; 31. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps; 32. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS); 33. Em conjunto com a solução de gerenciamento de redes e segurança, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 8 (oito) SSIDs com operação simultânea; 34. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 35. Em conjunto com a solução de gerenciamento de redes e segurança, deve ser compatível e implementar o método de autenticação WPA3 com 802.1X; 36. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 37. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos



	pelos servidores RADIUS; 38. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 39. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o <i>roaming</i>; 40. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 41. Deve implementar o padrão IEEE 802.11e; 42. Deve implementar o padrão IEEE 802.11h; 43. Deve implementar o padrão IEEE 802.3az; 44. Deve suportar consultas SNMP diretamente no ponto de acesso; 45. Deve suportar consultas REST API diretamente no ponto de acesso; 46. Deve possuir estrutura robusta para operação em ambientes externos e permitir ser instalado em paredes e postes. Deve acompanhar os acessórios para fixação em paredes e postes; 47. Deve ser capaz de operar em ambientes com temperaturas entre -10 e 60° C; 48. O equipamento deve possuir grau de proteção IP67. Não serão aceitos equipamentos instalados em acessórios, por exemplo caixas herméticas, para que alcancem este grau de proteção; 49. Deve possuir indicadores luminosos (LED) para indicação de status das interfaces físicas e dos rádios WiFi; 50. O ponto de acesso deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 51. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 52. Deve possuir certificado emitido pela Wi-Fi Alliance; 53. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 54. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 55. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 56. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.	
6	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 1 1. A PROPONENTE será responsável pela instalação/configuração da solução apresentada no item 20 conforme tabela acima respeitando a quantidade adquirida em ATA. 2. As instalações, que ocorrerão em etapas: 2.1. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano. 2.2. Este serviço deverá incluir avaliação de pré-implantação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 3. Fases: 3.1. Avaliação de pré-implantação 3.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 3.2. Cronograma do plano de implementação 3.2.1. Após a avaliação, o especialista contratado designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 3.3. Garantia de qualidade 3.3.1. A contratante deverá garantir a qualidade por meio	27090



	de testes em laboratório da CONTRATADA com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real. 3.4. Execução 3.4.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 3.4.2. A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 3.5. Monitoramento 3.5.1. A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente. 3.6. Relatório de implementação 3.6.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 8. Será de responsabilidade do CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto ao console de configuração do equipamento; 9. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 10. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. A CONTRATADA deverá fazer a migração de regras do Firewall da CONTRATANTE para a nova solução. 13. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas;	
7	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 2 1. A PROPONENTE será responsável pela instalação/configuração da solução apresentada no item 21 conforme tabela acima respeitando a quantidade adquirida em ATA. 2. As instalações, que ocorrerão em etapas: 2.1. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano. 2.2. Este serviço deverá incluir avaliação de pré-implantação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 3. Fases: 3.1. Avaliação de pré-implantação 3.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 3.2. Cronograma do plano	27090



	de implementação 3.2.1. Após a avaliação, o especialista contratado designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 3.3. Garantia de qualidade 3.3.1. A contratante deverá garantir a qualidade por meio de testes em laboratório da CONTRATADA com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real. 3.4. Execução 3.4.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 3.4.2. A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 3.5. Monitoramento 3.5.1. A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente. 3.6. Relatório de implementação 3.6.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 8. Será de responsabilidade do CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 9. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 10. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. A CONTRATADA deverá fazer a migração de regras do Firewall da CONTRATANTE para a nova solução. 13. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas;	
8	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 3 1. A PROPONENTE será responsável pela conexão física do Equipamento do item 22 conforme tabela acima respeitando a quantidade adquirida em ATA. 2. As instalações, que ocorrerão em etapas: 2.1. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano. 2.2. Este serviço deverá incluir avaliação	27090



	de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 3. Fases: 3.1. Avaliação de pré-implementação 3.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 3.2. Cronograma do plano de implementação 3.2.1. Após a avaliação, o especialista contratada designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 3.3. Garantia de qualidade 3.3.1. A contratante deverá garantir a qualidade por meio de testes em laboratório da CONTRATADA com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real. 3.4. Execução 3.4.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 3.4.2. A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 3.5. Monitoramento 3.5.1. A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente. 3.6. Relatório de implementação 3.6.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 9. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 10. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. A CONTRATADA deverá fazer a migração de regras do Firewall da CONTRANTE para a nova solução. 13. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas;	
9	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 4 1. A PROPONENTE será responsável pela	27090



conexão física do Equipamento do item 23 conforme tabela acima respeitando a quantidade adquirida em ATA. 2. As instalações, que ocorrerão em etapas: 2.1. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano. 2.2. Este serviço deverá incluir avaliação de pré-implantação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 3. Fases: 3.1. Avaliação de pré-implantação 3.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 3.2. Cronograma do plano de implementação 3.2.1. Após a avaliação, o especialista contratado designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 3.3. Garantia de qualidade 3.3.1. A contratante deverá garantir a qualidade por meio de testes em laboratório da CONTRATADA com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real. 3.4. Execução 3.4.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 3.4.2. A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 3.5. Monitoramento 3.5.1. A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente. 3.6. Relatório de implementação 3.6.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 9. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 10. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. A



	CONTRATADA deverá fazer a migração de regras do Firewall da CONTRANTE para a nova solução. 13. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas;	
10	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 5 1. A PROPONENTE será responsável pela conexão física do Equipamento do item 24 conforme tabela acima respeitando a quantidade adquirida em ATA. 2. As instalações, que ocorrerão em etapas: 2.1. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano. 2.2. Este serviço deverá incluir avaliação de pré-implantação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 3. Fases: 3.1. Avaliação de pré-implantação 3.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 3.2. Cronograma do plano de implementação 3.2.1. Após a avaliação, o especialista contratada designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 3.3. Garantia de qualidade 3.3.1. A contratante deverá garantir a qualidade por meio de testes em laboratório da CONTRATADA com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real. 3.4. Execução 3.4.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 3.4.2. A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 3.5. Monitoramento 3.5.1. A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente. 3.6. Relatório de implementação 3.6.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 9. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 10. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos	27090



	técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. A CONTRATADA deverá fazer a migração de regras do Firewall da CONTRATANTE para a nova solução. 13. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas;	
11	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 6 1. A PROPONENTE será responsável pela conexão física do Equipamento do item 25 conforme tabela acima respeitando a quantidade adquirida em ATA. 2. As instalações, que ocorrerão em etapas: 2.1. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano. 2.2. Este serviço deverá incluir avaliação de pré-implantação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 3. Fases: 3.1. Avaliação de pré-implantação 3.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 3.2. Cronograma do plano de implementação 3.2.1. Após a avaliação, o especialista contratada designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 3.3. Garantia de qualidade 3.3.1. A contratante deverá garantir a qualidade por meio de testes em laboratório da CONTRATADA com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real. 3.4. Execução 3.4.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 3.4.2. A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 3.5. Monitoramento 3.5.1. A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente. 3.6. Relatório de implementação 3.6.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 8. Será de responsabilidade da CONTRATANTE disponibilizar a	27090



	instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 9. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 10. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. A CONTRATADA deverá fazer a migração de regras do Firewall da CONTRANTE para a nova solução. 13. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas;	
12	SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE REDES E SEGURANÇA 1. A PROPONENTE será responsável pela instalação/configuração da solução apresentada no item 03 respeitando a quantidade adquirida em ATA. 2. As instalações, que ocorrerão em etapas: 2.1. O serviço de implantação será fornecido para implementar a implantação do dispositivo no ambiente de rede da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano. 2.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 3. Fases: 3.1. Avaliação de pré-implementação 3.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 3.2. Cronograma do plano de implementação 3.2.1. Após a avaliação, o especialista contratada designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 3.3. Garantia de qualidade 3.3.1. A contratante deverá garantir a qualidade por meio de testes em laboratório da CONTRATADA com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real. 3.4. Execução 3.4.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 3.4.2. A maior parte da implementação poderá ser realizada remotamente. E suporte no local também deverá ser fornecido durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 3.5. Monitoramento 3.5.1. A solução funciona como solução projetada. Se ocorrer algum problema, ele será tratado imediatamente. 3.6. Relatório de implementação 3.6.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. No caso de desativação de	27090



	equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 9. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 10. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas;	
13	SERVIÇO DE INSTALAÇÃO/CONFIGURAÇÃO - TELEFONIA TIPO 1 1. Este serviço deve englobar o serviço de instalação, configuração e customização dos seguintes itens deste grupo: 1.1. Sistema de Voz – Tipo I - VM 2. Este serviço será executado on-site, em cada um dos campus deste órgão; 3. Deve ser instalado nos locais definidos por este órgão; 4. Os serviços devem ser realizados por técnico com certificação técnica emitida pelo fabricante dos equipamentos; 5. No mínimo as seguintes configurações devem ser realizadas: 5.1. Instalação, configuração e testes do Controlador e Gateway de Voz; 5.2. Configurações para integração com o Controlador de Chamadas; 5.3. Plano de discagem; 5.4. Rota de Menor Custo; 5.5. Grupos de Captura; 5.6. Recurso de conferência; 5.7. Música em espera local; 5.8. Criptografia das Chamadas; 5.9. Configuração do entroncamento E1; 5.10. Configuração de entroncamento SIP; 5.11. Configuração de integração com serviço fone@RNP; 5.12. Configuração e testes do modo de emergência; 5.13. Instalação e configuração dos Terminais de Comunicação; 5.14. Demais parâmetros que forem alinhados na reunião de pré-projeto 6. Ao final da instalação deverá ser realizado, para cada equipamento instalado, um repasse de informações hands-on com pelo menos 2 horas de duração, demonstrando o correto funcionamento das funcionalidades solicitadas e apresentando as configurações realizadas nos equipamentos; 7. Este órgão irá fornecer pontos elétricos e lógicos necessários para a instalação dos equipamentos, assim como a configuração dos ativos de rede para o pleno funcionamento da solução; 8. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, reunião esta que pode ser por telefone ou webconferência, devendo a contratada sugerir as configurações de acordo com normas e boas práticas, cabendo a contratante a aceitação ou não; 9. Esta reunião de pré-projeto deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho) elaborado pela CONTRATADA. Neste documento devem conter o objetivo dos serviços, as atividades que serão realizadas, os prazos estimados para cada atividade, as diretrizes dos serviços que serão realizados, os locais de execução, as informações necessárias, os padrões que serão aplicados, o nome do(s) gerente(s) de projetos responsável e do(s) técnico(s) responsável(is) pela execução dos serviços. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes; 10. Os preços devem refletir a instalação, configuração e customização de todos os equipamentos descritos neste item; 11. Devem estar incluídas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços; Ao término do	27090



	serviço deve ser fornecido um relatório contendo todas as configurações realizadas de modo a facilitar a administração da solução por este órgão e permitir a continuidade do funcionamento da solução.	
14	SERVIÇO DE INSTALAÇÃO/CONFIGURAÇÃO - TELEFONIA TIPO 2 1. Este serviço deve englobar o serviço de instalação, configuração e customização dos seguintes itens deste grupo: 1.1. Sistema de Voz – Tipo II - VM 2. Este serviço será executado on-site, em cada um dos campus deste órgão; 3. Deve ser instalado nos locais definidos por este órgão; 4. Os serviços devem ser realizados por técnico com certificação técnica emitida pelo fabricante dos equipamentos; 5. No mínimo as seguintes configurações devem ser realizadas: 5.1. Instalação, configuração e testes do Controlador e Gateway de Voz; 5.2. Configurações para integração com o Controlador de Chamadas; 5.3. Plano de discagem; 5.4. Rota de Menor Custo; 5.5. Grupos de Captura; 5.6. Recurso de conferência; 5.7. Música em espera local; 5.8. Criptografia das Chamadas; 5.9. Configuração do entroncamento E1; 5.10. Configuração de entroncamento SIP; 5.11. Configuração de integração com serviço fone@RNP; 5.12. Configuração e testes do modo de emergência; 5.13. Instalação e configuração dos Terminais de Comunicação; 5.14. Demais parâmetros que forem alinhados na reunião de pré-projeto 6. Ao final da instalação deverá ser realizado, para cada equipamento instalado, um repasse de informações hands-on com pelo menos 2 horas de duração, demonstrando o correto funcionamento das funcionalidades solicitadas e apresentando as configurações realizadas nos equipamentos; 7. Este órgão irá fornecer pontos elétricos e lógicos necessários para a instalação dos equipamentos, assim como a configuração dos ativos de rede para o pleno funcionamento da solução; 8. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, reunião esta que pode ser por telefone ou webconferência, devendo a contratada sugerir as configurações de acordo com normas e boas práticas, cabendo a contratante a aceitação ou não; 9. Esta reunião de pré-projeto deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho) elaborado pela CONTRATADA. Neste documento devem conter o objetivo dos serviços, as atividades que serão realizadas, os prazos estimados para cada atividade, as diretrizes dos serviços que serão realizados, os locais de execução, as informações necessárias, os padrões que serão aplicados, o nome do(s) gerente(s) de projetos responsável e do(s) técnico(s) responsável(is) pela execução dos serviços. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes; 10. Os preços devem refletir a instalação, configuração e customização de todos os equipamentos descritos neste item; 11. Devem estar incluídas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços; Ao término do serviço deve ser fornecido um relatório contendo todas as configurações realizadas de modo a facilitar a administração da solução por este órgão e permitir a continuidade do funcionamento da solução.	27090
15	SERVIÇO TÉCNICO PARA SITE SURVEY 1. O serviço de Site Survey será utilizado para análise técnica do ambiente real dos câmpus do IFSC em todas as localidades do estado de Santa Catarina de forma presencial nos respectivos endereços, apoiada por ferramentas e softwares adequados, que indiquem: 1.1. O melhor posicionamento dos dispositivos pontos de acesso de rede sem fio para a maximização da cobertura do sinal de RF; 1.2. A quantidade exata de pontos de acesso a serem instalados por prédio; 1.3. Fontes e zonas de interferência; 1.4. O canal de frequência a ser utilizado por cada ponto de acesso; 1.5. As áreas de cobertura e as taxas de transmissão ou faixas de nível de recepção de sinal de RF em desenho colorido; 2. A unidade de serviço deve contemplar um campus independente da sua localidade; 3. Será de responsabilidade da CONTRATANTE a disponibilização de planta arquitetônica em CAD (*.dwg) para realização de predição teórica e confecção de as-built; 4. Será de responsabilidade da CONTRATADA os seguintes serviços abaixo: 4.1. A disponibilização de um ou mais técnicos para realização de testes em campos para	27090



	determinar a melhor disposição dos pontos de acesso de rede sem fio; 4.2. Relatório técnico de vistoria resultante da predição teórica das plantas fornecidas pela CONTRATANTE com as seguintes informações: 4.2.1. As possíveis limitações físicas ou dificuldades de implementação detectadas nos locais – restrições da construção, obstáculos, etc.; 4.2.2. Melhor posicionamento dos dispositivos em cada andar das localidades visando a maximização da cobertura do sinal de RF; 4.2.3. A quantidade exata de pontos de acesso a ser instalados em cada andar e locais previstos no projeto; 4.2.4. As zonas e faixas de interferência detectadas durante o mapeamento de rádio frequência; 4.2.5. As faixas de frequência a serem utilizadas para cada ponto de acesso; 4.2.6. As áreas de cobertura e as taxas de transmissão ou faixas de nível de recepção de sinal de RF avaliados durante o mapeamento; 5. O relatório técnico deverá ser emitido com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA; 6. Todos os instrumentos/equipamentos e softwares necessários para a execução do serviço serão fornecidos pela CONTRATADA; 7. O relatório técnico de vistoria com o resultado do estudo de site survey deverá ser entregue ao analista ou técnico de TI lotados no câmpus em avaliação, em via impressa ou em meio digital em até 30 (trinta) dias úteis após assinatura do contrato para os itens acima citados.	
16	SISTEMA DE VOZ - TIPO I - VM CARACTERÍSTICAS GERAIS: ----- Administração do Sistema 1. O sistema proposto deve ter pelo menos dois métodos de configuração através de uma interface Web e através de uma linha de comando acessível através de um console serial, telnet ou SSH. 2. O equipamento proposto deve possuir um endereço IP padrão em uma de suas interfaces para poder iniciar a instalação e configuração diretamente na interface Web. 3. O sistema proposto deve ter um assistente de configuração para poder realizar os passos iniciais da configuração até a realização de chamadas telefônicas. 4. Deve ter uma página web para que os usuários possam gerenciar suas extensões incluindo as seguintes funcionalidades: 5. Verificação do correio de voz, incluindo reproduzir, excluir ou salvar mensagens de correio de voz 6. Usar o operador de console para processar chamadas da empresa. 7. Verificar o registro de chamadas para chamadas discadas, recebidas e não atendidas ou armazene correios de voz 8. Revisar o diretório corporativo 9. Gerenciar chamadas 10. Configurar perfil de telefone 11. Personalizar arquivos de som. 12. Para acessar esta página da web, o usuário deve inserir seu número de ramal e um PIN na página. Monitoramento do Sistema 13. O sistema proposto deve ter um dashboard para verificar o estado geral do equipamento incluindo o número de série, o tempo de operação, a disponibilidade de recursos de memória, CPU e largura de banda de rede utilizada, a versão do sistema operacional, bem como um histórico de estatísticas de chamadas. 14. Esta Interface deve ser personalizável para poder selecionar as informações mais relevantes e até mesmo entrar na linha de comando por este meio. 15. O sistema de monitoramento dos equipamentos propostos deve permitir a visualização de chamadas de saída, chamadas em espera, chamadas em conferência, ramais, troncos, filas de chamadas, clientes DHCP e telefones não atribuídos. 16. Para chamadas ativas, o sistema deve mostrar em tempo real, incluindo os números que estão sendo chamados e de onde as chamadas estão sendo feitas, bem como os troncos que estão sendo usados naquele momento, o status da chamada e sua duração 17. Deve mostrar os detalhes das chamadas de conferência incluindo o nome da conferência, o número dos ramais na conferência e a duração da conferência. 18. Deve apresentar a informação de todos os ramais incluindo o estado, seu identificador, o número, o nome do usuário, o tipo de ramal e o tipo de telefone conectado. 19. Para o status dos troncos, o sistema deve mostrar em tempo real incluindo os nomes, endereços IP, tipo de tronco e se estiver conectado e cadastrado na operadora, o status deve mostrar se está em serviço, se está não disponível, se estiver em alarme ou se estiver desabilitado. 20. Exibir o status dos faxes. 21. O sistema deve ter um serviço de relatórios e entregá-los em HTML ou PDF 22. Deve ter um sistema de logs acessível diretamente da página web que deve permitir pesquisas com critérios personalizados e poder exportá-los para uma tabela.	474397



Configuração do sistema 23. O sistema proposto deve suportar IPv4 e IPv6 24. Deve suportar a criação de VLANs e a criação de interfaces redundantes combinando duas ou mais interfaces físicas para fornecer redundância. 25. Deve conter pelo menos 4 portas Ethernet 10/100/1000 BaseT. 26. Deve permitir a criação de rotas estáticas 27. Deve funcionar como servidor DHCP 28. Deve permitir a captura de pacotes e armazenar essas informações em um arquivo “.pcap” para análise posterior. 29. Suportar a criação de diferentes contas de administrador e poder limitar o acesso de endereços IP específicos. 30. A autenticação deve ser feita localmente ou por meio de um servidor LDAP 31. Suporte a diferentes perfis de administração, como contas de monitor, onde você só tem direitos de leitura do sistema 32. Suporta um esquema de alta disponibilidade com um dispositivo ativo e um dispositivo passivo, fazendo alterações no dispositivo ativo e replicando automaticamente a configuração no dispositivo passivo. 33. Selecione o fuso horário em que o equipamento vai funcionar bem como o uso de servidores NTP para garantir o horário dentro do equipamento. 34. Suporte a políticas de senha, como a escolha do número mínimo de caracteres solicitados na senha, bem como o uso de letras maiúsculas ou minúsculas e caracteres especiais. 35. Suporte SNMPv3 36. Configure pelo menos um servidor de correio para enviar mensagens de alerta do sistema. 37. Interface gráfica personalizável 38. Suportar uma pré-autorização para integrar o sistema através do uso de certificados digitais para fazer uma conexão segura. Configuração do sistema telefônico 39. Seleção do país onde será colocado o equipamento proposto. 40. Suporte à configuração do número de emergência 41. Configuração de prefixos para atender chamadas externas, interurbanas e internacionais. 42. Configurando padrões para planos de discagem para ramais 43. Configuração de templates para envio de emails e relatórios. 44. Configuração SIP para a seleção das portas RTP, TCP e UDP a serem utilizadas 45. Suporte ao provisionamento automático da configuração SIP do telefone 46. Suporte para uso de diferentes arquivos de áudio para atendedores automáticos e música em espera. 47. Configuração de diferentes perfis para ramais que incluem diferentes serviços como seleção de codec para telefones. 48. Suporte a fax sobre IP 49. Suporte à modificação do identificador de chamadas e possibilidade de mapeá-lo para um grupo de ramais 50. Configuração de atendimento de chamadas dependendo do agendamento 51. Configuração remota de teclas programáveis em telefones SIP 52. Quando apenas a conectividade SIP está disponível, o sistema também pode ser instalado em uma instância virtual no vSphere, HyperV, KVM e XEN Server. 53. Você deve poder contar com um módulo para hotéis Configurações das extensões 54. Configuração remota de teclas programáveis em telefones SIP 55. Configuração de ramais IP locais e remotos onde o usuário discará apenas o número do ramal e o sistema proposto discará um número local ou celular. 56. O sistema proposto deve ser capaz de gerar automaticamente senhas e PINs para cada ramal ou ser definido pelo administrador. 57. Deve ter a facilidade de importar e exportar a lista de extensões para um arquivo no formato CSV 58. Reinicializar o telefone remotamente 59. Deve ser fácil aplicar a mesma alteração ou modificação para variar as extensões ao mesmo tempo. 60. O sistema proposto deve detectar o tipo de telefone IP que cada um dos ramais possui. 61. Deve ser possível selecionar um perfil SIP para cada um dos ramais IP. 62. Deve ser possível conceder diferentes privilégios aos usuários dos ramais IP. 63. Cada ramal IP deve ter uma caixa postal de voz e os telefones IP devem ter um LED que permaneça aceso para notificar o usuário de que há uma entrada em sua caixa postal. 64. O sistema deve ser capaz de auditar ramais para determinar se há senhas fracas. 65. Deve possuir um sistema que permita a localização de ramais repetidos, em conflito ou sem número. 66. Suportará a importação de uma lista de extensões de um arquivo CSV 67. Suporta o protocolo T38 para manipulação de Fax sobre VoIP. 68. Definir após quantas vezes o ramal toca para ser enviado ao correio de voz 69. Enviar um e-mail com a mensagem do correio de voz como anexo. 70. Deve ser possível configurar o gerenciamento de chamadas de acordo com o calendário e qual ação deve ser seguida se o ramal estiver ocupado, não atender ou estiver em modo “não perturbe”. 71. Deve ser possível criar grupos de



	ramais, para que uma chamada de entrada toque da mesma forma em todos os ramais pertencentes a este grupo ou faça-o sequencialmente onde tocará em cada ramal separadamente dentro do grupo. 72. O sistema proposto deve ter um sistema de anúncio (paging) 73. Adicionalmente, deve ser possível criar grupos de trabalho onde um usuário possa atender uma chamada que esteja tocando em outro ramal pertencente ao seu grupo. 74. Você deve ter uma caixa postal geral. 75. Apoiar a criação de ramais virtuais que não serão fixos em um único telefone IP. Configuração de tronco 76. O sistema deve suportar vários tipos de troncos como E1, troncos SIP e linhas analógicas tradicionais. 77. Deve exibir o status de cada um dos troncos configurados 78. O sistema proposto deve ser capaz de configurar escritórios remotos para fazer chamadas entre escritórios como se fossem ramais IP. 79. Obter a lista telefônica do site remoto. Atendimento de chamadas 80. Deve ser possível programar diferentes planos de discagem para lidar com chamadas recebidas e efetuadas. 81. No caso de chamadas de entrada, deve ser possível configurar mapeamentos diretos (DIDs) para um ou vários ramais. 82. Para chamadas de saída, deve ser possível criar um plano de discagem que, dependendo dos dígitos selecionados, determine como o sistema irá canalizar aquela chamada. 83. Deve ter atendentes automáticos para atender as chamadas. 84. Cada atendedor automático deve ter opções e gravações diferentes. 85. Os ramais IP devem poder ser configurados para limitar chamadas internacionais ou de longa distância. 86. Apoiar a configuração de chamadas em conferência. 87. Suporte à configuração de discagem rápida 88. O sistema deve ser capaz de gravar chamadas recebidas e efetuadas sem a necessidade de qualquer software ou dispositivo adicional. 89. Suporte para configuração de filas de chamadas, podendo limitar o número de chamadas na fila e o tempo que a chamada permanecerá na fila. 90. Suporte a música em espera com possibilidade de upload de um arquivo de áudio para o sistema proposto. 91. Suporte para estacionar a chamada para poder colocá-la em espera e recuperá-la de outro ramal. Relatórios e registros 92. O sistema proposto deve armazenar em seu log todos os eventos relacionados ao sistema, como alterações na configuração, login e logout do administrador e os eventos relacionados às chamadas. 93. Deve ser possível selecionar o nível de gravidade do evento para determinar se ele está armazenado ou não. 94. O sistema proposto deve ser capaz de armazenar os logs em seu disco rígido ou utilizar um servidor Syslog. 95. Ser capaz de usar os logs como base do sistema de relatórios integrados. 96. Deve ser possível selecionar que tipo de logs serão armazenados. 97. Deve ter um perfil para configurar relatórios. 98. Deve possuir relatórios para detalhamento dos atendimentos e pode ser agendado para que o sistema os gere a cada determinado momento. 99. Os relatórios de chamadas devem ser enviados por e-mail. 100. O sistema proposto deve ter um relatório de cobrança de chamadas. 101. CDRs podem ser agendados e gerar um relatório em formato CSV. ESPECIFICAÇÕES TÉCNICAS----- Especificações de Hardware 1. A arquitetura da plataforma de comunicação corporativa deverá ser instalada em ambiente de virtualização compatível com VMware versão 6.0 ou superior fornecido pela Contratante. 2. O sistema deverá ser integrado à rede de dados corporativa da CONTRATANTE 3. Deve possuir no mínimo 02 vCPU 4. Deve possuir, no mínimo, 4GB de memória RAM 5. Deve possuir, no mínimo, 04 (quatro) interfaces de Rede RJ-45 10/100/1000 BASE-T 6. Deve possuir capacidade de armazenamento de até 8 TB. 7. Capacidade 8. Deve possuir, no mínimo, capacidade para suportar 24 (vinte e quatro) troncos VoIP 9. Deve possuir, no mínimo, capacidade para suportar 200 (duzentos) ramais IP 10. Deve possuir, no mínimo, capacidade para suportar até 36 (trinta e seis) chamadas simultaneamente. 11. Deve possuir, no mínimo, capacidade para suportar 10 (dez) chamadas de auto-atendimento. 12. Deve possuir, no mínimo, capacidade para suportar 10 (dez) Bridges de conferência. 13. Deve possuir, no mínimo, capacidade para suportar até 12 (doze) chamadas por Bridge de conferência. 14. Deve possuir, no mínimo, capacidade para suportar até 20 (vinte) agentes de Call Center.	
17	SISTEMA DE VOZ - TIPO II - VM CARACTERÍSTICAS GERAIS Administração do	474397



Sistema 1. O sistema proposto deve ter pelo menos dois métodos de configuração através de uma interface Web e através de uma linha de comando acessível através de um console serial, telnet ou SSH. 2. O equipamento proposto deve possuir um endereço IP padrão em uma de suas interfaces para poder iniciar a instalação e configuração diretamente na interface Web. 3. O sistema proposto deve ter um assistente de configuração para poder realizar os passos iniciais da configuração até a realização de chamadas telefônicas. 4. Deve ter uma página web para que os usuários possam gerenciar suas extensões incluindo as seguintes funcionalidades: 5. Verificação do correio de voz, incluindo reproduzir, excluir ou salvar mensagens de correio de voz 6. Usar o operador de console para processar chamadas da empresa. 7. Verificar o registro de chamadas para chamadas discadas, recebidas e não atendidas ou armazenar correios de voz 8. Revisar o diretório corporativo 9. Gerenciar chamadas 10. Configurar perfil de telefone 11. Personalizar arquivos de som. 12. Para acessar esta página da web, o usuário deve inserir seu número de ramal e um PIN na página. Monitoramento do Sistema 13. O sistema proposto deve ter um dashboard para verificar o estado geral do equipamento incluindo o número de série, o tempo de operação, a disponibilidade de recursos de memória, CPU e largura de banda de rede utilizada, a versão do sistema operacional, bem como um histórico de estatísticas de chamadas. 14. Esta Interface deve ser personalizável para poder selecionar as informações mais relevantes e até mesmo entrar na linha de comando por este meio. 15. O sistema de monitoramento dos equipamentos propostos deve permitir a visualização de chamadas de saída, chamadas em espera, chamadas em conferência, ramais, troncos, filas de chamadas, clientes DHCP e telefones não atribuídos. 16. Para chamadas ativas, o sistema deve mostrar em tempo real, incluindo os números que estão sendo chamados e de onde as chamadas estão sendo feitas, bem como os troncos que estão sendo usados naquele momento, o status da chamada e sua duração 17. Deve mostrar os detalhes das chamadas de conferência incluindo o nome da conferência, o número dos ramais na conferência e a duração da conferência. 18. Deve apresentar a informação de todos os ramais incluindo o estado, seu identificador, o número, o nome do usuário, o tipo de ramal e o tipo de telefone conectado. 19. Para o status dos troncos, o sistema deve mostrar em tempo real incluindo os nomes, endereços IP, tipo de tronco e se estiver conectado e cadastrado na operadora, o status deve mostrar se está em serviço, se está não disponível, se estiver em alarme ou se estiver desabilitado. 20. Exibir o status dos faxes. 21. O sistema deve ter um serviço de relatórios e entregá-los em HTML ou PDF 22. Deve ter um sistema de logs acessível diretamente da página web que deve permitir pesquisas com critérios personalizados e poder exportá-los para uma tabela. Configuração do sistema 23. O sistema proposto deve suportar IPv4 e IPv6 24. Deve suportar a criação de VLANs e a criação de interfaces redundantes combinando duas ou mais interfaces físicas para fornecer redundância. 25. Deve conter pelo menos 4 portas Ethernet 10/100/1000 BaseT. 26. Deve permitir a criação de rotas estáticas 27. Deve funcionar como servidor DHCP 28. Deve permitir a captura de pacotes e armazenar essas informações em um arquivo “.pcap” para análise posterior. 29. Suportar a criação de diferentes contas de administrador e poder limitar o acesso de endereços IP específicos. 30. A autenticação deve ser feita localmente ou por meio de um servidor LDAP 31. Suporte a diferentes perfis de administração, como contas de monitor, onde você só tem direitos de leitura do sistema 32. Suporta um esquema de alta disponibilidade com um dispositivo ativo e um dispositivo passivo, fazendo alterações no dispositivo ativo e replicando automaticamente a configuração no dispositivo passivo. 33. Selecione o fuso horário em que o equipamento vai funcionar bem como o uso de servidores NTP para garantir o horário dentro do equipamento. 34. Suporte a políticas de senha, como a escolha do número mínimo de caracteres solicitados na senha, bem como o uso de letras maiúsculas ou minúsculas e caracteres especiais. 35. Suporte SNMPv3 36. Configure pelo menos um servidor de correio para enviar mensagens de alerta do sistema. 37. Interface gráfica personalizável 38. Suportar uma pré-autorização para integrar o sistema através do



uso de certificados digitais para fazer uma conexão segura. Configuração do sistema telefônico 39. Seleção do país onde será colocado o equipamento proposto. 40. Suporte à configuração do número de emergência 41. Configuração de prefixos para atender chamadas externas, interurbanas e internacionais. 42. Configurando padrões para planos de discagem para ramais 43. Configuração de templates para envio de emails e relatórios. 44. Configuração SIP para a seleção das portas RTP, TCP e UDP a serem utilizadas 45. Suporte ao provisionamento automático da configuração SIP do telefone 46. Suporte para uso de diferentes arquivos de áudio para atendedores automáticos e música em espera. 47. Configuração de diferentes perfis para ramais que incluem diferentes serviços como seleção de codec para telefones. 48. Suporte a fax sobre IP 49. Suporte à modificação do identificador de chamadas e possibilidade de mapeá-lo para um grupo de ramais 50. Configuração de atendimento de chamadas dependendo do agendamento 51. Configuração remota de teclas programáveis em telefones SIP 52. Quando apenas a conectividade SIP está disponível, o sistema também pode ser instalado em uma instância virtual no vSphere, HyperV, KVM e XEN Server. 53. Você deve poder contar com um módulo para hotéis Configurações das extensões 54. Configuração remota de teclas programáveis em telefones SIP 55. Configuração de ramais IP locais e remotos onde o usuário discará apenas o número do ramal e o sistema proposto discará um número local ou celular. 56. O sistema proposto deve ser capaz de gerar automaticamente senhas e PINs para cada ramal ou ser definido pelo administrador. 57. Deve ter a facilidade de importar e exportar a lista de extensões para um arquivo no formato CSV 58. Reinicializar o telefone remotamente 59. Deve ser fácil aplicar a mesma alteração ou modificação para variar as extensões ao mesmo tempo. 60. O sistema proposto deve detectar o tipo de telefone IP que cada um dos ramais possui. 61. Deve ser possível selecionar um perfil SIP para cada um dos ramais IP. 62. Deve ser possível conceder diferentes privilégios aos usuários dos ramais IP. 63. Cada ramal IP deve ter uma caixa postal de voz e os telefones IP devem ter um LED que permaneça aceso para notificar o usuário de que há uma entrada em sua caixa postal. 64. O sistema deve ser capaz de auditar ramais para determinar se há senhas fracas. 65. Deve possuir um sistema que permita a localização de ramais repetidos, em conflito ou sem número. 66. Suportará a importação de uma lista de extensões de um arquivo CSV 67. Suporta o protocolo T38 para manipulação de Fax sobre VoIP. 68. Definir após quantas vezes o ramal toca para ser enviado ao correio de voz 69. Enviar um e-mail com a mensagem do correio de voz como anexo. 70. Deve ser possível configurar o gerenciamento de chamadas de acordo com o calendário e qual ação deve ser seguida se o ramal estiver ocupado, não atender ou estiver em modo “não perturbe”. 71. Deve ser possível criar grupos de ramais, para que uma chamada de entrada toque da mesma forma em todos os ramais pertencentes a este grupo ou faça-o sequencialmente onde tocará em cada ramal separadamente dentro do grupo. 72. O sistema proposto deve ter um sistema de anúncio (paging) 73. Adicionalmente, deve ser possível criar grupos de trabalho onde um usuário possa atender uma chamada que esteja tocando em outro ramal pertencente ao seu grupo. 74. Você deve ter uma caixa postal geral. 75. Apoiar a criação de ramais virtuais que não serão fixos em um único telefone IP. Configuração de tronco 76. O sistema deve suportar vários tipos de troncos como E1, troncos SIP e linhas analógicas tradicionais. 77. Deve exibir o status de cada um dos troncos configurados 78. O sistema proposto deve ser capaz de configurar escritórios remotos para fazer chamadas entre escritórios como se fossem ramais IP. 79. Obter a lista telefônica do site remoto. Atendimento de chamadas 80. Deve ser possível programar diferentes planos de discagem para lidar com chamadas recebidas e efetuadas. 81. No caso de chamadas de entrada, deve ser possível configurar mapeamentos diretos (DIDs) para um ou vários ramais. 82. Para chamadas de saída, deve ser possível criar um plano de discagem que, dependendo dos dígitos selecionados, determine como o sistema irá canalizar aquela chamada. 83. Deve ter atendentes automáticos para atender as chamadas. 84. Cada atendedor automático deve ter opções e gravações diferentes. 85. Os ramais IP devem poder ser configurados para limitar chamadas



	internacionais ou de longa distância. 86. Apoiar a configuração de chamadas em conferência. 87. Suporte à configuração de discagem rápida 88. O sistema deve ser capaz de gravar chamadas recebidas e efetuadas sem a necessidade de qualquer software ou dispositivo adicional. 89. Suporte para configuração de filas de chamadas, podendo limitar o número de chamadas na fila e o tempo que a chamada permanecerá na fila. 90. Suporte a música em espera com possibilidade de upload de um arquivo de áudio para o sistema proposto. 91. Suporte para estacionar a chamada para poder colocá-la em espera e recuperá-la de outro ramal. Relatórios e registros 92. O sistema proposto deve armazenar em seu log todos os eventos relacionados ao sistema, como alterações na configuração, login e logout do administrador e os eventos relacionados às chamadas. 93. Deve ser possível selecionar o nível de gravidade do evento para determinar se ele está armazenado ou não. 94. O sistema proposto deve ser capaz de armazenar os logs em seu disco rígido ou utilizar um servidor Syslog. 95. Ser capaz de usar os logs como base do sistema de relatórios integrados. 96. Deve ser possível selecionar que tipo de logs serão armazenados. 97. Deve ter um perfil para configurar relatórios. 98. Deve possuir relatórios para detalhamento dos atendimentos e pode ser agendado para que o sistema os gere a cada determinado momento. 99. Os relatórios de chamadas devem ser enviados por e-mail. 100. O sistema proposto deve ter um relatório de cobrança de chamadas. 101. CDRs podem ser agendados e gerar um relatório em formato CSV. ESPECIFICAÇÕES TÉCNICAS 1. A arquitetura da plataforma de comunicação corporativa deverá ser instalada em ambiente de virtualização compatível com VMware versão 6.0 ou superior fornecido pela Contratante. 2. O sistema deverá ser integrado à rede de dados corporativa da CONTRATANTE 3. Deve possuir no mínimo 01 vCPU 4. Deve possuir, no mínimo, 2GB de memória RAM 5. Deve possuir, no mínimo, 04 (quatro) interfaces de Rede RJ-45 10/100/1000 BASE-T 6. Deve possuir capacidade de armazenamento de até 8 TB. 7. Capacidade 8. Deve possuir, no mínimo, capacidade para suportar 16 (dezesesseis) troncos VoIP 9. Deve possuir, no mínimo, capacidade para suportar 100 (cem) ramais IP 10. Deve possuir, no mínimo, capacidade para suportar até 30 (trinta) chamadas simultaneamente. 11. Deve possuir, no mínimo, capacidade para suportar 10 (dez) chamadas de auto-atendimento. 12. Deve possuir, no mínimo, capacidade para suportar 08 (oito) Bridges de conferência. 13. Deve possuir, no mínimo, capacidade para suportar até 12 (doze) chamadas por Bridge de conferência. 14. Deve possuir, no mínimo, capacidade para suportar até 10 (dez) agentes de Call Center.	
18	SISTEMA DE VOZ GATEWAY - TIPO I APPLIANCE 1. Equipamento do tipo appliance, ou seja, equipamento e software do mesmo fabricante. Não serão aceitos computadores ou equipamentos baseados em computadores; 2. Os Gateways de voz devem fazer parte do sistema de comunicação corporativa, serão os equipamentos controlados pelo servidor principal de telefonia IP e exclusivamente utilizados para conectividade dos seguintes elementos: 2.1. Interfaces para suportar os protocolos PRI T1, PRI E1 e R2 em configurações de porta única e dupla. 2.2. Interfaces para entroncamento GSM com o SMP e o SME (Conversão SIP/GSM). 3. Deve possuir funcionalidade de operar como central IP com capacidade de registro e gerenciamento local para situações de emergência caso haja problemas na conectividade com a solução de comunicação central, suprimindo no mínimo as seguintes funcionalidades: registro dos telefones, chamadas entre os ramais registrados neste gateway, chamadas de/e para RTPC, colocar chamada em espera, captura, correio de voz (pela RTPC), transferência e geração de bilhetes local (CDR); 4. Deve entrar e sair deste modo de "emergência" (perda de conexão com a solução de comunicação central) automaticamente, sem intervenção humana; 5. Deve implementar, no mínimo, os Codecs de voz G711 e G729; 6. Deve possuir conectividade com a rede IP através de porta RJ-45 10/100/1000 (Gigabit Ethernet); 7. Deve possuir porta de console para gerenciamento local do equipamento; 8. Deve possuir entregue com pelo menos 2 (duas) interfaces E1; 9. Deve implementar IPv4 e IPv6; 10. Deve ser baseado no protocolo IP, com implementação do protocolo SIP	474397



	(RFC3261); 11. Deve implementar o protocolo cRTP; 12. Deve implementar Qualidade de Serviço (QoS), utilizando DiffServ (CoS), IP Precedence (ToS) ou Differentiated Services Code Point (DSCP); 13. Deve ser compatível para instalação em racks padrão 19". Deverá vir acompanhado de kits de fixação, cabos, acessórios e demais materiais necessários à sua instalação, configuração e operação; 14. Deve implementar buffer dinâmico e programável para controle de jitter; 15. Deve implementar cancelamento de eco, segundo o padrão G.165 ou G.168; 16. Deverá se comunicar com o sistema central via protocolo SIP; 17. Deverá possuir áudio seguro, com SRTP, onde todas as chamadas são criptografadas para máxima segurança; 18. As configurações devem ser armazenadas em memória tipo não volátil; 19. Deve suportar transmissão de fax, segundo padrão T.38; 20. Deverá permitir múltiplos usuários para administração, com níveis de acesso distintos; 21. Deve implementar criptografia para tráfego de sinalização e de voz além da criptografia IPSEC solicitada para tráfego entre os gateways e com os aparelhos telefônicos, esta criptografia não deverá ser perdida quando estiver em modo de emergência (perda de conexão com a solução de comunicação central); 22. Deve permitir a execução local de música em espera; 23. Deve implementar SNMP com criptografia; 24. Fonte de alimentação interna que opere de 110V a 220V automaticamente; 25. Deve ser garantida atualização de software/firmware do equipamento pelo período de garantia sem custos para este órgão; 26. A empresa deve possuir, após a assinatura do contrato, pelo menos 1 (um) profissional com certificação técnica emitida pelo fabricante do equipamento ofertado, capaz de prestar suporte de primeiro nível aos produtos em garantia, e escalar o suporte ao fabricante conforme necessidade; 27. Garantia de 36 (trinta e seis) meses;	
19	SISTEMA DE VOZ GATEWAY - TIPO II APPLIANCE 1. Equipamento do tipo appliance, ou seja, equipamento e software do mesmo fabricante. Não serão aceitos computadores ou equipamentos baseados em computadores; 2. Os Gateways de voz devem fazer parte do sistema de comunicação corporativa, serão os equipamentos controlados pelo servidor principal de telefonia IP e exclusivamente utilizados para conectividade dos seguintes elementos: 2.1. Interfaces para suportar os protocolos PRI T1, PRI E1 e R2 em configurações de porta única e dupla. 2.2. Interfaces para entroncamento GSM com o SMP e o SME (Conversão SIP/GSM). 3. Deve possuir funcionalidade de operar como central IP com capacidade de registro e gerenciamento local para situações de emergência caso haja problemas na conectividade com a solução de comunicação central, suprimindo no mínimo as seguintes funcionalidades: registro dos telefones, chamadas entre os ramais registrados neste gateway, chamadas de/e para RTPC, colocar chamada em espera, captura, correio de voz (pela RTPC), transferência e geração de bilhetes local (CDR); 4. Deve entrar e sair deste modo de "emergência" (perda de conexão com a solução de comunicação central) automaticamente, sem intervenção humana; 5. Deve implementar, no mínimo, os Codecs de voz G711 e G729; 6. Deve possuir conectividade com a rede IP através de porta RJ-45 10/100/1000 (Gigabit Ethernet); 7. Deve possuir porta de console para gerenciamento local do equipamento; 8. Deve possuir entregue com pelo menos 1 (uma) interfaces E1; 9. Deve implementar IPv4 e IPv6; 10. Deve ser baseado no protocolo IP, com implementação do protocolo SIP (RFC3261); 11. Deve implementar o protocolo cRTP; 12. Deve implementar Qualidade de Serviço (QoS), utilizando DiffServ (CoS), IP Precedence (ToS) ou Differentiated Services Code Point (DSCP); 13. Deve ser compatível para instalação em racks padrão 19". Deverá vir acompanhado de kits de fixação, cabos, acessórios e demais materiais necessários à sua instalação, configuração e operação; 14. Deve implementar buffer dinâmico e programável para controle de jitter; 15. Deve implementar cancelamento de eco, segundo o padrão G.165 ou G.168; 16. Deverá se comunicar com o sistema central via protocolo SIP; 17. Deverá possuir áudio seguro, com SRTP, onde todas as chamadas são criptografadas para máxima segurança; 18. As configurações devem ser armazenadas em memória tipo não volátil; 19. Deve suportar transmissão de fax, segundo padrão T.38; 20. Deverá permitir múltiplos	474397



	usuários para administração, com níveis de acesso distintos; 21. Deve implementar criptografia para tráfego de sinalização e de voz além da criptografia IPSEC solicitada para tráfego entre os gateways e com os aparelhos telefônicos, esta criptografia não deverá ser perdida quando estiver em modo de emergência (perda de conexão com a solução de comunicação central); 22. Deve permitir a execução local de música em espera; 23. Deve implementar SNMP com criptografia; 24. Fonte de alimentação interna que opere de 110V a 220V automaticamente; 25. Deve ser garantida atualização de software/firmware do equipamento pelo período de garantia sem custos para este órgão; 26. A empresa deve possuir, após a assinatura do contrato, pelo menos 1 (um) profissional com certificação técnica emitida pelo fabricante do equipamento ofertado, capaz de prestar suporte de primeiro nível aos produtos em garantia, e escalar o suporte ao fabricante conforme necessidade; 27. Garantia de 36 (trinta e seis) meses;	
20	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 1 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de virtual, ou seja, cada elemento deverá ser composto software do respectivo fabricante; 3. Deve suportar compatibilidade com Hypervisors abaixo: a. VMware ESXi v5.5 / v6.0 / v6.5 / v6.7 / v7.0 b. VMware NSX-T* v2.3 / v2.4 / v2.5 c. Microsoft Hyper-V Server 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 d. Microsoft AzureStack e. Citrix Xen XenServer v5.6 sp2, v6.0, v6.2 and later f. Open source Xen v3.4.3, v4.1 and later g. KVM qemu 0.12.1 & libvirt 0.10.2 and later for Red Hat Enterprise Linux / CentOS 6.4 and later / Ubuntu 16.04 LTS (generic kernel) h. KVM qemu 2.3.1 for SuSE Linux Enterprise Server 12 SP1 LTSS i. Nutanix AHV (AOS 5.10, Prism Central 5.10) j. Cisco Cloud Services Platform 2100 k. Cisco ENCS (NFVIS 3.12.3) 4. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 5. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 6. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 7. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 8. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 9. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 10. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 11. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 12. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 19. A solução deve, através da interface gráfica, ser capaz de aplicar	27456



ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 96 (novecentos e seis) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo, todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 36. A solução deverá ser capaz de encaminhar 4.5 Gbps de tráfego encapsulado via VPN IPSec; 37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 38. A VPN IPSec deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 39. A VPN IPSec deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 42. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 45. A



Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 47. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 48. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 57. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 58. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 59. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 60. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 61. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 62. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 63. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 64. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 65. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 66. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 67. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em



5GHz através do recurso conhecido como Band Steering; 68. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 69. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 70. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 71. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 72. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 73. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 74. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 75. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 76. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 77. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: a) Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); b) Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; c) ASLEAP; d) Null Probe Response or Null SSID Probe Response; e) Long Duration; f) Ataques contra Wireless Bridges; g) Weak WEP; h) Invalid MAC OUI. 78. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 79. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 80. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 81. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 82. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 83. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 84. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 85. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 86. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 87. A solução deverá suportar Single-Sign-On (SSO); 88. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 89. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 90. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 91. A solução deve implementar recurso



para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 92. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 93. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 94. A solução deve permitir a configuração do captive portal com endereço IPv6; 95. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 96. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 97. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 98. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 99. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 100. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 101. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 102. A solução deverá ser capaz de inspecionar 3.5 Gbps de tráfego SSL; 103. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 104. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 105. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo continuar; 106. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 107. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 108. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 109. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 110. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 111. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 112. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 113. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 114. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 115. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 116. A solução deverá ser capaz de tratar 4 (quatro) Gbps de tráfego por meio do filtro de aplicações; 117. A solução deve registrar todos os logs de eventos



com bloqueios e liberações das aplicações que foram acessadas na rede; 118. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 119. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 120. A solução deverá permitir a criação manual de novos padrões de aplicações; 121. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 122. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 123. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 124. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 125. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 126. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 127. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 128. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 129. A solução deverá ser capaz de tratar 20 (vinte) Gbps de tráfego por meio das regras de firewall stateful; 130. A solução deverá ser capaz de suportar 270.000 (duzentos e setenta) novas sessões por segundo; 131. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 132. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 133. A solução deverá suportar PBR – Policy Based Routing; 134. A solução deverá suportar roteamento multicast; 135. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 136. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323; 137. A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 138. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 139. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 140. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 141. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 142. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 143. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 144. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 145. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 146. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 147. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 148. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual



	agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 149. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 150. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 151. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 152. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 153. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 154. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 155. A solução deverá suportar Netflow ou sFlow; 156. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 157. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 158. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 159. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 160. A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap; 161. A solução deve possuir ferramentas de diagnósticos e debug 162. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 163. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 164. A solução deve suportar comunicação com elementos externos através de REST API; 165. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 166. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 167. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 168. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.	
21	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 2 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de virtual, ou seja, cada elemento deverá ser composto software do respectivo fabricante; 3. Deve suportar compatibilidade com Hypervisors abaixo: a) VMware ESXi v5.5 / v6.0 / v6.5 / v6.7 / v7.0 b) VMware NSX-T* v2.3 / v2.4 / v2.5 c) Microsoft Hyper-V Server 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 d) Microsoft AzureStack e) Citrix Xen XenServer v5.6 sp2, v6.0, v6.2 and later f) Open source Xen v3.4.3, v4.1 and later g) KVM qemu 0.12.1 & libvirt 0.10.2 and later for Red Hat Enterprise Linux / CentOS 6.4 and later / Ubuntu 16.04 LTS (generic kernel) h) KVM qemu 2.3.1 for SuSE Linux Enterprise Server 12 SP1 LTSS i) Nutanix AHV (AOS 5.10, Prism Central 5.10) j) Cisco Cloud Services Platform 2100 k) Cisco ENCS (NFVIS 3.12.3) 4. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 5. Quaisquer licenças e/ou softwares necessários para plena	27456



execução de todas as características descritas neste termo de referência deverão ser fornecidos; 6. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 7. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 8. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 9. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 10. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 11. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 12. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 96 (novecentos e seis) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 31. A solução deve permitir habilitar o recurso



de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo, todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 36. A solução deverá ser capaz de encaminhar 9.4 Gbps de tráfego encapsulado via VPN IPSec; 37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 38. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 39. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 42. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 47. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 48. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações



distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 67. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); b. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; c. ASLEAP; d. Null Probe Response or Null SSID Probe Response; e. Long Duration; f.



Ataques contra Wireless Bridges; g. Weak WEP; h. Invalid MAC OUI. 75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 84. A solução deverá suportar Single-Sign-On (SSO); 85. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 91. A solução deve permitir a configuração do captive portal com endereço IPv6; 92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 99. A solução deverá ser capaz de inspecionar 6.2 Gbps de tráfego SSL; 100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de



continuar sua navegação ao mesmo site através de um botão do tipo continuar; 103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 113. A solução deverá ser capaz de tratar 6 (seis) Gbps de tráfego por meio do filtro de aplicações; 114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 116. A solução deverá permitir a criação manual de novos padrões de aplicações; 117. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 118. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 119. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 120. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 121. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 122. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 123. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 124. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 125. A solução deverá ser capaz de tratar 27 (vinte e sete) Gbps de tráfego por meio das regras de firewall stateful; 126. A solução deverá ser capaz de suportar 450.000 (quatrocentos e cinquenta) novas sessões por segundo; 127. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 128. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 129. A solução deverá suportar PBR – Policy Based Routing; 130. A solução deverá suportar roteamento multicast; 131. A solução deverá possuir mecanismo de anti-spoofing tipo



RPF (Reverse Path Forward) ou similar; 132. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323; 133. A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 134. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 135. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 136. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 65. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 147. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 148. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 149. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 150. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 151. A solução deverá suportar Netflow ou sFlow; 152. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 153. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 154. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 155. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 156. A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap; 157. A solução deve possuir ferramentas de diagnósticos e debug 158. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 159. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 160. A solução deve suportar comunicação com elementos externos através de REST API; 161. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 162. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei



	14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a. da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 163. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 164. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.	
22	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 3 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 6 (seis) interfaces 1000Base-T e 2 (duas) interfaces 1 Gigabit Ethernet padrão 1GBase-LX para permitir a conexão com a rede; 4. Deve possuir interface console com conector RJ-45 ou USB para gerenciamento local; 5. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar os cabos de alimentação; 6. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 7. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 8. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 9. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 10. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 11. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 12. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 13. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 14. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 15. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 768 (setecentos e sessenta e oito) portas de switch ou um total de 16 (dezesesseis) switches; 16. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 17. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 18. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 19. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 21. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 22. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 23. A solução deve, através da interface gráfica, ser capaz de realizar	150100



configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 24. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 25. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 26. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 96 (novecentos e seis) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 27. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 28. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 29. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 30. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 31. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 32. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 33. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 34. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 35. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 36. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 37. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 38. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 39. A solução deverá ser capaz de encaminhar 6.5 Gbps de tráfego encapsulado via VPN IPSec; 40. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 41. A VPN IPSec deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 42. A VPN IPSec deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 43. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 44. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 45. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 46. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 47. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 48. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 49. A solução deve implementar recursos que



possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 50. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 51. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 52. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 53. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 54. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 55. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 56. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 57. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 58. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 59. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 60. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 61. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 62. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 63. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 64. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 65. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 66. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 67. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 68. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 69. A



solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 70. A solução deve permitir a configuração dos parâmetros BLE (Blueooth Low Energy) nos pontos de acesso; 71. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 72. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 73. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 74. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 75. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 76. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 77. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: 77.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); 77.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; 77.3. ASLEAP; 77.4. Null Probe Response or Null SSID Probe Response; 77.5. Long Duration; 77.6. Ataques contra Wireless Bridges; 77.7. Weak WEP; 77.8. Invalid MAC OUI. 78. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 79. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 80. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 81. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 82. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 83. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 84. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 85. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 86. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 87. A solução deverá suportar Single-Sign-On (SSO); 88. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 89. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 90. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 91. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o



acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 92. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 93. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 94. A solução deve permitir a configuração do captive portal com endereço IPv6; 95. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 96. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 97. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 98. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 99. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 100. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 101. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 102. A solução deverá ser capaz de inspecionar 950 (novecentos e cinquenta) Mbps de tráfego SSL; 103. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 104. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 105. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 106. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 107. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 108. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 109. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 110. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 111. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 112. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 113. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 114. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 115. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 116. A solução deverá ser capaz de tratar 1 (um) Gbps de tráfego por meio do filtro de aplicações; 117. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 118. A base de reconhecimento de aplicações através de DPI deve identificar, no



mínimo, 2000 (duas mil) aplicações; 119. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 120. A solução deverá permitir a criação manual de novos padrões de aplicações; 121. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 122. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 123. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 124. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 125. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 126. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 127. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 128. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 129. A solução deverá ser capaz de tratar 7 (sete) Gbps de tráfego por meio das regras de firewall stateful; 130. A solução deverá ser capaz de suportar 1.500.000 (um milhão e quinhentos mil) de sessões simultâneas/concorrentes e 45.000 (quarenta e cinco) novas sessões por segundo; 131. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 132. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 133. A solução deverá suportar PBR – Policy Based Routing; 134. A solução deverá suportar roteamento multicast; 135. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 136. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323; 137. A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 138. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 139. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 140. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 141. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 142. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 143. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 144. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 145. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 146. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 147. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 148. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento



	utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 149. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 150. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 151. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 152. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 153. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 154. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 155. A solução deverá suportar Netflow ou sFlow; 156. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 157. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 158. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 159. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 160. A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap; 161. A solução deve possuir ferramentas de diagnósticos e debug 162. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 163. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 164. A solução deve suportar comunicação com elementos externos através de REST API; 165. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 166. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 167. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 168. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.	
23	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 4 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 16 (dezesesseis) interfaces 1 Gigabit Ethernet padrão 1000Base-T ou 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Caso sejam ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX; 4. Deve possuir interface console com conector RJ-45 ou USB para gerenciamento local; 5. Cada appliance físico deve possuir fonte de alimentação redundante com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 6. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 7. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de	150100



referência deverão ser fornecidos; 8. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 9. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 10. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 11. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 12. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 13. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 14. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 15. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 288 (duzentos e oitenta e oito) portas de switch ou um total de 64 (sessenta e quatro) switches; 16. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 17. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 18. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 19. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 21. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 22. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 23. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 24. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 25. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 26. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 128 (cento e vinte e oito) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 27. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 28. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 29. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 30. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 31. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 32. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 33. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de



encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 34. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 35. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 36. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 37. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 38. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPsec e SSL com elementos externos; 39. A solução deverá ser capaz de encaminhar 13 Gbps de tráfego encapsulado via VPN IPsec; 40. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 41. A VPN IPsec deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 42. A VPN IPsec deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 43. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 44. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPsec; 45. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 46. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 47. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 48. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 49. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 50. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 51. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 52. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 53. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 54. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 55. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 56. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 57. A solução deve



permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 58. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 59. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 60. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 61. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 62. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 63. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 64. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 65. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 66. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 67. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 68. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 69. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 70. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 71. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 72. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 73. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 74. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 75. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 76. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 77. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: 77.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); 77.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; 77.3.



ASLEAP; 77.4. Null Probe Response or Null SSID Probe Response; 77.5. Long Duration; 77.6. Ataques contra Wireless Bridges; 77.7. Weak WEP; 77.8. Invalid MAC OUI. 78. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 79. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 80. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 81. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 82. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 83. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 84. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 85. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 86. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 87. A solução deverá suportar SingleSign-On (SSO); 88. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 89. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 90. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 91. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 92. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 93. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 94. A solução deve permitir a configuração do captive portal com endereço IPv6; 95. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 96. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 97. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 98. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 99. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 100. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 101. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 102. A solução deverá ser capaz de inspecionar 500 (quinhentos) Mbps de tráfego SSL; 103. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 104. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 105. Ao bloquear o acesso de um



usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 106. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 107. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 108. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 109. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 110. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 111. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 112. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 113. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 114. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 115. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 116. A solução deverá ser capaz de tratar 3.5 Gbps de tráfego por meio do filtro de aplicações; 117. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 118. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 119. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 120. A solução deverá permitir a criação manual de novos padrões de aplicações; 121. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 122. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 123. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 124. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 125. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 126. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 127. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 128. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 129. A solução deverá ser capaz de tratar 11 Gbps de tráfego por meio das regras de firewall stateful; 130. A solução deverá ser capaz de suportar 3.000.000 (três milhões) de sessões simultâneas/concorrentes e 280.000 (duzentos e oitenta) novas sessões por segundo; 131. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 132. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 133. A solução deverá suportar PBR – Policy



Based Routing; 133. A solução deverá suportar roteamento multicast; 134. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 135. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323; 136. A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 137. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 138. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 139. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 140. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 141. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 142. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 143. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 144. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 145. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 146. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 147. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 148. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 149. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 150. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 151. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 152. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 153. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 154. A solução deverá suportar Netflow ou sFlow; 155. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 156. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 157. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 158. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 159. A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap; 160. A solução deve possuir ferramentas de diagnósticos e debug 161. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 162. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 163. A solução deve suportar comunicação com elementos externos através de REST API; 164. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 165. Garantia de 36 (trinta



	e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 166. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 167. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 168. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.	
24	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 5 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 8 (oito) interfaces 1 Gigabit Ethernet padrão 1000Base-T e 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Adicionalmente devem ser fornecidos 2 (dois) transceivers SFP+ conforme padrão 10GBase-SR; 4. Deve possuir interface console com conector RJ-45 ou USB para gerenciamento local; 5. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 6. Deve suportar a instalação de fonte de alimentação redundante; 7. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 8. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 9. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 10. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 11. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 12. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 13. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 14. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 15. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 16. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 4608 (quatro mil e seiscentos e oito) portas de switch ou um total de 96 (noventa e seis) switches; 17. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 18. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 19. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 20. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 21. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para	150100



autenticação 802.1X nas interfaces dos switches; 22. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 23. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 24. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 25. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 26. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 27. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de, no mínimo, quinhentos (quinhentos) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 28. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 29. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 30. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 31. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 32. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 33. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 34. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 35. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 36. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 37. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 38. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 39. A solução deverá, ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 40. A solução deverá ser capaz de encaminhar 20 Gbps de tráfego encapsulado via VPN IPSec; 41. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 42. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 43. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 44. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 45. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 46. A



solução deverá ser capaz de atuar como um cliente de VPN SSL; 47. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 48. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 49. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 50. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 51. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 52. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 53. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 54. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 55. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 56. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 57. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 58. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 59. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 60. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 61. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 62. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 63. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 64. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 65. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 66. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 67. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 68. Para garantir uma



melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 69. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 70. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 71. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 72. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 73. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 74. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 75. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 76. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 77. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 78. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); b. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; c. ASLEAP; d. Null Probe Response or Null SSID Probe Response; e. Long Duration; f. Ataques contra Wireless Bridges; g. Weak WEP; h. Invalid MAC OUI. 79. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 80. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 81. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 82. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 83. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 84. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 85. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 86. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 87. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 88. A solução deverá suportar SingleSign-On (SSO); 89. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 90. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores



RADIUS; 91. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 92. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 93. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 94. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 95. A solução deve permitir a configuração do captive portal com endereço IPv6; 96. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 97. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 98. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 99. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 100. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 101. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 102. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 103. A solução deverá ser capaz de inspecionar 8 Gbps de tráfego SSL; 104. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 105. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 106. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 107. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 109. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 110. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios préconfigurados em sua base de conhecimento; 111. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 112. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 113. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 114. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 115. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 116. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise



mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 117. A solução deverá ser capaz de tratar 9.5 Gbps de tráfego por meio do filtro de aplicações; 118. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 119. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 120. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 121. A solução deverá permitir a criação manual de novos padrões de aplicações; 122. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 123. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 124. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 125. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 126. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 127. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 128. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 129. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 130. A solução deverá ser capaz de tratar 27 Gbps de tráfego por meio das regras de firewall stateful; 131. A solução deverá ser capaz de suportar 8.000.000 (oito milhões) de sessões simultâneas/concorrentes e 450.000 (quatrocentos e cinquenta mil) novas sessões por segundo; 132. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 133. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 134. A solução deverá suportar PBR – Policy Based Routing; 135. A solução deverá suportar roteamento multicast; 136. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 137. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323; 138. A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 139. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 140. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 141. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 142. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 143. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPsec, para que componham a interface virtual agregada; 144. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 145. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 146. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPsec; 147. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos:



	Ping, HTTP, TCP-Echo e UDP-Echo. 148. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 149. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 150. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 151. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 152. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 153. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 154. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 155. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 156. A solução deverá suportar Netflow ou sFlow; 157. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 158. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 159. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 160. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 161. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap; 162. A solução deve possuir ferramentas de diagnósticos e debug 163. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 164. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 165. A solução deve suportar comunicação com elementos externos através de REST API; 166. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 167. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a. da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 168. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 169. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.	
25	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 6 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 16 (dezesesseis) interfaces 1 Gigabit Ethernet padrão 1000Base-T, 4 (quatro) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede, 2 (duas) interfaces 40 Gigabit Ethernet padrão 40GBase-LR e 2 (duas) interfaces 25 Gigabit Ethernet padrão 25GBase-LR. Caso sejam ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX; 4. Deve possuir interface console com	150100



conector RJ-45 ou USB para gerenciamento local; 5. Cada appliance físico deve suportar fonte de alimentação redundante (Hot Swappable) com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 6. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 7. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 8. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 9. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 10. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 11. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 12. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 13. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 14. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 15. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 9.408 (nove mil e quatrocentos e oito mil) portas de switch ou um total de 196 (cento e noventa e seis) switches; 16. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 17. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 18. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 19. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 21. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 22. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 23. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 24. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 25. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 26. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 2000 (dois mil) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 27. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 28. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 29. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 30. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 31. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição



adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 32. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 33. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 34. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 35. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 36. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 37. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 38. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 39. A solução deverá ser capaz de encaminhar 48 Gbps de tráfego encapsulado via VPN IPSec; 40. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 41. A VPN IPSEC deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 42. A VPN IPSEC deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 43. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 44. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 45. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 46. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 47. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 48. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 49. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 50. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 51. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 52. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 53. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 54. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface



LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 55. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 56. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 57. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 58. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 59. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 60. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 61. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 62. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 63. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 64. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 65. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 66. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 67. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 68. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 69. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 70. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 71. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 72. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 73. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 74. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 75. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 76. A solução deve permitir a configuração de redes Mesh entre



os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 3. 77. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); b. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; c. ASLEAP; d. Null Probe Response or Null SSID Probe Response; e. Long Duration; f. Ataques contra Wireless Bridges; g. Weak WEP; h. Invalid MAC OUI. 78. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 79. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 80. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 81. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 82. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 83. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 84. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 85. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 86. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 87. A solução deverá suportar SingleSign-On (SSO); 88. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 89. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 90. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 91. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 92. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 93. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 94. A solução deve permitir a configuração do captive portal com endereço IPv6; 95. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 96. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 97. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 98. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 99. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 100. A solução deverá permitir a operação tanto em modo proxy explícito



quanto em modo proxy transparente; 101. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 102. A solução deverá ser capaz de inspecionar 8.4 Gbps de tráfego SSL; 103. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 104. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 105. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo continuar; 106. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 107. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 108. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 109. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios préconfigurados em sua base de conhecimento; 110. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 111. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 112. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 113. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 114. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 115. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 116. A solução deverá ser capaz de tratar 9.8 Gbps de tráfego por meio do filtro de aplicações; 117. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 118. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 119. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 120. A solução deverá permitir a criação manual de novos padrões de aplicações; 121. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 122. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 123. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 124. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 125. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 126. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 127. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 128. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 129. A solução deverá ser capaz de tratar 27(vinte e sete) Gbps de tráfego por meio das



regras de firewall stateful; 130. A solução deverá ser capaz de suportar 8.000.000 (oito milhões) de sessões simultâneas/concorrentes e 500.000 (quinhentos mil) novas sessões por segundo; 131. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 132. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 133. A solução deverá suportar PBR – Policy Based Routing; 134. A solução deverá suportar roteamento multicast; 135. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 136. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323; 137. A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 138. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 139. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 140. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 141. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 142. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPsec, para que componham a interface virtual agregada; 143. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 144. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 145. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPsec; 146. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 147. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 148. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 149. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 150. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 151. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 152. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 153. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 154. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 155. A solução deverá suportar Netflow ou sFlow; 156. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 157. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 158. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 159. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 160. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap; 161. A



	solução deve possuir ferramentas de diagnósticos e debug 162. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 163. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 164. A solução deve suportar comunicação com elementos externos através de REST API; 165. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 166. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a. da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 170. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 171. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.	
26	SWITCH TIPO 1 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA Características Mínimas: 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a autonegociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 5. Deve possuir 1 (uma) interface USB; 6. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 32.000 endereços; 9. Deve operar com latência igual ou inferior à 1us (microsegundo); 10. 8. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 11. 9. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 12. 10. Deve suportar a comutação de Jumbo Frames; 13. 11. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 14. 12. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 15. 10.13. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 16. 14. Deve implementar serviço de DHCP Relay; 17. 15. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (um mil) entradas na tabela; 18. 16. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 19. 17. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 20. 18. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 21. 19. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente nível 2; 22. 20. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units)	463274



caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido umBPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 23. 21. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 24. 22. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 25. 23. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 26. 24. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 27. 25. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 28. 26. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 29. 27. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF; 28. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 32. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 35. Deve suportar MAC Authentication Bypass (MAB); 36. Deve implementar RADIUS CoA (Change of Authorization); 37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 38. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 40. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 43. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 44. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 45. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 47. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 50. Deve suportar o protocolo



	HTTPS para configuração e administração remota através de interface web; 51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 52. Deve permitir ser gerenciado através de IPv6; 53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 55. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 58. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 59. Deverá suportar ser configurado e monitorado através de REST API; 60. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 61. Deve suportar temperatura de operação de até 45° Celsius; 62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 64. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 65. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 66. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 67. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 68. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 69. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 70. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.	
27	SWITCH TIPO 3 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA Características Mínimas: 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W a serem alocados em qualquer uma das portas 1000Base-T; 5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 6. Deve possuir 1 (uma) interface USB; 7. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo); 8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 9. Deve possuir	463274



tabela MAC com suporte a 32.000 endereços; 10. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 11. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 12. Deve suportar a comutação de Jumbo Frames; 13. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 14. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 15. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 16. Deve implementar serviço de DHCP Relay; 17. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (quinhentas) entradas na tabela; 18. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 19. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 20. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 21. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente nível 2; 22. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 23. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 24. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 25. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 26. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 27. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 28. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 29. Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF; 30. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 31. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 32. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 33. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 34. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 35. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 36. Deve suportar MAC Authentication Bypass (MAB); 37. Deve implementar RADIUS CoA (Change of Authorization); 38. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 39. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 40. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 41. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X.



Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 42. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 43. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 44. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 45. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 46. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 47. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 48. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 49. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 50. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 51. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 52. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 53. Deve permitir ser gerenciado através de IPv6; 54. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 55. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 56. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 57. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 58. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 59. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 60. Deverá suportar ser configurado e monitorado através de REST API; 61. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 62. Deve suportar temperatura de operação de até 45° Celsius; 63. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 64. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 65. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 66. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 67. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 68. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 69. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a. da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 70. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 71. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.



28	SWITCH TIPO 4 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA Características Mínimas: 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10000Base-SR operando em 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 5. Deve possuir 1 (uma) interface USB; 6. Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 32.000 endereços; 9. Deve operar com latência igual ou inferior à 1us (microsegundo); 10. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 11. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 12. Deve suportar a comutação de Jumbo Frames; 13. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 14. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 15. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 16. Deve implementar serviço de DHCP Relay; 17. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela; 18. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 19. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 20. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 21. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente nível 2; 22. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 23. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 24. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 25. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 26. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 27. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 28. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 29. Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF; 30. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 31. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o	463274



protocolo ARP; 30. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 31. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 32. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 33. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 34. Deve suportar MAC Authentication Bypass (MAB); 35. Deve implementar RADIUS CoA (Change of Authorization); 36. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 37. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 38. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 39. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 40. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 41. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 42. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 43. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 44. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 45. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 46. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 47. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 48. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 49. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 50. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 51. Deve permitir ser gerenciado através de IPv6; 52. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 53. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 54. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 55. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 56. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 57. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 58. Deverá suportar ser configurado e monitorado através de REST API; 59. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 60. Deve suportar temperatura de operação de até 45° Celsius; 61. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 62. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 63. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 64. O switch deverá ser compatível e ser gerenciado pela solução de



	gerenciamento de redes e segurança deste processo; 65. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 66. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 67. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).	
29	SWITCH TIPO 5 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA Características Mínimas: 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10000Base-SR operando em 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W; 5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 1. Deve possuir 1 (uma) interface USB; 6. Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 32.000 endereços; 2. Deve operar com latência igual ou inferior à 1us (microsegundo); 9. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 10. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 11. Deve suportar a comutação de Jumbo Frames; 12. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 13. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 14. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 15. Deve implementar serviço de DHCP Relay; 16. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela; 17. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 18. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 19. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 20. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente nível 2; 21. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 22. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 23. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 24. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o	448242



switch deve descartar os pacotes ou aplicar rate limit; 25. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 26. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 27. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 28. Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF; 29. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 32. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 35. Deve suportar MAC Authentication Bypass (MAB); 36. Deve implementar RADIUS CoA (Change of Authorization); 37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 38. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 40. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 43. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 44. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 45. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 47. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 50. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 52. Deve permitir ser gerenciado através de IPv6; 53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 55. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 57. Deverá ser capaz de executar testes nas interfaces para identificar



	problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 58. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 59. Deverá suportar ser configurado e monitorado através de REST API; 60. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 61. Deve suportar temperatura de operação de até 45° Celsius; 62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 64. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 65. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 66. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 67. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 68. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 69. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 70. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.	
30	TARIFADOR - TELEFONIA VOiP 1. O sistema de tarifação deverá operar em sistema operacional Windows 2016 Server ou superior. 2. O Sistema Automático de Tarifação e Bilhetagem deverá armazenar suas informações em banco de dados relacional que deve ser entregue junto com a solução; 3. Funcionalidade WEB: acesso disponível, a partir de qualquer ponto da rede, às consultas gráficas e relatórios via browser; 4. O Sistema deverá seguir a filosofia baseada no controle por USUÁRIO, os quais poderão acessar os relatórios e/ou gráficos a partir de qualquer estação (windows ou linux) na rede Intranet, via Web-Browser, através do uso de senha de autenticação, segundo o PERFIL que será estabelecido pela CONTRATANTE para os usuários. Para maior segurança das estações e servidor não será permitida a instalação de aplicativos ou componentes necessários para emular o ambiente web, como Active-X, por exemplo. O sistema deverá permitir a associação do usuário a um ou mais ramais e /ou uma ou mais senhas. 5. O sistema deverá permitir a criação de perfis diferenciados de acesso, com permissões 5.1. por usuário. 6. Tarifação on-line: o Sistema Automático de Tarifação e Bilhetagem deverá atribuir valor monetário imediatamente, ao receber as informações dos bilhetes telefônicos, conforme as tabelas das operadoras. 7. Retarificação automática: a retarificação deverá ser automática e imediata, ou seja, recalculada imediatamente a partir do momento em que uma alteração diretamente relacionada com o custo da ligação ocorra. 8. Relatórios via Intranet: o Sistema Automático de Tarifação e Bilhetagem deverá possibilitar o acesso a qualquer informação via browser. 9. Os relatórios deverão permitir a geração nos formatos HTML, TXT, Excel, Word e PDF. 10. Agendamento de Tarefas: O sistema deverá permitir o agendamento de emissão de 10.1. relatórios periódicos, exportação dos dados das ligações, fechamento da tarifação, ou seja, no momento definido o próprio sistema se incumbirá de executar a atividade previamente agendada. 11. Cópia de segurança compacta e programável: o sistema deverá ter uma rotina interna de backup automática, cuja periodicidade pode ser programada. 12. O sistema deverá controlar o histórico de utilização de cada ramal por usuário. 13. O sistema deverá efetuar a coleta dos bilhetes gerados pelos PABXs e/ou	27456



	equipamentos IP e os tarifar e processar de forma centralizada. 14. O sistema deverá possuir um recurso de Controle de Gastos, onde poderão ser definidos valores de gastos por usuário e/ou departamentos e o sistema deverá enviar notificações periódicas indicando se o usuário está dentro ou fora de sua meta (budget), seja essa notificação por uma porcentagem de consumo ou por uma tendência de consumo. 15. O sistema deverá possuir um recurso que permita a monitoração do andamento do 15.1. sistema. Esta janela deverá alertar o usuário de eventuais falhas em alguma aplicação ou serviço da solução. Paralelamente, a solução de gerenciamento de falhas deverá enviar alertas por email ou visuais para os responsáveis, por cada evento defeituoso. O próprio recurso de monitoramento deverá tentar restabelecer os serviços que caírem. 16. A coleta dos bilhetes deverá ser efetuada através da rede, de forma automática, com a geração de alarmes quando da falha na coleta dos bilhetes, com envio de mensagem eletrônica. 17. O sistema deverá possuir no mínimo os seguintes relatórios: Relatórios flexíveis, com 17.1. informações de identificação de usuários, ramais (origem e destino), tempo e data de cada chamada, centro de custo, Grupos de Usuários, custo da ligação, relatórios de tráfego (tráfego de entrada ou de saída, tráfego de por rota ou por ramal), etc.; 18. O Sistema deverá permitir a observação de dados de tráfego, de tal forma que possibilite a 18.1. medição e registros diários, relatório de tráfego na Hora e Dia de Maior Movimento, em forma de relatórios específicos para análise de custos, ocupação de troncos e ramais, duração de chamadas e avaliação do nível de serviço em períodos pré-determinados. 19. O Sistema deverá permitir a simulação de Tráfego em cima das informações fornecidas pela observação citada anteriormente e indicar o número ideal de Troncos e/ou links necessários para correto dimensionamento da central. 20. O Sistema deverá permitir a geração de Gráficos comparativos entre os centros de custo do órgão, mostrando a evolução dos últimos 13 meses. Essa evolução deverá ser apresentada 20.1. por: Custo das ligações, Quantidade de ligações e Duração das ligações e também Usuário por Plano de Serviço e Centro de Custo por Planos de Serviço. 21. O Sistema deverá possuir recurso para permitir que o próprio usuário valide as ligações particulares via Web Browser e que as mesmas sejam cadastradas automaticamente no banco de dados. 22. O sistema deve incluir a atualização automática mensal via Internet das tarifas, prefixos, localidades e novos planos praticados e publicados pelas operadoras e homologadas pela ANATEL. 23. Tabela de tarifas flexível e configurável. 24. Deve estar dimensionado e licenciado para 1100 ramais; 25. Deve ser compatível com o "Controlador de Chamadas" fornecido neste grupo; 26. Garantia de 36 (trinta e seis) meses;	
31	TERMINAL DE COMUNICAÇÃO - TIPO I 1. Terminal de comunicação IP composto por telefone, monofone e acessórios para pleno funcionamento; 2. O conjunto deve ser nativo no protocolo IP. Não serão aceitos equipamentos híbridos com telefonia analógica ou que necessitem de adaptadores externos para o funcionamento; 3. Deve possuir display com resolução mínima de 320x240 pontos. Este display deve prover informações de data e hora, correio de voz, ícone de chamadas perdidas, detalhes da chamada durante uma ligação, histórico de chamadas efetuadas e recebidas e configurações do aparelho; 4. Deve permitir a alimentação de energia através de PoE, com consumo máximo de 4W para redução do consumo de energia; 5. Deve implementar protocolo SIP nativamente; 6. Deve possuir duas interfaces Ethernet RJ-45 10/100, sendo uma para conexão a LAN e outro para ligar um computador. Deve funcionar como "Ethernet Switch", permitindo ligar a rede de um computador no telefone compartilhando entre o PC e o telefone um único cabo e uma única porta no switch da rede; 7. Deve suportar LLDP; 8. Deve suportar o protocolo TFTP; 9. Deve suportar DSCP; 10. Deve possuir uma interface RJ-22 para conexão do monofone, de forma que seja fácil a sua substituição em caso de defeito do monofone ou do próprio cabo; 11. Deve permitir a fixação do aparelho na parede. Caso tal recurso não seja nativo no hardware do aparelho, os acessórios para fixação em parede devem ser fornecidos; 12. Deve suportar o idioma Português (Brasil); 13. Deve permitir duas chamadas simultâneas; 14. Deve suportar música em espera; 15. Deve possuir	453584



	indicador de mensagem em espera no correio de voz; 16. Deve suportar conferência e captura de chamadas; 17. Deve possuir no mínimo 4 teclas físicas de atalhos específicas para as funcionalidades mais utilizadas: colocar chamada em espera, rediscar, mudo, volume (mais/menos); 18. Deve possuir a funcionalidade de "viva-voz" (microfone e alto-falante), sendo esta funcionalidade ativada/desativada por uma tecla física específica para este fim. Deve ser possível desabilitar o "viva-voz" no menu de configurações; 19. Deve possuir teclado numérico físico; 20. Deve ser compatível com os codecs G711 e G729a; 21. Deve possuir cliente DHCP, permitindo configuração automática de endereçamento IP; 22. Deve suportar também a configuração manual de endereçamento IP; 23. Deve possuir a funcionalidade de "Não pertube", com o objetivo de não ser notificado de se uma ligação esta entrando. 24. Deve ser gerenciável através de interface web; 25. Deve ser fornecido em cor neutra (preta ou cinza); 26. Garantia de 36 (trinta e seis) meses;	
32	TRANSCEIVER 1000BASE-LX (2023) 1. Transceiver SFP para conexão de fibras ópticas monomodo; 2. Deve ser compatível com o padrão 1000BASE-X para fibras ópticas de até 10 quilômetros; 3. Deve possuir conector LC duplex; 4. Velocidade de 1GBe; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).	150812
33	TRANSCEIVER 10GBASE-LR (2023) 1. Transceiver SFP para conexão de fibras ópticas monomodo; 2. Deve ser compatível com o padrão 10GBASE-LR para fibras ópticas de até 10 quilômetros; 3. Deve possuir conector LC duplex; 4. Velocidade de 10GBe; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).	150812
34	TRANSCEIVER 1000BASE-SX (2023) 1. Transceiver SFP para conexão de fibras ópticas multimodo; 2. Deve ser compatível com o padrão 1000BASE-SX para fibras ópticas de até 400 metros; 3. Deve possuir conector LC duplex; 4. Velocidade de 1GBe; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).	150812
35	TRANSCEIVER 10GBASE-SR 1. Transceiver SFP para conexão de fibras ópticas multimodo; 2. Deve ser compatível com o padrão 10GBASE-SR para fibras ópticas de até 300 metros; 3. Deve possuir conector LC duplex; 4. Velocidade de 10GBe; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).	150812

Fonte CATSER/CATMAT: <https://catalogo.compras.gov.br/cnbs-web/busca>

3 – JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

- 3.1.1.** O Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina – IFSC – possui 23 unidades, sendo 22 Câmpus (unidades de ensino) e 01 Reitoria (unidade administrativa).
- 3.1.2.** No momento que este Termo de Referência foi elaborado, está sendo executado o Projeto IFSC Conecta através dos processos 23292.010214/2021-24 e 23292.010041/2022-36 disponíveis em <https://sipac.ifsc.edu.br/public/listaEditais.do?tipo=2&aba=p-editais-atas&buscaTodas=true&acao=544>.
- 3.1.3.** Para a conclusão do projeto deverá ser implantada controladoras de rede sem fio com funcionalidades de firewall em 12 unidades do IFSC (do total de 23); para 06 unidades será necessário a aquisição de pontos de acesso, switches e injetores PoE.
- 3.1.4.** Essa infraestrutura permitirá o gerenciamento local da rede sem fio e a gestão de segurança através da implementação de firewall. Esta estrutura permitirá a aquisição da solução de telefonia VoIP, que será atrelada ao firewall e permitirá um ambiente completo e seguro.
- 3.1.5. ESTA CONTRATAÇÃO RESULTARÁ NA FORMAÇÃO DE ATA DE REGISTRO DE PREÇOS COM POSSIBILIDADE DE ADESAO conforme Decreto 7.892/2013:**

Art.3º O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:

IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	Objetivos Estratégicos
OE.06	PETIC - Garantir infraestrutura adequada para manter e suportar as soluções de TIC

ALINHAMENTO AO PDTIC 2021/2022		
ID	Ação do PDTIC	Meta do PDTIC
ID-03	Ação 5 - Manter e expandir a infraestrutura de TIC. Substituição da solução de rede sem fio.	62,5% do quantitativo estimado.

ALINHAMENTO AO PAC 2022	
Item	Descrição
8216 a 8217	Aquisição de Pontos de Acesso.

3.3. Estimativa da demanda

- 3.3.1.** As estimativas serão realizadas de acordo com a necessidade de finalização da solução.

3.4. Parcelamento da Solução de TIC

- 3.4.1.** A solução será agrupada em lote único conforme disposto no inciso I, do artigo 15 da lei 8.666/93 (Art. 15. As compras, sempre que possível, deverão: I - atender ao princípio da padronização, que imponha compatibilidade de especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas;)
- 3.4.2.** Os equipamentos, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante dos demais equipamentos deste processo.

3.5.Resultados e Benefícios a Serem Alcançados

- 3.5.1.Ampliação da cobertura de rede sem fio;
- 3.5.2.Ampliação do acesso dos estudantes a rede sem fio;
- 3.5.3.Ampliação da segurança dos dados institucionais;
- 3.5.4.Substituição da telefonia convencional por telefonia VoIP;
- 3.5.5.Integração de soluções de segurança.

4 – ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

- 4.1.1.Aquisição de equipamentos e serviços que permitam a finalização do Projeto Conecta IFSC criando um ambiente seguro para a gestão dos dados institucionais e utilização da rede sem fio por todos os usuários (alunos, professores e servidores).

4.2. Requisitos de Capacitação

- 4.2.1. Repasse de conhecimento (hands on).

4.3.Requisitos Legais

- 4.3.1.A contratação deverá estar em conformidade com a legislação que rege os processos de contratação (Lei 8.666/93 e Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019 com suas alterações e regulamentações).

4.4. Requisitos de Manutenção e Suporte Técnico

- 4.4.1.Todos os equipamentos deverão ser ofertados com garantia de três anos com reposição de componentes ou fornecimento de novos equipamentos em acordo com a legislação vigente. O envio de peças/equipamentos de reposição deve acontecer em até 3 dias úteis.
- 4.4.2.A CONTRATADA deverá disponibilizar suporte técnico em nível corporativo com, no mínimo, as seguintes características:
 - 4.4.2.1.a) Manter central de atendimento para abertura de chamados no regime 24x7 para atendimento dos chamados de suporte técnico. A central deverá ser acionada por meio de ligação gratuita ou abertura de chamados pela internet. O atendimento deverá ser realizado em língua portuguesa.

4.5. Requisitos Temporais

- 4.5.1.Os equipamentos deverão ser entregues em até 120 dias a partir do envio da Autorização de Fornecimento e empenho. Os serviços deverão ser executados em até 30 dias a partir do envio da Autorização de Fornecimento e empenho.
- 4.5.2.Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos.
- 4.5.3.Os prazos definidos neste Termo de Referência deverão ser estritamente observados sob pena da aplicação de sanções conforme previsto na seção 7.4 deste Termo de Referência.

4.6.Requisitos de Segurança e Privacidade

- 4.6.1.Não se aplica, pois os serviços a serem instalados/configurados não envolvem o tratamento de dados pessoais.

4.7.Requisitos de Segurança da Informação

- 4.7.1.A execução dos serviços deverá ocorrer sob a supervisão de técnicos de TIC da contratante.

4.8. Requisitos de Sustentabilidade

4.8.1.A CONTRATADA deverá cumprir os seguintes requisitos de uso racional de recursos:

- 4.8.1.1.a) deverá entregar os documentos solicitados na forma digital, com vistas a evitar ou reduzir o uso de papel e impressão, em atendimento ao Art. 9º da Política Nacional de Resíduos Sólidos (Lei nº 12.305, de 2 de agosto de 2010);
- 4.8.1.1.2.b) as configurações de hardware e software deverão ser realizadas visando alto desempenho com a utilização racional de energia, evitando-se a sobrecarga de equipamentos ou dispositivos elétricos e eletrônicos;

4.9. Requisitos de Segurança dos Dados e Informações

- 4.9.1.a) É vedado o acesso da CONTRATADA aos dados hospedados na infraestrutura da CONTRATANTE, sem prévia e formal autorização desta;
- 4.9.2.b) A CONTRATADA deverá criar uma política de atualização de versão de software, indicando sua criticidade e acordar junto à CONTRATANTE qual a melhor data para ser aplicada.
- 4.9.3.c) A CONTRATADA deverá assinar Termo de Compromisso de Manutenção de Sigilo (ANEXO III), resguardando que os recursos, dados e informações de propriedade da CONTRATANTE, e quaisquer outros, repassados por força do objeto desta licitação e do contrato, constituem informação privilegiada e possuem caráter de confidencialidade.

4.10. Requisitos de Arquitetura Tecnológica

- 4.10.1.A solução deverá atender as exigências de tecnologia detalhadas no Quadro de Especificações Mínimas.

4.11. Requisitos de Implantação

- 4.11.1.A CONTRATADA em conjunto com a CONTRATANTE deverá estabelecer as diretrizes de implantação em reuniões de *Kickoff*, além daquelas previstas no Quadro de Especificações Mínimas.

4.12.. Requisitos de Garantia e Assistência Técnica

- 4.12.1.A CONTRATADA deverá reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos nos recursos e serviços contratados.

4.13. Requisitos de Experiência Profissional

- 4.13.1.A CONTRATADA deverá disponibilizar pessoal técnico qualificado para a execução dos serviços de instalação/configuração da solução contratada.

4.14. Requisitos de Capacidade Técnica

- 4.14.1.A CONTRATADA deverá fornecer atestados de capacidade técnica que comprovem o fornecimento da solução a ser contratada, de acordo com o edital.

4.15. Requisitos de Compatibilidade Técnica

- 4.15.1.A solução deverá ser do mesmo fabricante da solução implantada na infraestrutura da CONTRATANTE.

5 – RESPONSABILIDADES

5.1. Deveres e responsabilidades da CONTRATANTE

- 5.1.1. Encaminhar formalmente a demanda por meio de Autorização de Fornecimento de Bens e Serviços, de acordo com os critérios estabelecidos neste Termo de Referência;
- 5.1.2. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- 5.1.3. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
- 5.1.4. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
- 5.1.5. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

- 5.1.6. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável;
- 5.1.7. Verificar, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e, posterior, recebimento definitivo;
- 5.1.8. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;
- 5.1.9. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;
- 5.1.10. Pagar à Contratada o valor resultante da aquisição de bens e prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência;
- 5.1.11. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da contratada, no que couber, em conformidade com o item 6 do Anexo XI da IN SEGES/MP n. 5/2017.
- 5.1.12. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento das obrigações pela Contratada;

5.2. Deveres e responsabilidades da CONTRATADA

- 5.2.1. Efetuar a entrega dos bens em perfeitas condições, conforme especificações, prazo e local constantes no subitem 6.1.1 deste Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;
- 5.2.2. Os bens deverão ser entregues acompanhados de manual do usuário, com uma versão em português ou inglês, e da relação da rede de assistência técnica autorizada;
- 5.2.3. As licenças de software e extensões de garantia deverão ser entregues conforme especificação por e-mail ou através de download em portal do fabricante, **em até 15 (quinze) dias corridos** a partir da emissão de Autorização de Fornecimento.
- 5.2.4. Os bens importados deverão ser entregues **em até 120 dias corridos** a partir da emissão da Autorização de Fornecimento pelo IFSC, podendo ser prorrogados por mais **30 dias corridos** a partir de solicitação formal, desde que comprovada a não responsabilidade da empresa vencedora por este atraso.
- 5.2.5. Os serviços de instalação/configuração dos bens fornecidos poderão ser executados remotamente em comum acordo com a CONTRATANTE.
- 5.2.6. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);
- 5.2.7. Substituir, reparar ou corrigir, às suas expensas, no prazo de 05 (cinco) dias úteis, o objeto com avarias ou defeitos;
- 5.2.8. Materiais entregues em desacordo com o Edital e não retirados em até 05 (cinco) dias úteis após comunicação formal do IFSC, serão descartados. Este prazo poderá ser prorrogado, desde que formalizado, justificado e aceito pelo IFSC. Esta prorrogação somente será aceita caso seja feita dentro do prazo da notificação.
- 5.2.9. Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;
- 5.2.10. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
- 5.2.11. Responder pelas perdas e danos causados por seus empregados, durante o fornecimento do material, ainda que involuntariamente, às instalações do prédio, máquinas, equipamentos e demais bens do IFSC, substituindo os referidos bens por outros semelhantes em prazo que lhe será expressamente combinado pela Contratante.
- 5.2.12. Todos os itens constantes da nota de empenho devem ser entregues no mesmo momento, nas condições e locais conforme consta deste Anexo (não será aceita a entrega parcelada dos itens).
- 5.2.13. Retirar a nota de empenho em até 03 (três) dias úteis, após a convocação.
- 5.2.14. Cumprir o prazo de garantia de acordo com o especificado em cada item neste Termo de Referência ou conforme o prazo estabelecido na proposta de preços, caso este seja maior que o mínimo estabelecido.
- 5.2.15. Os problemas apresentados durante o prazo de garantia devem ser solucionados em até 30 (trinta) dias corridos.
- 5.2.16. Arcar com todos os custos para cumprimento da garantia, inclusive no caso de necessidade de transporte (técnicos ou equipamentos).
- 5.2.17. A Contratada assume o compromisso de receber as Autorizações de Fornecimento (AF's) e Empenhos pelo e-mail institucional informado na **DECLARAÇÃO DE CONCORDÂNCIA À ATA DE REGISTRO DE PREÇOS** concordando que não sendo confirmado o recebimento do e-mail, o IFSC considerará como recebido, iniciando a contagem do prazo de entrega. Assumindo o compromisso de avisar o IFSC quando houver mudança do e-mail.

5.2.18. Manter atualizado seu cadastro no órgão através do envio do documento preenchido referente ao Anexo V deste edital sempre que houver mudanças em seus dados cadastrais.

5.3. Deveres e Responsabilidades do Órgão Gerenciador da Ata de Registro de Preços

- 5.3.1. Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;
- 5.3.2. Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;
- 5.3.3. Definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:
- 5.3.3.1. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e
- 5.3.3.2. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável.
- 5.3.4. Definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:
- 5.3.4.1. a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;
- 5.3.5. As regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a realização de Prova de Conceito, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica;

6 – MODELO DE EXECUÇÃO DO CONTRATO

6.1. Rotinas de Execução

6.1.1. Realização da Reunião Inicial

- 6.1.1.1. Para o início da implementação dos serviços contratados deverá ser realizada reunião de *kickoff* estabelecendo todos os passos necessários para a execução do serviço.

6.1.2. Procedimentos para encaminhamento e controle de solicitações

- 6.1.2.1. O IFSC encaminhará à empresa vencedora a Autorização de Fornecimento de Bens e Serviços e Nota de Empenho.

6.1.3. Forma de execução e acompanhamento dos serviços

- 6.1.3.1. Os serviços serão fornecidos pela contratada e gerenciados pela contratante pela natureza do mesmo.

6.1.4. Prazos, horários de fornecimento de bens ou prestação dos serviços

- 6.1.4.1. Será estabelecido o horário comercial para o tratamento das demandas específicas do serviço contratado.

6.1.5. Local de entrega, quando aplicável:

CÂMPUS	ENDEREÇO
Câmpus Araranguá	Av. XV de Novembro, s/nº – Bairro Aeroporto – CEP: 88900-000 – Araranguá – SC – Fone: (48) 3311-5000; e-mail: compras.ararangua@ifsc.edu.br .
Câmpus Caçador	Av. Fahdo Thomé, 3000, Champagnat – Caçador – SC – 89503-550, Fone: (49) 3561-5700; e-mail: compras.cdr@ifsc.edu.br .
Câmpus Canoinhas	AV. Expedicionários, 2150 – Bairro Campo do Água Verde – CEP 89460-000 – Canoinhas SC: Fone: (47) 3627-4500; e-mail: compras.canoinhas@ifsc.edu.br .
Cerfead	Rua Duarte Schutel, 99 – Centro – Florianópolis/SC – CEP 88015-640; e-mail: compras@ifsc.edu.br ; Fone: (48) 3131-8816.
Câmpus Chapecó	Av. Nereu Ramos, 3450 D – Bairro Seminário – Chapecó/SC CEP: 89813-000 – Fone: (49) 3313-1240; e-mail: compras.chapeco@ifsc.edu.br .
Câmpus Criciúma	SC 443, km 01, nº. 845 – Bairro Vila Rica – Criciúma – SC – CEP 88813-600; Esquina com Rua Antônio Daré; Fone: (48) 3462-5000; e-mail: compras.criciuma@ifsc.edu.br .



Câmpus Florianópolis	Av. Mauro Ramos, 950 – Centro – Florianópolis/SC. CEP: 88020-300 – Almojarifado, Fone: (48) 3211-6000; e-mail: compras.fpolis@ifsc.edu.br .
Câmpus Florianópolis-Continente	Rua 14 de Julho, 150 – Coqueiros – Florianópolis/SC – CEP: 88.075-010; Fone (48) 3877-8400; e-mail: compras.continente@ifsc.edu.br .
Câmpus Garopaba	Rua Maria Aparecida Barbosa, nº 153, Loteamento Vila de Campo – Bairro Campo Duna – Garopaba – SC – CEP 88495-000; Fone (48) 3254-7330; e-mail: compras.garopaba@ifsc.edu.br .
Câmpus Gaspar	Rua Adriano Kormann, 510 – Bairro Bela Vista – Gaspar – SC; CEP 89110-971; Fone: (47) 3318-3700; e-mail: compras.gaspar@ifsc.edu.br .
Câmpus Itajaí	Av. Vereador Abrahão João Francisco, 3899, Bairro Ressacada – Itajaí – SC; CEP 88307-303; Fone: (47) 3390-1200; e-mail: compras.itj@ifsc.edu.br .
Câmpus Jaraguá do Sul – Rau	Rua dos Imigrantes, nº 445 – Bairro Rau – 89254-430 – Jaraguá do Sul; Fone: (47) 3276-9600; e-mail: compras.rau@ifsc.edu.br
Câmpus Jaraguá do Sul	Av. Getúlio Vargas, nº 830 – Centro – Jaraguá do Sul – CEP: 89251-000, Fone: (47) 3276-8700; e-mail: compras.jar@ifsc.edu.br .
Câmpus Joinville	Rua Pavão, 1337 – Loteamento Novo Horizonte – Bairro Costa e Silva, Joinville/SC – CEP: 89220-618 – Fone: (47) 3431-5600; e-mail: compras.joinville@ifsc.edu.br .
Câmpus Lages	Rua Heitor Villa-Lobos, s/n – Bairro São Francisco – Lages – CEP 88506-400, Fone: (49) 3221-4200; e-mail: compras.lages@ifsc.edu.br .
Câmpus Palhoça-Bílingue	Rua João Bernardino da Rosa – Bairro Cidade Universitária Pedra Branca – Palhoça – SC – CEP 88137-010; Fone: (48) 3341-9700; e-mail: compras.phb@ifsc.edu.br .
Câmpus São Carlos	Rua Aloísio Stoffell, 1271 – Jardim Alvorada – São Carlos/SC – CEP 89885-000; Fone: (49) 3325-4149; e-mail: compras.sca@ifsc.edu.br
Câmpus São José	R. José Lino Kretzer, 608 – Bairro Praia Comprida – CEP: 88103-310 São José – SC; Fones: (48) 3381-2800 e Fax: 3381-2812; e-mail: compras.sje@ifsc.edu.br
Câmpus São Lourenço do Oeste	Rua Aderbal Ramos da Silva, 496-514 – Bairro Progresso. São Lourenço do Oeste – CEP 89990 000; Fones: (049) 3344-8495; e-mail: compras.slo@ifsc.edu.br .
Câmpus São Miguel do Oeste	Rua 22 de Abril, s/n – Bairro São Luiz – São Miguel do Oeste – SC 89900-970, Fone: (49)3631-0400; e-mail: compras.smo@ifsc.edu.br .
Câmpus Tubarão	BR 101 Sul, km 336 – Fone: (48) 3301-9101; E-mail: compras.tub@ifsc.edu.br

Câmpus Urupema	Estrada do Senadinho s/n – Centro – Urupema – SC – 88625-970, Fone: (49) 3236-3100; e-mail: compras.urupema@ifsc.edu.br .
Câmpus Xanxerê	Rua Euclides Hack, 1603 – Bairro Veneza – Xanxerê – SC – 89820-000; Fone: (49) 3441-7900; e-mail: compras.xxe@ifsc.edu.br .
Reitoria	Av. 14 de julho 150 – Coqueiros – Florianópolis – SC – CEP:88075-010 – Fones: (48) 3877-9000; e-mail: compras@ifsc.edu.br .

6.1.6.Documentação mínima exigida

6.1.6.1.Para habilitação da licitante a documentação está especificada no edital e neste Termo de Referência.

6.1.6.2.Para a definição correta dos materiais deve ser observado o Quadro de Especificações Mínimas, que é o documento de referência.

6.1.7.Formas de transferência de conhecimento

6.1.7.1. Repasse de conhecimento (hands on).

6.2.Mecanismos formais de comunicação

6.2.1.O canal de comunicação entre IFSC e a empresa será o e-mail srp@ifsc.edu.br e almoxarifado.reitoria@ifsc.edu.br ;

6.2.2.Para formalizar as solicitações será utilizado a Autorização de Fornecimento de Bens e Serviços e Nota de Empenho.

6.3.Manutenção de Sigilo e Normas de Segurança

6.3.1.A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.3.2.O **Termo de Compromisso e Manutenção de Sigilo**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e **Termo de Ciência**, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos ANEXOS III e IV.

7 – MODELO DE GESTÃO DO CONTRATO

O fornecimento da solução será mediante o envio de Autorização de Fornecimento de Bens e Serviços e Nota de Empenho

7.1.Critérios de Aceitação

7.1.1. Os bens serão recebidos provisoriamente no momento de sua entrega, por servidor(a) do IFSC devidamente identificado, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

7.1.2. Os bens serão recebidos provisoriamente no prazo de 20 (vinte) dias, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

7.1.3. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 (quinze) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.1.4. Os bens serão recebidos definitivamente no prazo de 10 (dez) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado.

7.1.5.. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

7.1.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

7.1.7. A contratada se obriga a entregar todo o material, no mesmo momento, na quantidade informada na Autorização de Fornecimento (AF). Somente poderá ser aceita a entrega parcial, nas hipóteses abaixo, sob pena de devolução de todo

material, no caso do empenho/AF não estar completa:

- 7.1.7.1. O material só poderá ser entregue parcialmente, se a licitante encaminhar justificativa, solicitando o cancelamento dos itens pendentes juntamente ao material, para ser avaliada pela Administração e posterior aplicação de penalidades;
- 7.1.7.2. A Administração poderá solicitar a antecipação da entrega de parte dos materiais constantes da Autorização de Fornecimento, somente se a licitante conseguir atender ao pedido.

8 – Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

8.1. Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a Contratada que:

- 8.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
- 8.1.2. ensejar o retardamento da execução do objeto;
- 8.1.3. falhar ou fraudar na execução do contrato;
- 8.1.4. comportar-se de modo inidôneo;
- 8.1.5. cometer fraude fiscal;

8.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

- 8.2.1. **Advertência**, por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;
- 8.2.2. multas (que deverão ser recolhidas em favor do Instituto Federal de Educação, Ciências e Tecnologia de Santa Catarina, a ser preenchido de acordo com instruções fornecidas pela Contratante):
 - 8.2.2.1. de 1% (um por cento) sobre o valor total do somatório dos itens entregues com atraso (AF), por dia de atraso na entrega do material, limitados a 10% (dez por cento) do mesmo valor.
 - 8.2.2.2. de 10% (dez por cento) sobre o valor total da Autorização de Fornecimento (AF), por infração a qualquer cláusula ou condição do Edital, não especificada na alínea “a” deste inciso, aplicada em dobro na reincidência.
 - 8.2.2.3. de 10% (dez por cento) sobre o valor total da Proposta de preços vencedora, no caso de recusa injustificada da licitante adjudicatária em assinar a Ata de Registro de Preço ou deixar de apresentar os documentos exigidos, nos prazos e condições estabelecidas neste Edital.
 - 8.2.2.4. de 10% (dez por cento) sobre o valor total da Proposta de preço, no caso de rescisão do contrato por ato unilateral da administração, motivado por culpa da Contratada, garantida prévia defesa, independente das demais sanções cabíveis;
 - 8.2.2.5. de 10% (dez por cento) sobre o valor total do somatório dos itens entregues em desacordo, por apresentação de marca e/ou modelo que não estão de acordo com a especificação do edital e apresentada na proposta de preço da licitante;
 - 8.2.2.6. de 10% (dez por cento) do valor total do somatório dos itens entregues em desacordo com o Edital e a proposta de preços aceita na sessão do pregão;
 - 8.2.2.7. de 0,5% (cinco décimos por cento) ao dia sobre o valor adjudicado, no caso de não-substituição do material no prazo determinado no Termo de Referência, caso não estaria de acordo com a especificação exigida em Edital, limitada a incidência a 10 (dez) dias úteis. Após o décimo dia e a critério da Administração, poderá ocorrer a não-aceitação do material e/ou a sua substituição, de forma a configurar, nessa hipótese inexecução parcial da obrigação assumida;
 - 8.2.2.8. de 10% (dez por cento) sobre o valor total da Ata de Registro de Preços, no caso de cancelamento integral da ata por ato unilateral da administração, motivada por culpa da Contratada ou a pedido da mesma;
 - 8.2.2.9. Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;
 - 8.2.2.10. Impedimento de licitar e contratar com órgãos e entidades da União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;
- 8.3. A sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 8.2 deste Termo de Referência.
- 8.4. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;
- 8.5. As sanções previstas nos subitens acima poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.
- 8.6. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:
 - 8.6.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;
 - 8.6.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;
 - 8.6.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.
- 8.7. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.
- 8.8. As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.
- 8.9. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 05 (cinco) dias úteis, a contar da data do recebimento da comunicação enviada pela autoridade competente.
- 8.10. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.
- 8.11. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o

- caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.
- 8.12. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.
- 8.13. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.
- 8.14. As penalidades serão obrigatoriamente registradas no SICAF.

9 – Do Pagamento e Reajuste

9.1. Forma de pagamento

- 9.1.1. O Pagamento será feito de acordo com o consumo mensal (pagamento por Gigabytes/mês);
- 9.1.2. O pagamento deverá ser efetuado integral até o 15º (décimo quinto) dia útil após o aceite definitivo do material, em sua totalidade, e atesto da Nota Fiscal ou Documento de Cobrança, através de ordem bancária, para crédito em banco, com o código da agência e o número da conta-corrente que forem indicados pelo contratado.
- 9.1.3. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.
- 9.1.4. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.
- 9.1.5. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.
- 9.1.6. Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.
- 9.1.7. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.
- 9.1.8. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
- 9.1.9. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.
- 9.1.10. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.
- 9.1.11. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.
- 9.1.12. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.
- 9.1.13. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.
- 9.1.14. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.
- 9.1.15. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade,

segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

9.1.16. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

9.1.17. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

9.1.18. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

$EM = I \times N \times VP$, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$I = (TX)$

$I = \frac{(6 / 100)}{365}$

$I = 0,00016438$

TX = Percentual da taxa anual = 6%

9.1.19. A Nota fiscal/fatura ou documento de cobrança deverá ser sempre emitida com o CNPJ do Câmpus requisitante, conforme descrição abaixo:

CÂMPUS	CNPJ
Araranguá	11.402.887/0008-37
Caçador	11.402.887/0018-09
Canoinhas	11.402.887/0012-13
Chapecó	11.402.887/0007-56
Continente	11.402.887/0004-03
Criciúma	11.402.887/0009-18
Florianópolis	11.402.887/0002-41
Garopaba	11.402.887/0021-04
Gaspar	11.402.887/0010-51
Jaraguá do Sul - Rau	11.402.887/0019-90
Itajaí	11.402.887/0013-02
Jaraguá do Sul	11.402.887/0005-94



Joinville	11.402.887/0006-75
Lages	11.402.887/0011-32
Palhoça Bilíngue	11.402.887/0015-66
Reitoria	11.402.887/0001-60
São José	11.402.887/0003-22
São Miguel do Oeste	11.402.887/0014-85
Tubarão	11.402.887/0020-23
Urupema	11.402.887/0016-47
Xanxerê	11.402.887/0017-28

9.1.19.1. Para o Câmpus Avançado de São Lourenço do Oeste, a Nota Fiscal deverá ser emitida no CNPJ da Reitoria, sendo os materiais entregues no respectivo Câmpus.

10 – Reajuste

- 10.1.1.1. Os preços são fixos e irrevogáveis no prazo de um ano contado da data limite para a apresentação das propostas.
- 10.1.1.2. Dentro do prazo de vigência da Ata de Registro de Preços e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o intervalo de um ano, aplicando-se o Índice de Custos de Tecnologia da Informação – ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA.
- 10.1.1.3. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.
- 10.1.1.4. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.
- 10.1.1.5. Caso o índice estabelecido para reajuste venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.
- 10.1.1.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.
- 10.1.1.6.1. O reajuste será realizado por apostilamento.

11 – ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

Item	Descrição	Unidade	Quant	Preço Unit. (R\$)	Valor Total (R\$)
LOTE/GRUPO 1: Solução de Gerenciamento de Rede, Telefonia e Segurança					
1	INJETOR POE – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA	UNIDADE	80	1.307,74	104.619,20
2	PONTO DE ACESSO INDOOR	UNIDADE	90	8.839,36	795.542,40
3	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE REDE E SEGURANÇA	LICENÇA	2	246.688,18	493.376,36



4	LICENÇAS PARA TELEFONE - SOFTFONE	LICENÇA	400	327,67	131.068,00
5	PONTO DE ACESSO OUTDOOR	UNIDADE	20	13.128,20	262.564,00
6	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 1	SERVIÇO	10	16.786,03	167.860,30
7	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 2	SERVIÇO	4	25.899,76	103.599,04
8	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 3	SERVIÇO	15	4.413,66	66.204,90
9	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 4	SERVIÇO	5	6.693,41	33.467,05
10	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 5	SERVIÇO	2	18.297,83	36.595,66
11	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 6	SERVIÇO	2	57.209,14	114.418,28
12	SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE REDES E SEGURANÇA	SERVIÇO	2	15.936,70	31.873,40
13	SERVIÇO DE INSTALAÇÃO/CONFIGURAÇÃO - TELEFONIA TIPO 1	SERVIÇO	2	23.493,59	46.987,18
14	SERVIÇO DE INSTALAÇÃO/CONFIGURAÇÃO - TELEFONIA TIPO 2	SERVIÇO	10	13.038,54	130.385,40
15	SERVIÇO TÉCNICO PARA SITE SURVEY	SERVIÇO	5	22.740,72	113.703,60
16	SISTEMA DE VOZ - TIPO I - VM	UNIDADE	2	40.481,28	80.962,56
17	SISTEMA DE VOZ - TIPO II - VM	UNIDADE	10	32.148,63	321.486,30
18	SISTEMA DE VOZ GATEWAY - TIPO I APPLIANCE	UNIDADE	10	39.184,41	391.844,10
19	SISTEMA DE VOZ GATEWAY - TIPO II APPLIANCE	UNIDADE	10	30.499,24	304.992,40
20	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 1	UNIDADE	8	82.713,49	661.707,92
21	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 2	UNIDADE	3	233.187,55	699.562,65
22	SOLUÇÃO DE GERENCIAMENTO DE REDES E	UNIDADE	15	36.854,99	552.824,85



	SEGURANÇA PARA CAMPUS TIPO 3				
23	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 4	UNIDADE	5	74.799,59	373.997,95
24	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 5	UNIDADE	2	242.425,90	484.851,80
25	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CÂMPUS TIPO 6	UNIDADE	2	607.549,39	1.215.098,78
26	SWITCH TIPO 1	UNIDADE	30	9.061,03	271.830,90
27	SWITCH TIPO 3	UNIDADE	30	19.120,30	573.609,00
28	SWITCH TIPO 4	UNIDADE	15	14.853,24	222.798,60
29	SWITCH TIPO 5	UNIDADE	20	25.693,00	513.860,00
30	TARIFADOR - TELEFONIA VOIP	LICENÇA	10	3.600,58	36.005,80
31	TERMINAL DE COMUNICAÇÃO - TIPO I	UNIDADE	50	1.807,44	90.372,00
32	TRANSCEIVER 1000BASE-LX	UNIDADE	20	972,71	19.454,20
33	TRANSCEIVER 10GBASE-LR	UNIDADE	20	2.479,88	49.597,60
34	TRANSCEIVER 1000BASE-SX	UNIDADE	20	488,12	9.762,40
35	TRANSCEIVER 10GBASE-SR	UNIDADE	20	953,22	19.064,40
VALOR TOTAL				9.525.948,98	

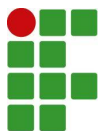
- 11.1.O valor de **R\$ 9.525.948,98 (nove milhões, quinhentos e vinte e cinco mil, novecentos e quarenta e oito reais e noventa e oito centavos)** enquadra-se na Instrução Normativa SGD/ME nº 5, de 11 de janeiro de 2021.
- 11.2.“A Instrução Normativa SGD/ME nº 5, de 11 de janeiro de 2021, regulamenta os requisitos e procedimentos para aprovação de contratações ou de formação de atas de registro de preços, a serem efetuados por órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, relativos a bens e serviços de TIC. Dessa forma, os órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional deverão submeter à Secretaria de Governo Digital do Ministério da Economia solicitação para aprovação de:
- 11.2.1.contratações relativas a bens e serviços de TIC com valor global estimado do objeto superior a 20 (vinte) vezes o previsto no art. 23, inciso II, alínea "c", da Lei nº 8.666, de 21 de junho de 1993; e
- 11.2.2.formação de atas de registro de preços de serviços de TIC passíveis de adesão por parte de órgãos ou entidades não participantes.
- 11.3.Ou seja, devem ser submetidas à apreciação da Secretaria de Governo Digital as contratações de TIC cujo valor estimado do objeto seja superior a R\$ 28.600.000,00 (vinte e oito milhões e seiscentos mil reais) e os processos licitatórios que resultem em formação de atas de registro de preços (ARP) que permitam adesão cujo valor estimado seja superior a R\$ 9.533.333,33 (nove milhões, quinhentos e trinta e três mil trezentos e trinta e três reais e trinta e três centavos).”

Fonte:

<https://www.gov.br/governodigital/pt-br/contratacoes/informacoes-sobre-a-instrucao-normativa-sgd-me-no-5-de-2021>

12. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

- 12.1.Por tratar-se de Registro de Preço a fonte de recursos será informada no momento da contratação.



13. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

13.1. Regime, Tipo e Modalidade da Licitação

13.1.1. De acordo com o Art. 1º do Decreto nº 10.024, de 20 de setembro de 2019, esta licitação deve ser realizada na modalidade de Pregão, na forma eletrônica, com julgamento pelo critério de menor preço por item/lote para o sistema de registro de preços.

13.2. Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência

13.2.1. Decreto nº 7.174/2010

13.2.1.1. Art. 3º Além dos requisitos dispostos na legislação vigente, nas aquisições de bens de informática e automação, o instrumento convocatório deverá conter, obrigatoriamente: [...]

13.2.1.2. II - as exigências, na fase de habilitação, de certificações emitidas por instituições públicas ou privadas credenciadas pelo Instituto Nacional de Metrologia, Normalização e Qualidade Industrial - Inmetro, que atestem, conforme regulamentação específica, a adequação dos seguintes requisitos: [...]

13.2.1.3. b) compatibilidade eletromagnética; [...]

13.2.1.4. Item: 2 - Injetor PoE.

13.2.1.5. Art. 5º Será assegurada preferência na contratação, nos termos do disposto no art. 3º da Lei nº 8.248, de 1991, para fornecedores de bens e serviços, observada a seguinte ordem:

13.2.1.6. I - bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

13.2.1.7. II - bens e serviços com tecnologia desenvolvida no País; e

13.2.1.8. III - bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal.

13.2.1.9. Parágrafo único. As microempresas e empresas de pequeno porte que atendam ao disposto nos incisos do caput terão prioridade no exercício do direito de preferência em relação às médias e grandes empresas enquadradas no mesmo inciso.

13.2.1.10. Itens produzidos no Brasil: Não se aplica.

13.2.2. Lei Complementar nº 123, de 2006

13.2.2.1. Preferência para me/epp: Não se aplica.

13.3. Critérios de Qualificação Técnica para a Habilitação

13.3.1. As licitantes deverão apresentar Atestados de Capacidade Técnica para comprovação de aptidão para o fornecimento de bens em características e quantidades compatíveis com o objeto desta licitação, ou com o item pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

13.3.2. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

13.3.3. Os atestados de capacidade técnica podem ser apresentados em nome da matriz ou da filial da empresa licitante;

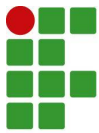
13.3.4. Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante, pois essa situação se equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação, nos termos do item 10.9 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

14 – DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

14.1.

Conforme o §6º do art. 12 da IN SGD/ME nº 1, de 2019, o Termo de Referência ou Projeto Básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC, e aprovado pela autoridade competente.

Integrante Requisitante	Integrante Técnico



Integrante Administrativo	Integrante Administrativo

Autoridade Máxima da Área de TIC

Aprovo,

Autoridade Competente

**ATA DE REGISTRO DE PREÇOS
(SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO)**

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA

ATA DE REGISTRO DE PREÇOS
N.º

O INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA, com sede na Rua 14 de Julho, 150 – Enseada dos Marinheiros – Coqueiros, Florianópolis/SC – CEP: 88.075-010, inscrito(a) no CNPJ/MF sob o nº 11.402.887/0001-60, neste ato representado pelo seu Reitor, Sr. Maurício Gariba Júnior, nomeado(a) pelo Decreto de 9 de agosto de 2021, publicado no Diário Oficial da União de 10 de agosto de 2021, edição 150, seção 2, Página 1, portador da matrícula funcional nº 0277933, considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para REGISTRO DE PREÇOS nº/20..., publicada no de/...../20....., processo administrativo nº 23292.030398/2022-96 - PE 31105/2022 - REI, RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no edital, sujeitando-se as partes às normas constantes na Lei nº 8.666, de 21 de junho de 1993 e suas alterações, no Decreto nº 7.892, de 23 de janeiro de 2013, e em conformidade com as disposições a seguir:

1. DO OBJETO

1.1. A presente Ata tem por objeto o registro de preços para eventual fornecimento de equipamentos e serviços para gerenciamento seguro da rede LAN/WLAN do IFSC, especificados nos itens 1 a 26 do Termo de Referência, anexo I do edital de Pregão nº 31105/2022, que é parte integrante desta Ata, assim como a proposta vencedora, independentemente de transcrição.

2. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1. O preço registrado, as especificações do objeto e as demais condições ofertadas na(s) proposta(s) são as que seguem:

Fornecedor da solução (<i>razão social, CNPJ/MF, endereço, contatos, representante</i>)				
ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	Unidade de Medida	Quantidade	Valor Unitário
1				
2				
3				
...				

3. DA ADESAO À ATA DE REGISTRO DE PREÇOS

3.1. A ata de registro de preços, durante sua validade, poderá ser utilizada por qualquer órgão ou entidade da administração pública que não tenha participado do certame licitatório, mediante anuência do órgão gerenciador, desde que devidamente

justificada a vantagem e respeitadas, no que couber, as condições e as regras estabelecidas na Lei nº 8.666, de 1993 e no Decreto nº 7.892, de 2013.

- 3.1.1. A manifestação do órgão gerenciador de que trata o subitem anterior, salvo para adesões feitas por órgãos ou entidades de outras esferas federativas, fica condicionada à realização de estudo, pelos órgãos e pelas entidades que não participaram do registro de preços, que demonstre o ganho de eficiência, a viabilidade e a economicidade para a administração pública federal da utilização da ata de registro de preços, conforme estabelecido em ato do Secretário de Gestão do Ministério da Economia.
- 3.1.2. Salvo para Atas de Registro de Preços gerenciadas no âmbito do Ministério da Economia, a adesão de que trata este item, para fins de contratação de serviço de tecnologia da informação e comunicação, só será permitida após a aprovação da ata de registro de preços pela Secretaria de Governo Digital do Ministério da Economia na forma do art. 22, §10, II do Decreto nº 7.892, de 2013 e da Instrução Normativa SGD/ME nº 2, de 4 de abril de 2019.
 - 3.1.2.1. O subitem anterior não se aplica às hipóteses em que a contratação de serviço esteja vinculada ao fornecimento de bens de tecnologia da informação e comunicação constante da mesma ata de registro de preços.
- 3.2. Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento, desde que este fornecimento não prejudique as obrigações anteriormente assumidas com o órgão gerenciador e órgãos participantes.
- 3.3. As aquisições ou contratações adicionais a que se refere este item não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador.
- 3.4. As adesões à ata de registro de preços são limitadas, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador, independente do número de órgãos não participantes que eventualmente aderirem.
 - 3.4.1. Tratando-se de item exclusivo para microempresas e empresas de pequeno porte e cooperativas enquadradas no artigo 34 da Lei nº 11.488, de 2007, o órgão gerenciador somente autorizará a adesão caso o valor da contratação pretendida pelo aderente, somado aos valores das contratações já previstas para o órgão gerenciador e participantes ou já destinadas à aderentes anteriores, não ultrapasse o limite de R\$ 80.000,00 (oitenta mil reais) (Acórdão TCU nº 2957/2011 – P).
- 3.5. Ao órgão não participante que aderir à ata competem os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, informando as ocorrências ao órgão gerenciador.
- 3.6. Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a contratação solicitada em até noventa dias, observado o prazo de validade da Ata de Registro de Preços.
 - 3.6.1. Caberá ao órgão gerenciador autorizar, excepcional e justificadamente, a prorrogação do prazo para efetivação da contratação, respeitado o prazo de vigência da ata, desde que solicitada pelo órgão não participante.

4. VALIDADE DA ATA

4.1. A validade da Ata de Registro de Preços será de 12 meses, a partir do(a)....., não podendo ser prorrogada.

5. REVISÃO E CANCELAMENTO

5.1. A Administração realizará pesquisa de mercado periodicamente, em intervalos não superiores a 180 (cento e oitenta) dias, a fim de verificar a vantajosidade dos preços registrados nesta Ata.

5.2. Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo do objeto registrado, cabendo à Administração promover as negociações junto ao(s) fornecedor(es).

5.3. Quando o preço registrado se tornar superior ao preço praticado no mercado por motivo superveniente, a Administração convocará o(s) fornecedor(es) para negociar(em) a redução dos preços aos valores praticados pelo mercado.

5.4. O fornecedor que não aceitar reduzir seu preço ao valor praticado pelo mercado será liberado do compromisso assumido, sem aplicação de penalidade.

5.4.1. A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação original.

5.5. Quando o preço de mercado se tornar superior aos preços registrados e o fornecedor não puder cumprir o compromisso, o órgão gerenciador poderá:

5.5.1. liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados; e

5.5.2. convocar os demais fornecedores para assegurar igual oportunidade de negociação.

5.6. Não havendo êxito nas negociações, o órgão gerenciador deverá proceder à revogação desta ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

5.7. O registro do fornecedor será cancelado quando:

5.7.1. descumprir as condições da ata de registro de preços;

5.7.2. não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, sem justificativa aceitável;

5.7.3. não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado; ou

5.7.4. sofrer sanção administrativa cujo efeito torne-o proibido de celebrar contrato administrativo, alcançando o órgão gerenciador e órgão(s) participante(s).

5.8. O cancelamento de registros nas hipóteses previstas nos itens 6.7.1, 6.7.2 e 6.7.4 será formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa.

5.9. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados:

5.9.1. por razão de interesse público; ou

5.9.2. a pedido do fornecedor.

6. DAS PENALIDADES

6.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no Edital.

6.1.1. As sanções do item acima também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente, nos termos do art. 49, §1º do Decreto nº 10.024/19.

6.2. É da competência do órgão gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço (art. 5º, inciso X, do Decreto nº 7.892/2013), exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos participantes, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade (art. 6º, Parágrafo único, do Decreto nº 7.892/2013).

6.3. O órgão participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no art. 20 do Decreto nº 7.892/2013, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

7. CONDIÇÕES GERAIS

7.1. As condições gerais do fornecimento, tais como os prazos para entrega e recebimento do objeto, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, anexo ao Edital.

7.2. É vedado efetuar acréscimos nos quantitativos fixados nesta ata de registro de preços, inclusive o acréscimo de que trata o § 1º do art. 65 da Lei nº 8.666/93, nos termos do art. 12, §1º do Decreto nº 7.892/13.

7.3. *A ata de realização da sessão pública do pregão, contendo a relação dos licitantes que aceitarem cotar os bens ou serviços com preços iguais ao do licitante vencedor do certame, será anexada a esta Ata de Registro de Preços, nos termos do art. 11, §4º do Decreto n. 7.892, de 2013.*

Para firmeza e validade do pactuado, a presente Ata foi lavrada em 1 (uma) via, que, depois de lida e achada em ordem, vai assinada pela autoridade competente. A adesão das empresas vencedoras a esta Ata se dá pelas Declarações de Concordância Anexas.

Local e data
Assinaturas

Representante legal do órgão gerenciador



ANEXO III

Modelo de Termo de Compromisso de Manutenção de Sigilo

O Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, sediado à rua 14 de Julho, 150, Coqueiros, CEP: 88075-010, Florianópolis-SC, CNPJ n.º 11.402.887/0001-60, doravante denominado CONTRATANTE, e, de outro lado a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n.º <CNPJ>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do ATA DE REGISTRO DE PREÇOS N.º XX/20XX doravante denominado ARP, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção; CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto da ARP celebrado entre as partes e em acordo com o que dispõem a Lei nº 12.527, de 18/11/2011 e os Decretos nº 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

ARP: Instrumento celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não a ARP, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Cláusula Quarta – DOS LIMITES DO SIGILO



As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – Sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento da ARP.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa do CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes. **Parágrafo Quinto** – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados e contratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I. – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções



adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II. – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III. – Comunicar ao CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL. A vigência deste Termo independe do prazo de vigência do contrato assinado ou ARP.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão da ARP firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme art. 87 da Lei nº. 8.666/93.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de confidencialidade é parte integrante e inseparável da ARP.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro - Havendo necessidade legal devido a Programas de Governo, a CONTRATADA assume o compromisso de assinar Termo de Sigilo (ou equivalente) adicional relacionado ao Programa, prevalecendo as cláusulas mais restritivas em benefício do CONTRATANTE.

Parágrafo Quarto – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I. – O CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;



II. – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

III. – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

IV. – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

V. – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizam ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VI. – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VII. – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

O CONTRATANTE elige o foro de Florianópolis, onde está localizada a sede do CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja. E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

Florianópolis, XX de XXXXXXXX de 2022

De acordo.

CONTRATANTE	CONTRATADA
Nome: Matrícula:	Nome: Qualificação:
Testemunhas	
Testemunha 1	Testemunha 2



 Nome: Qualificação:	 Nome: Qualificação:



 Nome: Qualificação:	 Nome: Qualificação:
 Nome: Qualificação:	 Nome: Qualificação:
 Nome: Qualificação:	 Nome: Qualificação:

ANEXO V
DADOS PARA CADASTRAMENTO DA EMPRESA
PROCESSO 23292.030398/2022-96
PREGÃO ELETRÔNICO - SRP 31105/2022

Confirmo que os dados abaixo relacionados, referentes à empresa XXXXXXXXXXXXXXXXXX, estão atualizados e podem ser utilizados para atendimento ao disposto no Edital de licitação.

Assumo a responsabilidade de manter estes dados atualizados, junto ao IFSC, através do e-mail srp@ifsc.edu.br, no mínimo durante a vigência da referida ATA/Contrato.

EMPRESA (Razão Social)			
CNPJ			
ENDEREÇO			
CEP			
CIDADE		ESTADO	
TELEFONE/FAX			
REPRESENTANTE LEGAL			
CPF REPRESENTANTE			
ENDEREÇO ELETRÔNICO VÁLIDO (e-mail)			

Cidade, XX de XXXXXXXX de 20XX.

Atenciosamente,

Representante da Empresa

Cargo Ocupado

[Baixar arquivo editável](#)



Buscar...



Pesquisa de Satisfação



Validar Documento



Sistema de Gerenciamento Institucional



Diário Oficial



Lei Geral de Proteção de Dados



Sistema Eletrônico de Informações

Pregão Eletrônico – Adesão a Ata de Registro de Preços

Por Assessoria de Comunicação em 6 de junho de 2023

Conforme o Decreto nº 46311/2013, art. 20, § 1º, a Defensoria Pública do Estado de Minas Gerais comunica a intenção de adesão, como órgão não-participante (carona), à Ata de Registro de Preços nº 31105/2022 do Pregão Eletrônico nº 31105/2022, cujo órgão gestor é o Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, para aquisição de Solução de Segurança.

Compartilhar com:

Tags:

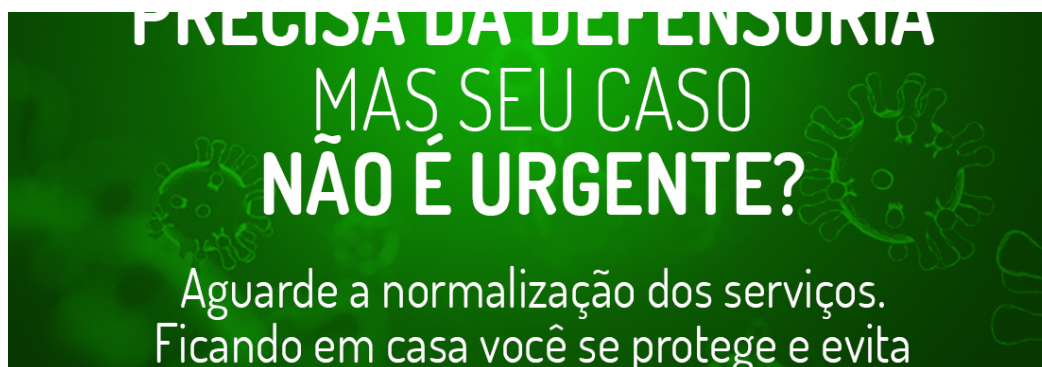
PRÓXIMO POST

OUTRAS NOTÍCIAS RELACIONADAS





Seis meses após o desastre de Brumadinho, Defensoria Pública de MG ultrapassa 2.500 atendimentos e viabiliza acordos em favor dos atingidos...



Coronavírus: Defensoria Pública de Minas Gerais atua em regime de plantão no período de 19 a 27 de março...



Defensoria Pública mineira participa de curso do TCEMG voltado para orientação de prestações de contas das APACs...



Defensoria Pública participa de entrega de verbas pecuniárias a projetos sociais...



DPMG

Perfil
Planejamento
Estratégico
Estrutura
Organizacional
Escola Superior
Legislação
Histórico

CORPO GESTOR

Defensoria
Pública-Geral
Subdefensoria-
Geral
Conselho
Superior
Corregedoria-
Geral

UNIDADES

Municípios com
DPMG

SERVIÇOS

Cível
Consumidor
Criminal
Defesa da Mulher
Direitos
Humanos
Família e
Sucessões
Pessoa Idosa
Criança e
Adolescente
Justiça Militar
Pessoa com
Deficiência
Saúde
Segunda
Instância e
Tribunais
Superiores

AÇÕES

A Defensoria vai
até você
Além da Culpa
Aprendendo a
Conciliar
Audiências de
Custódia
Casamento
Comunitário
Casamento
Igualitário
Conciliar: Só
Depende de Você
Defensoras
Populares
Defensoria
Itinerante
Defensoria no Lar
Defensoria no
PPCAAM
Dia Mundial dos
Pobres
Direito a Ser
Dono
Direito a Ter Pai

ESPAÇO CIDADÃO

Cartilhas SEEU
Cartilhas sobre
direitos
Concursos da
DPMG
Critérios de
atendimento
Documentos p/
Atendimento
Estágio
Processos
Seletivos
Estágio
obrigatório –
convênios
Estágio –
Apresentação
Informativos
temáticos
Lei Geral de
Proteção de
Dados
Perguntas
Frequentes

Escola de	Revista da
Convivência	Defensoria
Familiar	Unidades da
Gestação Legal	Defensoria
Inclusão Verde	
Mundo – Rede	
em Proteção	
MESC – Paz em	
Ação	
Mutirão das	
Famílias	
Prenome e	
Gênero das	
travestis e	
transexuais	
Proteção Integral	
Realização	
Exames de DNA	

TRANSPARÊNCIA

Execução orçamentária
 Gestão de documentos
 LOA e LDO
 Planejamento Estratégico
 Plano Geral de Atuação
 Produtividade
 Projetos Convênios e Parcerias
 Quadro de Pessoas
 Relação de contratos
 Relação das licitações
 Relatório de Remuneração
 Relatório de Gestão
 Relatório de Gestão Fiscal

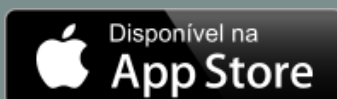
IMPRENSA

Ascom
 Deu na mídia
 Especiais
 Identidade Visual
 Notícias



Rua dos Guajajaras, 1707 - Barro Preto Belo Horizonte, Minas Gerais
CEP: 30.180.099
(31) 3526-0500

Baixe o App da DPMG





MAPA COMPARATIVO DE PREÇOS - DETALHADO

Número do mapa: 1441003 000128/2023

Pedido de material e serviço: 1441003 000106/2023

Data de criação: 06/06/2023

Situação: Assinado

Responsável: HELBERT BRUNO PAULINO LOURENCO

Objetivo:

Instruir o pedido de compras - Disponibilidade orçamentária

Instruir o Processo de compras

Itens do mapa

Nº	Código do item	Desc. do item de material	Unid. de aquisição	Quantitativo orçado	Valor mínimo (R\$)	Valor máximo (R\$)	Orçamento estimado unitário(R\$)	Orçamento estimado total (R\$)	Metodologia definida
1	001910418	SOLUCAO GERENCIAMENTO DE EVENTOS DE SEGURANCA - CAPACIDADE: MINIMA 5GB DE LOGS DIARIOS; ARMAZENAMENTO: MINIMO 3 TB (AREA LIVRE PARA LOGS); INTERFACE: V	UNIDADE	1,0000	67.511,0200	67.511,0200	67.511,0200	67.511,02	Menor preço
2	001910027	MODULO TRANSCEPTOR PARA FIBRA OPTICA - PADRAO: SFP; CONECTOR: LC DUPLEX; MODO DE OPERACAO: DISTANCIA ATE 400 METROS PARA FIBRAS MULTIMODO; DETALHES: CO	1,00 UNIDADE	8,0000	487,0400	487,0400	487,0400	3.896,32	Menor preço
3	001910434	FIREWALL (HARDWARE) - IDENTIFICACAO: APPLIANCE - SOLUCAO DE SEGURANCA DE FIREWALL NGFW; TAXA DE TRANSFERENCIA: 8.4 GBPS DE TRAFEGO SSL; CONEXAO: 16 INT	1,00 UNIDADE	1,0000	343.861,9100	343.861,9100	343.861,9100	343.861,91	Menor preço
4	001726145	MODULO TRANSCEPTOR PARA FIBRA OPTICA - PADRAO: SPF+; CONECTOR: LC PADRAO SR 10GB; MODO DE OPERACAO: MULTIMODO FULL DUPLEX; DETALHES: NAO APLICAVEL;	1,00 UNIDADE	8,0000	946,2300	946,2300	946,2300	7.569,84	Menor preço
							Total orçado:	422.839,09	

Detalhamento do orçamento estimado

Descrição do item:

SOLUCAO GERENCIAMENTO DE EVENTOS DE SEGURANCA - CAPACIDADE: MINIMA 5GB DE LOGS DIARIOS; ARMAZENAMENTO: MINIMO 3 TB (AREA LIVRE PARA LOGS); INTERFACE: VNIC INTERFACES/PORTS; CONEXAO: APPLIANCE VIRTUAL (MAQUINA VIRTUAL);

Índice de atualização associado à classe: Não existe índice de atualização vinculado à classe de material no momento da geração desse relatório.

Novo índice de atualização selecionado para o item deste mapa: -

Metodologia de cálculo:

Menor valor:R\$ 67.511,0200

Média:R\$ 67.511,0200

Mediana:R\$ 67.511,0200

Preços que compõem o orçamento estimado

Origem do preço	Nº documento de referência	Processo de compra / item	Qtde.	Data de homologação / Data de referência	Marca / Modelo	Procedimento de contratação	Fornecedor	Preço unitário homologado / consultado (R\$)	Preço unitário reajustado (R\$)
Inserção manual / Aquisições e contratações realizadas pela Administração Pública (inciso II)	1	-	1,0000	13/04/2023	-	-	03.232.670/0001-21 - ADVANTA SISTEMAS DE TELECOMUNICACOES E SERVICOS DE INFORMATICA LTDA.	67.511,0200	67.511,0200

Preços desconsiderados - Acima da mediana Inciso I - Quantidade: 0

nenhum item desconsiderado

Preços desconsiderados em função dos filtros de pesquisa aplicados - Inciso I - Quantidade: 0

nenhum item desconsiderado

Preços desconsiderados - Justificativas - Quantidade: 0

nenhum item desconsiderado

Descrição do item:

MODULO TRANSCPTOR PARA FIBRA OPTICA - PADRAO: SFP; CONECTOR: LC DUPLEX; MODO DE OPERACAO: DISTANCIA ATE 400 METROS PARA FIBRAS MULTIMODO; DETALHES: COMPATIVEL COM O PADRAO 1000BASE-SX;

Índice de atualização associado à classe: Não existe índice de atualização vinculado à classe de material no momento da geração desse relatório.

Novo índice de atualização selecionado para o item deste mapa: -

Metodologia de cálculo:

Menor valor:	R\$ 487,0400
Média:	R\$ 487,0400
Mediana:	R\$ 487,0400

Preços que compõem o orçamento estimado

Origem do preço	Nº documento de referência	Processo de compra / item	Qtde.	Data de homologação / Data de referência	Marca / Modelo	Procedimento de contratação	Fornecedor	Preço unitário homologado / consultado (R\$)	Preço unitário reajustado (R\$)
Inserção manual / Aquisições e contratações realizadas pela Administração Pública (inciso II)	1	-	8,0000	13/04/2023	-	-	03.232.670/0001-21 - ADVANTA SISTEMAS DE TELECOMUNICACOES E SERVICOS DE INFORMATICA LTDA.	487,0400	487,0400

Preços desconsiderados - Acima da mediana Inciso I - Quantidade: 0

nenhum item desconsiderado

Preços desconsiderados em função dos filtros de pesquisa aplicados - Inciso I - Quantidade: 0

nenhum item desconsiderado

Preços desconsiderados - Justificativas - Quantidade: 0

nenhum item desconsiderado

Nº: 3 Código do item de material ou serviço: 001910434 Unidade de aquisição: 1,00 UNIDADE

Descrição do item:

FIREWALL (HARDWARE) - IDENTIFICACAO: APPLIANCE - SOLUCAO DE SEGURANCA DE FIREWALL NGFW; TAXA DE TRANSFERENCIA: 8.4 GBPS DE TRAFEGO SSL; CONEXAO: 16 INTERFACES 1 GIGABIT ETHERNET PADRAO 1000BASE; INTERFACE: 4 INTERFACES 10 GIGABIT ETHERNET PADRAO 10GBASE-X; COMPONENTE (4): SEM COMPONENTES; FONTE DE ALIMENTACAO: REDUNDANTE (HOT SWAPPABLE); TENSAO: BIVOLT AUTOMATICO;

Índice de atualização associado à classe: Não existe índice de atualização vinculado à classe de material no momento da geração desse relatório.

Novo índice de atualização selecionado para o item deste mapa: -

Metodologia de cálculo:

Menor valor:	R\$ 343.861,9100
Média:	R\$ 343.861,9100
Mediana:	R\$ 343.861,9100

Preços que compõem o orçamento estimado

Origem do preço	Nº documento de referência	Processo de compra / item	Qtde.	Data de homologação / Data de referência	Marca / Modelo	Procedimento de contratação	Fornecedor	Preço unitário homologado / consultado (R\$)	Preço unitário reajustado (R\$)
Inserção manual / Aquisições e contratações realizadas pela Administração Pública (inciso II)	1	-	1,0000	13/04/2023	-	-	03.232.670/0001-21 - ADVANTA SISTEMAS DE TELECOMUNICACOES E SERVICOS DE INFORMATICA LTDA.	343.861,9100	343.861,9100

Preços desconsiderados - Acima da mediana Inciso I - Quantidade: 0

nenhum item desconsiderado

Preços desconsiderados em função dos filtros de pesquisa aplicados - Inciso I - Quantidade: 0

nenhum item desconsiderado

Preços desconsiderados - Justificativas - Quantidade: 0

nenhum item desconsiderado

Nº: 4 Código do item de material ou serviço: 001726145 Unidade de aquisição: 1,00 UNIDADE

Descrição do item:

MODULO TRANSCPTOR PARA FIBRA OPTICA - PADRAO: SPF+; CONECTOR: LC PADRAO SR 10GB; MODO DE OPERACAO: MULTIMODO FULL DUPLEX; DETALHES: NAO APLICAVEL;

Índice de atualização associado à classe: Não existe índice de atualização vinculado à classe de material no momento da geração desse relatório.

Novo índice de atualização selecionado para o item deste mapa: -

Metodologia de cálculo:

Menor valor: R\$ 946,2300

Média: R\$ 946,2300

Mediana: R\$ 946,2300

Preços que compõem o orçamento estimado

Origem do preço	Nº documento de referência	Processo de compra / item	Qtde.	Data de homologação / Data de referência	Marca / Modelo	Procedimento de contratação	Fornecedor	Preço unitário homologado / consultado (R\$)	Preço unitário reajustado (R\$)
Inserção manual / Aquisições e contratações realizadas pela Administração Pública (inciso II)	1	-	8,0000	13/04/2023	-	-	03.232.670/0001-21 - ADVANTA SISTEMAS DE TELECOMUNICACOES E SERVICOS DE INFORMATICA LTDA.	946,2300	946,2300

Preços desconsiderados - Acima da mediana Inciso I - Quantidade: 0

nenhum item desconsiderado

Preços desconsiderados em função dos filtros de pesquisa aplicados - Inciso I - Quantidade: 0

nenhum item desconsiderado

Preços desconsiderados - Justificativas - Quantidade: 0

nenhum item desconsiderado

(*) Condições que influenciam o preço e justificam a desconsideração neste processo:

- 1 - Prazo, frete ou local de entrega
- 2 - Instalação ou montagem do be
- 3 - Modo de execução do serviço
- 4 - Termos de garantia exigidos
- 5 - Marca e/ou modelo
- 6 - Escala da quantidade do objeto
- 7 - Forma de pagamento
- 8 - Preço Inexequível
- 9 - Sobrepreço
- 10 - Custos indiretos
- 11 - Outra (Verifique no site do Portal de Compras)

O Mapa Comparativo de Preços foi elaborado de acordo com a Resolução SEPLAG nº 102, de 29 de Dezembro de 2022, disponível para consulta no link BANCO DE NORMAS GESTÃO LOGÍSTICA PATRIMÔNIO - CADASTROS - SISMP do site www.compras.mg.gov.br.

Assinatura digital - Signatário:

Nome:

HELBERT BRUNO PAULINO LOURENCO

Masp:

X0083427

CPF:

xxx.254.496-xx

Emissor do certificado:

Portal de Compras - MG / Assinatura eletrônica

Data da assinatura:

06/06/2023 11:11:00

Código de Autenticidade:

Código verificador: 230000214889322188962023



MAPA COMPARATIVO DE PREÇOS - DETALHADO

Número do mapa: 1441003 000129/2023

Pedido de material e serviço: 1441003 000108/2023

Data de criação: 06/06/2023

Situação: Assinado

Responsável: HELBERT BRUNO PAULINO LOURENCO

Objetivo:

Instruir o pedido de compras - Disponibilidade orçamentária

Instruir o Processo de compras

Itens do mapa

Nº	Código do item	Desc. do item de material	Unid. de aquisição	Quantitativo orçado	Valor mínimo (R\$)	Valor máximo (R\$)	Orçamento estimado unitário(R\$)	Orçamento estimado total (R\$)	Metodologia definida
1	000046000	SERVICO DE MONTAGEM, INSTALACAO, CONFIGURACAO E PADRONIZACAOE SOFTWARE E EQUIPAMENTO DA SOLUCAO DE DATACENTER	1,00 UNIDADE	2,0000	20.564,8150	20.564,8150	20.564,8150	41.129,63	Menor preço
							Total orçado:	41.129,63	

Detalhamento do orçamento estimado

Nº: 1

Código do item de material ou serviço: 000046000

Unidade de aquisição: 1,00 UNIDADE

Descrição do item:

SERVICO DE MONTAGEM, INSTALACAO, CONFIGURACAO E PADRONIZACAOE SOFTWARE E EQUIPAMENTO DA SOLUCAO DE DATACENTER

Índice de atualização associado à classe:

Não existe índice de atualização vinculado à classe de material no momento da geração desse relatório.

Novo índice de atualização selecionado para o item deste mapa:

-

Metodologia de cálculo:

Menor valor: R\$ 20.564,8150

Média: R\$ 20.564,8150

Mediana: R\$ 20.564,8150

Preços que compõem o orçamento estimado

Origem do preço	Nº documento de referência	Processo de compra / item	Qtde.	Data de homologação / Data de referência	Marca / Modelo	Procedimento de contratação	Fornecedor	Preço unitário homologado / consultado (R\$)	Preço unitário reajustado (R\$)
Inserção manual / Aquisições e contratações realizadas pela Administração Pública (inciso II)	1	-	2,0000	13/04/2023	-	-	03.232.670/0001-21 - ADVANTA SISTEMAS DE TELECOMUNICACOES E SERVICOS DE INFORMATICA LTDA.	20.564,8150	20.564,8150

Preços desconsiderados - Acima da mediana Inciso I - Quantidade: 0

nenhum item desconsiderado

Preços desconsiderados em função dos filtros de pesquisa aplicados - Inciso I - Quantidade: 0

nenhum item desconsiderado

Preços desconsiderados - Justificativas - Quantidade: 0

nenhum item desconsiderado

(*) Condições que influenciam o preço e justificam a desconsideração neste processo:

- 1 - Prazo, frete ou local de entrega
- 2 - Instalação ou montagem do be
- 3 - Modo de execução do serviço
- 4 - Termos de garantia exigidos
- 5 - Marca e/ou modelo
- 6 - Escala da quantidade do objeto
- 7 - Forma de pagamento
- 8 - Preço Inexequível
- 9 - Sobrepreço
- 10 - Custos indiretos
- 11 - Outra (Verifique no site do Portal de Compras)

O Mapa Comparativo de Preços foi elaborado de acordo com a Resolução SEPLAG nº 102, de 29 de Dezembro de 2022, disponível para consulta no link BANCO DE NORMAS GESTÃO LOGÍSTICA PATRIMÔNIO - CADASTROS - SISMP do site www.compras.mg.gov.br.

Assinatura digital - Signatário:

Nome: HELBERT BRUNO PAULINO LOURENCO

Masp: X0083427

CPF: xxx.254.496-xx

Emissor do certificado:

Portal de Compras - MG / Assinatura eletrônica

Data da assinatura: 06/06/2023 11:28:06

Código de Autenticidade:

Código verificador: 230000214996610560412023



DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS
Assessoria Jurídica

Processo SEI nº: 9990000001.003832/2023-69

PARECER n.º068/2023.

Exma. Sra. Defensora Pública-Geral,
Dra. Raquel Gomes de Sousa da Costa Dias

EMENTA: aquisição de solução de segurança de rede com gerenciamento e instalação com configuração, observadas as condições e especificações técnicas estabelecidas - Ata de Registro de Preços 31105/2022 - IFSC – Adesão da Defensoria Pública como não participante – Possibilidade.

I – RELATÓRIO

1.1 Trata-se do procedimento administrativo nº 068/2023 em que a Defensoria Pública do Estado de Minas Gerais (DPMG) pretende aquisição de solução de segurança de rede com gerenciamento e instalação com configuração, observadas as condições e especificações técnicas estabelecidas, como não participante, da Ata de Registro de Preços nº 31105/2022 do **INSTITUTO FEDERAL DE SANTA CATARINA**, conforme solicitação e justificativa do Diretor de Informação e Dados, 0105677 e Termo de Referência 0105943.

1.2. Nesses termos, o procedimento foi encaminhado para esta Assessoria Jurídica para análise de sua regularidade jurídica, conforme determina o art. 38, parágrafo único, da Lei n.º 8.666/93.

Assessoria Jurídica - tel.: (31) 2522-8722 / 2522-8723
Rua Bernardo Guimarães, nº 2731 – Santo Agostinho - Belo Horizonte/MG – CEP 30.140-085

TADEU RODRIGO
TITO DE
OLIVEIRA:90345562

Assinado de forma digital
por TADEU RODRIGO TITO
DE OLIVEIRA:90345562
Dados: 2023.06.19
11:33:41 -03'00'



DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS
Assessoria Jurídica

II – FUNDAMENTAÇÃO

2.1 O Sistema de Registro de Preços pode ser definido como o conjunto de procedimentos para registro formal de preços relativos à prestação de serviços e aquisição de bens, para contratações futuras, realizado por meio de uma única licitação, na modalidade de concorrência ou pregão, em que as empresas disponibilizam os bens e serviços a preços e prazos registrados em ata específica e que a aquisição ou contratação é feita quando melhor convier aos órgãos/entidades que integram a Ata (participantes), ou que venham integrá-la (não participante).

2.2 No âmbito do Estado de Minas Gerais, atendendo ao disposto no art. 15, II, da Lei n.º 8.666, de 21 de junho de 1993, as contratações de serviços e aquisição de bens, quando efetuadas pelo Sistema de Registro de Preços, são regidas pelo Decreto Estadual n.º 46.311, de 16 de setembro de 2013.

2.3 Consoante definição contida no art. 2º do referido Decreto, órgão participante é o “órgão ou entidade da Administração Pública que participa dos procedimentos iniciais da licitação para registro de preços e integra a ARP” (art. 2º, inciso XI) e órgão não participante é o “órgão ou entidade da Administração Pública que, não tendo participado dos procedimentos iniciais da licitação, faz adesão à ARP durante sua vigência, atendidos os requisitos desta norma” (art. 2º, inciso XII).

2.4 Sobre o tema é importante ressaltar que o Tribunal de Contas do Estado de Minas Gerais possui julgado esclarecedor sobre os pressupostos para a contratação por registro de preços, e, em especial, sobre a figura do não participante, em que pese se tratar de julgado anterior à citada norma, continua aplicável ao presente caso, vejamos:

TADEU RODRIGO
TITO DE
OLIVEIRA:90345562

Assinado de forma digital
por TADEU RODRIGO TITO
DE OLIVEIRA:90345562
Dados: 2023.06.19
11:33:59 -03'00'



DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS
Assessoria Jurídica

Consulta. Possibilidade de autarquia municipal utilizar como ‘carona’ o sistema de registro de preços elaborado pelo Poder Executivo do Município. “(...) o §3º do art. 15 da Lei Federal nº 8.666/93 estatui que o sistema de registro de preços será regulamentado por decreto (...). Em Minas Gerais, o assunto [foi] (...) disciplinado pelo Decreto nº 42.652/03, alterado pelo Decreto nº 43.979/05, [sendo ambos posteriormente revogados pelo Decreto nº 44.787/2008]. (...) mister esclarecer sobre as figuras que integram esse sistema: Gerenciador é o órgão ou entidade da Administração Pública responsável pela condução do conjunto de procedimentos do certame (...) e [pelo] gerenciamento da Ata de Registro de Preços dele decorrente, que, por sua vez, é o documento vinculativo, obrigacional, com característica de compromisso para a futura contratação, em que se registram os preços, os fornecedores, os órgãos participantes e as condições a serem praticadas (...). A seu termo, participante é aquele órgão que, sob a coordenação do gerenciador, participa da implantação do sistema de registro de preços, informando as quantidades e qualidade dos objetos pretendidos. **‘Carona’ é o apelido do órgão ou entidade que não participou da licitação que deu origem à Ata de Registro de Preços, [mas que] aderiu a ela durante a sua vigência.** (...) as contratações para o sistema de registro de preço são realizadas mediante uma única licitação, nas modalidades concorrência pública, do tipo ‘menor preço’, ou pregão. Nessa licitação, o órgão gerenciador e os participantes deverão estabelecer os serviços ou quantidade aproximada de material que pretendem adquirir nos próximos 12 (doze) meses e estimar o quantitativo mensal do consumo. Realizada a licitação, a Administração deverá firmar a Ata de Registro de Preços, válida por um ano, na qual ficará registrado o preço oferecido pelos fornecedores, que estarão obrigados a mantê-lo fixo por esse prazo, contado da data da apresentação da proposta. Assim, a Administração terá a liberdade de, a qualquer momento em que precisar de uma determinada quantidade daquele material/serviço constante no sistema de registro de preço, fazer o pedido ao fornecedor, que estará obrigado a entregá-lo exatamente pelo preço registrado, podendo a Administração adquirir o quantitativo total previsto no edital ou quantidade inferior, ou até deixar de adquirir o produto, sem que isso implique qualquer compromisso de indenização ao fornecedor, caso aquele material/serviço por motivo justificado deixe de ser por ela utilizado. Conforme consignado fartamente na doutrina, o sistema de registro de preço apresenta uma série de vantagens, como a diminuição do número de licitações, melhor organização e otimização das estratégias de suprimento, facilitação na execução do orçamento, celeridade na aquisição de bens etc. Entretanto, ao lado dos aspectos positivos, a figura do ‘carona’ é polêmica, pois poderia representar o avesso do princípio licitatório (...). **O ‘carona’ apenas se beneficia da Ata de outrem, a ela aderindo mediante o cumprimento de algumas exigências formais.** (...) nos ensina o mestre Marçal Justen Filho: ‘Em primeiro lugar, incumbe ao órgão que pretende valer-se do sistema alheio justificar cumpridamente os motivos pelos quais não integrou desde o início a implantação do sistema. (...) Em segundo lugar, deve comprovar-se que



DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS
Assessoria Jurídica

o empréstimo não acarretará a frustração de qualquer dos requisitos de validade da licitação cabível'. (Comentários à Lei de Licitações e Contratos Administrativos, 11ª edição, Dialética, São Paulo, 2000, pág.159). (...) **De toda sorte, deverá o interessado (carona) elaborar processo administrativo por sua iniciativa, qual seja, providenciar termo de referência no qual constem as especificações do objeto que deseja adquirir, após ampla pesquisa de preços de mercado, e, ainda, informações relativas à existência de Ata de Registro de Preço sobre o objeto desejado, para fins de acionar o órgão/entidade gerenciador, externando sua intenção de utilizar a respectiva Ata. O órgão gerenciador consultará ao fornecedor acerca da possibilidade de atender àquela adesão, uma vez que haverá acréscimo ao quantitativo pactuado. A justificativa apresentada deverá demonstrar a vantagem econômica da adesão à referida Ata, mencionando, ainda, a similitude de condições, tempestividade do prazo, suficiência das quantidades e qualidade do bem. A esse processo administrativo deve ser agregada, também, a anuência formal da entidade/órgão gerenciador sobre a possibilidade de utilização da Ata de Registro de Preços, para a adesão ao preço registrado, bem como dos fornecedores, obedecendo-se à ordem de classificação. Quanto à publicidade do instrumento de adesão e das aquisições que dele decorrerem prevalece, a meu juízo, o dever de observar a regra geral da licitação contida na legislação de regência, em especial a Lei Federal nº 8666/93, valendo para o 'carona' as mesmas regras impostas às outras entidades/órgãos envolvidos no certame**". (Consulta n.º 757978. Rel. Conselheiro Subst. Gilberto Diniz. Sessão do dia 08/10/2008)

2.5 Dessa forma, conclui-se que a formalização do procedimento para a adesão à Ata de Registro de Preços segue a mesma instrução dos demais procedimentos de compra, sendo necessário, *"elaborar processo administrativo por sua iniciativa, qual seja, providenciar termo de referência no qual constem as especificações do objeto que deseja adquirir, após ampla pesquisa de preços de mercado"*. A opção pela adesão, como dito alhures, é etapa posterior, só ocorre após a especificação do objeto, o levantamento de seu quantitativo e pesquisa mercadológica, elementos fundamentais para se concluir pela vantajosidade da adesão.

TADEU RODRIGO
TITO DE
OLIVEIRA:903455
62

Assinado de forma digital
por TADEU RODRIGO TITO
DE OLIVEIRA:90345562
Dados: 2023.06.19
11:34:20 -03'00'



DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS
Assessoria Jurídica

2.5.1 Visando corroborar o acima asseverado, colacionamos o entendimento da Advocacia Geral da União (AGU), exposta no parecer PARECER/CONJUR/MTE/Nº 134/2010, Processo nº 46130.003834/2010-72, de relatoria do Advogado da União, Joaquim Pereira dos Santos¹:

(...)

6. Pois bem, feitas tais considerações a respeito do instituto, passa-se à análise da demanda propriamente dita, que consiste em manifestação quanto a se seria necessário ou não a elaboração de "novo" termo de referência, em caso de adesão à ata de registro de preços de outro órgão, considerando que tal documento já fora elaborado quando do registro de preços originário, pelo órgão gerenciador.

7. Inicialmente, vale evidenciar os procedimentos que deverão ser observados pelo Administrador, antes de fazer a opção pela adesão ou não a uma dada ata de registro de preços.

8. A fase inicial de um procedimento de adesão a preços já registrados coincide com a fase inicial - interna - de um procedimento licitatório comum. Neste sentido, colaciona-se trecho de autorizada doutrina, verbis²:

"Suponhamos a formalização de um processo de aquisição de um objeto (bem ou serviços) em que a Administração Pública MOTIVADAMENTE (sic) e conforme seu PLANEJAMENTO resolve fazer uma adesão a uma ARP.

Os procedimentos iniciais da formalização processual, em geral, são os mesmos da elaboração de um processo licitatório para registro de preços ou uma licitação convencional, mas a seqüência de atos pode variar conforme a estrutura organizacional de cada instituição. Porém, como estamos descrevendo um roteiro seria esta seqüência dos documentos que entendemos que devam constar nos autos de um processo de adesão:

¹ Disponível em: <http://www.agu.gov.br/sistemas/site/PaginasInternas/NormasInternas/AtoDetalhado.aspx?idAto=252289>

² FURTADO, Madeline Rocha. Instrução processual de adesão a Ata de Registro de Preços (ARP) - Autora: Madeline Rocha Furtado. Clubjus, Brasília/DF: 08 mar. 2010. Disponível em: <<http://www.clubjus.com.br/?artigos&ver=2.29655>>



DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS
Assessoria Jurídica

1. Documento inicial - Como todo processo de aquisição, deverá ser iniciado com um documento de solicitação/requisição do objeto, devidamente assinado pelo responsável/requisitante contendo as devidas justificativas da sua necessidade, conforme o seu planejamento.
(...)
2. Projeto Básico - PB ou Termo de Referência - TR: necessidade de descrição do objeto - especificação e detalhamento, lembrando que tais documentos deverão ser aprovados pela autoridade competente, conforme sua estrutura organizacional.
3. Pesquisa de preços: ampla pesquisa de preços no mercado; neste momento, já se verifica se existe algum preço registrado em Ata condizente com o objeto pretendido.
(...)
4. Ofício expedido ao órgão gerenciador da ARP: constatada a existência de preço registrador para solicitar a sua anuência à adesão pretendida.
5. Ofício expedido pelo órgão gerenciador: a anuência do órgão gerenciador à adesão propiciará ao carona a fundamentação necessária à instrução do processo, pois é ele (órgão gerenciador) quem conhece o fornecedor, tendo em vista que cabe a ele a administração da Ata e o comportamento do fornecedor quanto ao cumprimento das suas obrigações. Diante de tais informações oficiadas pelo órgão gerenciador ao carona, a Administração analisa a possibilidade de adesão à ARP.
6. Documento técnico emitido pelo requisitante: caberá à área requisitante analisar a especificação técnica do objeto registrado na ARP pretendida, considerando vários requisitos, como: qualidade e forma de entrega do objeto, e, atentando, principalmente, quanto ao cumprimento dos prazos de entrega estabelecidos no contrato, o que será verificado junto ao Órgão Gerenciador do registro de preços.
7. Documento emitido pela área de compras/contratos que demonstre a vantajosidade da adesão: ao verificar que a Ata encontrada no mercado atende às especificações definidas no Projeto/Termo de Referência pelo órgão aderente (carona) podemos efetivar a Adesão, lembrando que esta sempre estará condicionada à comprovação da vantajosidade do preço e demais requisitos técnicos, comparando-o àquele preço encontrado no mercado durante a pesquisa, observando ainda o prazo de vigência dessa ARP'-2 [Destacou-se]
9. Ademais, oportuno colacionar os dispositivos da Lei nº 8.666/1993 que disciplinam a matéria. Confira-se:
"Art. 1º Esta Lei estabelece normas gerais sobre licitações e contratos administrativos pertinentes a obras, serviços, inclusive de publicidade, compras, alienações e locações no âmbito dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios.

TADEU RODRIGO
TITO DE
OLIVEIRA:90345562
Assinado de forma digital
por TADEU RODRIGO TITO
DE OLIVEIRA:90345562
Dados: 2023.06.19 11:34:40
-03'00'



DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS
Assessoria Jurídica

Parágrafo único. Subordinam-se ao regime desta Lei, além dos órgãos da administração direta, os fundos especiais, as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

(...)

Seção V

Das Compras

Art. 14. Nenhuma compra será feita sem a adequada caracterização de seu objeto e indicação dos recursos orçamentários para seu pagamento, sob pena de nulidade do ato e responsabilidade de quem lhe tiver dado causa.

Art. 15. As compras, sempre que possível, deverão:

I - atender ao princípio da padronização, que imponha compatibilidade de especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas;

II - ser processadas através de sistema de registro de preços;

III - submeter-se às condições de aquisição e pagamento semelhantes às do setor privado;

IV - ser subdivididas em tantas parcelas quantas necessárias para aproveitar as peculiaridades do mercado, visando economicidade;

V - balizar-se pelos preços praticados no âmbito dos órgãos e entidades da Administração Pública;

(...)

Nas compras deverão ser observadas, ainda:

I - a especificação completa do bem a ser adquirido sem indicação de marca;

I - a definição das unidades e das quantidades a serem adquiridas em função do consumo e utilização prováveis, cuja estimativa será obtida, sempre que possível, mediante adequadas técnicas quantitativas de estimação;

III- as condições de guarda e armazenamento que não permitam a deterioração do material". [Destacou-se]

10. Constata-se, da leitura dos dispositivos legais acima citados, que as compras realizadas por órgãos públicos federais, seja em decorrência de procedimento licitatório, de contratação direta (dispensa e inexigibilidade) ou mesmo de adesão à Ata de Registro de Preços de outro órgão, deverão ser precedidas de prévio levantamento da necessidade do órgão contratante.

11. Em especial, colhe-se do art. 14 e do § 7º do art. 15, todos da Lei de Licitações, que nenhuma compra poderá ser feita sem a adequada caracterização de seu objeto, sendo oportuno colacionar ao processo administrativo, além da "especificação completa do bem a ser adquirido" a definição das unidades e quantidades pretendidas.



DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS
Assessoria Jurídica

12. Como antes dito, **a fase inicial do procedimento administrativo para adesão à Ata de Registro de Preços de outro Órgão guarda conformidade com o de uma licitação.** O processo de aquisição deverá, portanto, ser iniciado com uma solicitação/requisição do objeto, contendo as devidas justificativas de sua necessidade, de acordo com o planejamento do órgão. **Oportuno, ainda, instruir os autos com documento, elaborado pela área técnica competente, que contenha as especificações do objeto que se pretende adquirir, sem indicação de marca.** Numa terceira etapa, apenas, é que se deverá fazer uma ampla pesquisa de mercado a fim de estimar o valor da contratação e, conseqüentemente, verificar a existência de dotação orçamentária para fazer face à futura despesa.
- 13. Com efeito, é no momento da pesquisa de mercado (terceira etapa) que a Administração poderá examinar se há alguma Ata de Preços, de outros órgãos ou entidades, que guarde estrita consonância com o objeto que se pretende licitar.**
14. **Tenha-se presente que somente a partir da confecção do Termo de Referência é que se evidenciam todas as peculiaridades (especificações técnicas, quantitativos, etc) daquilo que a Administração pretende adquirir. Sem este instrumento não há como verificar se os itens da ata a que se pretende aderir realmente correspondem às reais necessidades do órgão.**
15. Sua elaboração, portanto, melhora o desempenho na execução dos projetos da Administração, na medida em que exige a descrição prévia do produto desejado, avaliação da qualidade, dos recursos necessários.
Exige, em suma, que haja um planejamento.
16. Não é demasiado lembrar que a exigência decorre, também, de normativo legal, consubstanciado no art. 3º, § 3º, do Decreto nº 3.931/013
- 17. Reitera-se, por sua relevância, que a verificação quanto à existência de ata de registro de preços de outro órgão em vigor deve ser ato posterior à constatação, pela administração, de suas reais necessidades de aquisição de determinado objeto, tudo devidamente justificado.** (Grifos nossos)

2.6 *In casu*, verifica-se que o Diretor de Informação e Dados desenvolveu o Termo de Referência da contratação (0105943), fez orçamentos com empresas distintas e buscou em atas de registro de preços e contratos para indicar o valor da contratação requerida (0106003, 0106004, 0106005, 0106007, 0106008, 0106011, 0106012, 0106016 e 0106017).

2.6.1 Após, identificou a Ata de Registro de Preço nº 31105/2022 do **INSTITUTO FEDERAL DE SANTA CATARINA**, com mesmo objeto pretendido e preços mais vantajosos para a Administração.



DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS
Assessoria Jurídica

2.7 Prosseguindo, face ao objeto, foi solicitada adesão à Ata de Registro de Preços nº 31105/2022 sendo a adesão autorizada conforme resposta constantes no documento 0105995.

2.7.1 Da mesma forma foi realizado o pedido de adesão ao fornecedor sendo aceita a adesão pela empresa **Advanta conectividade Inteligente** (0105947).

2.8. Em conformidade com o disposto no art. 3º, § 1º, do sobredito Decreto Estadual de Minas Gerais, a licitação para registro de preços deve ser realizada na modalidade concorrência ou pregão, do tipo menor preço, podendo ser utilizado o tipo técnica e preço, no primeiro caso.

2.9 Segundo se depreende da cópia do Edital (0106019), tal exigência foi observada pelo órgão gestor³, pois o Registro de Preço promovido pelo Instituto Federal de Santa Catarina Santo realizou a licitação na modalidade pregão eletrônico, do tipo menor preço.

2.10. Prosseguindo, o art. 8º do Decreto Estadual nº 46.311/2013 estabelece como condição para adesão ao Sistema de Registro de Preços, quanto ao órgão “não participante”, a prática dos mesmos atos necessários à adesão como órgão participante, *verbis*:

Art. 8º Ao órgão não participante do registro de preços aplicam-se, no que couber, as atribuições do órgão participante, previstas no art. 7º.

§ 1º O Termo de Adesão do órgão não participante deve ser dirigido ao órgão gerenciador, com indicação do objeto de seu interesse e da quantidade estimada para conhecimento e aprovação daquele órgão, aplicando-se, sempre que possível, o §3º do art. 5º.

³ Órgão Gerenciador: órgão ou entidade da Administração Pública responsável pela condução do conjunto de procedimentos para registro de preços e gerenciamento da ARP. (art. 2º, X, do Decreto Estadual n.º 46.311, de 16 de setembro de 2013).



DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS
Assessoria Jurídica

§ 2º A responsabilidade do órgão não participante é restrita às informações por ele produzidas, não respondendo por eventuais irregularidades do procedimento licitatório.

§ 3º O órgão gerenciador não responde por atos praticados pelo órgão não participante.

2.10.1. Ou seja, em face do dispositivo supratranscrito, aplica-se no que couber o estabelecido no art. 7º do Decreto Estadual.⁴

2.11. Outrossim, determina o artigo 19, no inciso I, do Decreto Estadual a necessidade de comprovação da vantagem a tal adesão.

Cumprindo a referida exigência da norma, o Diretor de Informação e Dados juntou a comprovação da pesquisa de mercado.

2.12. Quanto à formalização, pelo órgão não participante dos atos pertinentes ao procedimento para sua adesão ao registro de preços (art. 19, II c/c art. 8º, ambos do Decreto Estadual nº 46.311/2013), bem como sua aprovação pela autoridade competente. Verifica-se que

⁴ Art. 7º Caberá ao órgão participante do registro de preços:

I – fazer a análise de sua expectativa de consumo para os itens que pretenda incluir no registro de preços, no período previsto para vigência da ata;

II – manifestar, no prazo estipulado pelo órgão gerenciador, o interesse em participar do registro de preços, a ele providenciando o encaminhamento do termo de adesão, nos termos dos §§ 3º e 4º do art. 5º, contendo:

a) estimativa de consumo;

b) cronograma previsto para contratação; e

c) demais informações solicitadas;

III – sugerir itens a serem registrados e condições de contratação, quando for o caso;

IV – garantir que todos os atos inerentes ao procedimento para sua inclusão no registro de preços a ser realizado estejam devidamente formalizados e aprovados pela autoridade competente;

V – tomar conhecimento da ARP, inclusive das respectivas alterações porventura ocorridas, com o objetivo de assegurar o correto cumprimento de suas disposições; e

VI – indicar o gestor do contrato, a quem compete, além das atribuições previstas no art. 67 da Lei Federal nº 8.666, de 1993:

a) promover consulta prévia junto ao órgão gerenciador, quando da necessidade de contratação, a fim de obter a indicação do fornecedor, os respectivos quantitativos e os valores a serem praticados;

b) zelar pelos atos relativos ao cumprimento das obrigações contratualmente assumidas, inclusive pela aplicação de eventuais penalidades aos fornecedores, decorrentes do descumprimento de cláusulas contratuais, nos termos do art. 26; e

c) informar ao órgão gerenciador a eventual recusa do fornecedor em atender às condições estabelecidas no edital, firmadas na ARP, as divergências relativas à entrega, características e origem dos bens licitados, bem como a recusa em assinar o contrato para fornecimento ou prestação de serviços.

TADEU RODRIGO
TITO DE
OLIVEIRA:90345562

Assinado de forma digital
por TADEU RODRIGO TITO
DE OLIVEIRA:90345562
Dados: 2023.06.19
11:35:24 -03'00'



DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS
Assessoria Jurídica

tal providência foi adotada tendo a empresa fornecedora e o gestor acenado positivamente ao pleito. Foram juntadas, ainda, cópias do edital de licitação e da ARP (00106019 e 0105944).

2.13. Lado outro, verifica-se que foi atendido o requisito descrito no inciso III, do art. 19, do referido diploma legal, qual seja, observância da quantidade licitada do objeto constante da Ata.

2.14. Ademais, foi anexada comprovação de divulgação no portal da internet do aviso de intenção (0114345) com a antecedência necessária para a eventual impugnação, em cumprimento do § 1º do art. 20 do citado Decreto Estadual.

2.15. Registre-se que, no desenvolvimento do presente procedimento, exige-se, das autoridades e unidades administrativas integrantes da Defensoria Pública, a fiel observância dos dispositivos constantes do Decreto Estadual n.º 46.311/2013 e na Lei nº 8.666/93, bem como de outros diplomas legais pertinentes e aplicáveis, sob pena de responsabilidade administrativa, penal e civil.

2.16. Exige-se, ainda, das autoridades e funcionários administrativos competentes para a realização dos atos relacionados ao procedimento de registro de preços, a condução de suas atividades em conformidade com os princípios aplicáveis à licitação, bem como com os que regem a Administração Pública em geral, previstos constitucionalmente (art. 37), especialmente o da supremacia e indisponibilidade do interesse público, o da impessoalidade, o da moralidade e da probidade administrativa.

2.17. Em assim sendo, verifico nos autos que o Setor de Compras providenciou a instrução dos autos contendo a declaração de disponibilidade orçamentária e financeira (0112841) necessária e suficiente para cobrir as despesas com a contratação atestada pelos setores técnicos competentes. Foi ainda, obtido junto ao SIAD os relatórios (0114346, 0114347, 0114348, 0114350 e 0114353) e o mapa comparativo de preços, (0114351 e 0114352).

TADEU RODRIGO
TITO DE
OLIVEIRA:903455
62

Assinado de forma
digital por TADEU
RODRIGO TITO DE
OLIVEIRA:90345562
Dados: 2023.06.19
11:35:35 -03'00'



DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS
Assessoria Jurídica

2.18. No que concerne à habilitação jurídica, fiscal e trabalhista e econômico-financeira da contratada ADVANTA SISTEMAS DE TELECOMUNICACOES E SERVICOS DE INFORMATICA LTDA os documentos nº 0114375, 0114377, 0114770 comprovam a sua regularidade.

2.19. No que tange à minuta do ato de dispensa do instrumento contratual (0114781) verifico que foram expostos os motivos e as razões de direito para a dispensa do instrumento contratual.

III – CONCLUSÃO

3.1. Do exposto, consoante as razões anteriormente apontadas, concluo pela regularidade jurídica do procedimento administrativo em análise, em especial da adesão da Defensoria Pública à Ata de Registro de Preços nº 31105/2022, promovida pelo Instituto Federal de Santa Catarina, na qualidade de não participante, para a aquisição de solução de segurança de rede com gerenciamento e instalação com configuração.

Este é o parecer.

TADEU RODRIGO
TITO DE
OLIVEIRA:90345562

Assinado de forma digital por
TADEU RODRIGO TITO DE
OLIVEIRA:90345562
Dados: 2023.06.19 11:35:47
-03'00'



Autorização de fornecimento

Autorização de fornecimento nº: 000089

Processo: 1441003 000068/2023 Procedimento de contratação: Registro de preços não realizado no SIRP

Órgão ou entidade: DEFENSORIA PUBLICA DO ESTADO DE MINAS GERAIS

CNPJ: 05.599.094/0001-80

Unidade de compra: 1441003

DPMG / COMPRAS E CONTRATOS

Dados do empenho

Nº e ano do empenho	Data do empenho	Unid. contábil/executora	Unid. orçamentária	Nº do contrato
55/2023	27/06/2023	1440005	1441	0

Elemento-item de despesa: 5207 - EQUIPAMENTOS DE INFORMATICA

Fornecedor: 03.232.670/0001-21

ADVANTA SISTEMAS DE TELECOMUNICACOES E SERVICOS DE INFORMATICA LTDA.

Endereço:

AVENIDA COPACABANA, 325 - 18º ANDAR - SALAS 1810 A 1814 - DEZOITO DO FORTE EMPRESARIAL/ALPHAVILLE. - BARUERI - SP CEP: 06472-001

Telefones: (11) 4504-5900; (11) 4504-5902 5912

Banco: -

Agência: - Conta corrente: -

Unidade de pedido: 1441003 DPMG / COMPRAS E CONTRATOS

Local de entrega:

Rua da Bahia, 2277, Lourdes, Belo Horizonte

Nº do item da AF: 1

Local de entrega:

Rua da Bahia, 2277, Lourdes, Belo Horizonte

Item de material: 001910418

Especificação:

SOLUCAO GERENCIAMENTO DE EVENTOS DE SEGURANCA - CAPACIDADE: MINIMA 5GB DE LOGS DIARIOS; ARMAZENAMENTO: MINIMO 3 TB (AREA LIVRE PARA LOGS); INTERFACE: VNIC INTERFACES/PORTS; CONEXAO: APPLIANCE VIRTUAL (MAQUINA VIRTUAL);

Complementação da especificação do item de material - CATMAS

ESTE ITEM POSSUI ESPECIFICACAO LONGA ANEXADA NO CAMPO ARQUIVOS;
OBS: E
SSE ANEXO NAO APARECE NO RELATORIO DO ITEM, CONSULTAR O ITEM NO PORTAL DE COMPRAS.

Unid. aquisição / forneciment	Prazo de entrega (dias)	Garantia (meses)	Marca	Modelo	Frequência de entrega	Qtd.	Valor unitário (R\$)	Valor total (R\$)
UNIDADE	120	0	sem marca fabricante	-	Anual	1,0000	67511,0200	67511,02

Nº do item da AF: 2

Local de entrega:

Rua da Bahia, 2277, Lourdes, Belo Horizonte

Item de material: 001910434

Especificação:

FIREWALL (HARDWARE) - IDENTIFICACAO: APPLIANCE - SOLUCAO DE SEGURANCA DE FIREWALL NGFW; TAXA DE TRANSFERENCIA: 8.4 GBPS DE TRAFEGO SSL; CONEXAO: 16 INTERFACES 1 GIGABIT ETHERNET PADRAO 1000BASE; INTERFACE: 4 INTERFACES 10 GIGABIT ETHERNET PADRAO 10GBASE-X; COMPONENTE (4): SEM COMPONENTES; FONTE DE ALIMENTACAO: REDUNDANTE (HOT SWAPPABLE); TENSAO: BIVOLT AUTOMATICO;

Complementação da especificação do item de material - CATMAS

ESTE ITEM POSSUI ESPECIFICACAO ANEXADA NO CAMPO ARQUIVOS - (RELATORIO DO ITEM NAO TEM ANEXO, DEVE CONSULTAR O ITEM).

Unid. aquisição / forneciment	Prazo de entrega (dias)	Garantia (meses)	Marca	Modelo	Frequência de entrega	Qtd.	Valor unitário (R\$)	Valor total (R\$)
1,00 UNIDADE	120	0	sem marca fabricante	-	Anual	1,0000	343861,9100	343861,91

Valor total da autorização: R\$411.372,93

quatrocentos e onze mil trezentos e setenta e dois reais e noventa e três centavos

Valor da operação: _____
ICMS a recuperar: _____

SENHOR FORNECEDOR, não emitir cobrança bancária. Os nossos pagamentos são efetuados através de ordem de pagamento direto para sua conta corrente.

CONDIÇÕES GERAIS

As notas fiscais deverão ser emitidas em nome de:

Nome: Defensoria Pública do Estado de Minas Gerais
CNPJ: 05.599.094/0001-80 Telefones: 31 2522-8670
Endereço:
Rua dos Guajajaras, nº 1707, bairro Barro Preto, Belo Horizonte/MG

Observações:
-

Assistência técnica: -
Condições de pagamento: Integral - até 30 dias após o recebimento definitivo

A inadimplência por atraso na entrega do material acarretará, ao fornecedor, a aplicação de multa observados os seguintes limites:

- multa de 0.3% por dia, a partir do primeiro dia útil subsequente ao do vencimento do prazo para cumprimento da obrigação, até o trigésimo dia de atraso, sobre o valor do fornecimento não realizado;
- multa de 20% sobre o valor do fornecimento não realizado, a partir do primeiro dia útil subsequente ao do vencimento do prazo para cumprimento das obrigações, no caso de atraso superior a 30 (trinta) dias na entrega dos bens constantes do instrumento contratual, ou entrega de objeto com vícios ou defeitos ocultos que o torne impróprio ao uso a que é destinado, ou diminuem-lhe o valor ou, ainda, fora das especificações contratadas;
- multa de 0.3% por dia, pelo descumprimento de qualquer cláusula ou condição prevista no Edital ou instrumento equivalente e não discriminado nas alíneas anteriores, sobre o valor contratado, contada da comunicação da da Contratante (via internet, fax, correio etc.), até cessar a inadimplência.

Belo Horizonte, _____ de _____ de _____

LEONARDO BRUNO POSSA
ANDRADE:70005160

Assinado de forma digital por LEONARDO
BRUNO POSSA ANDRADE:70005160
Dados: 2023.06.27 14:22:51 -03'00'

Aprovação pela unidade responsável

Assinatura do fornecedor

Data: ____/____/____



Autorização de fornecimento

Autorização de fornecimento nº: 000090

Processo: 1441003 000068/2023 Procedimento de contratação: Registro de preços não realizado no SIRP

Órgão ou entidade: DEFENSORIA PUBLICA DO ESTADO DE MINAS GERAIS

CNPJ: 05.599.094/0001-80

Unidade de compra: 1441003

DPMG / COMPRAS E CONTRATOS

Dados do empenho

Nº e ano do empenho	Data do empenho	Unid. contábil/executora	Unid. orçamentária	Nº do contrato
56/2023	27/06/2023	1440005	1441	0

Elemento-item de despesa: 3016 - MATERIAL DE INFORMATICA

Fornecedor: 03.232.670/0001-21

ADVANTA SISTEMAS DE TELECOMUNICACOES E SERVICOS DE INFORMATICA LTDA.

Endereço:

AVENIDA COPACABANA, 325 - 18º ANDAR - SALAS 1810 A 1814 - DEZOITO DO FORTE EMPRESARIAL/ALPHAVILLE. - BARUERI - SP CEP: 06472-001

Telefones: (11) 4504-5900; (11) 4504-5902 5912

Banco: -

Agência: - Conta corrente: -

Unidade de pedido: 1441003 DPMG / COMPRAS E CONTRATOS

Local de entrega:

Rua da Bahia, 2277, Lourdes, Belo Horizonte

Nº do item da AF: 2

Local de entrega:

Rua da Bahia, 2277, Lourdes, Belo Horizonte

Item de material: 001726145

Especificação:

MODULO TRANSECTOR PARA FIBRA OPTICA - PADRAO: SPF+; CONECTOR: LC PADRAO SR 10GB; MODO DE OPERACAO: MULTIMODO FULL DUPLEX; DETALHES: NAO APLICAVEL;

Unid. aquisição / forneciment	Prazo de entrega (dias)	Garantia (meses)	Marca	Modelo	Frequência de entrega	Qtd.	Valor unitário (R\$)	Valor total (R\$)
1,00 UNIDADE	120	0	FORTINET	-	Anual	8,0000	946,2300	7569,84

Nº do item da AF: 1

Local de entrega:

Rua da Bahia, 2277, Lourdes, Belo Horizonte

Item de material: 001910027

Especificação:

MODULO TRANSECTOR PARA FIBRA OPTICA - PADRAO: SFP; CONECTOR: LC DUPLEX; MODO DE OPERACAO: DISTANCIA ATE 400 METROS PARA FIBRAS MULTIMODO; DETALHES: COMPATIVEL COM O PADRAO 1000BASE-SX;

Unid. aquisição / forneciment	Prazo de entrega (dias)	Garantia (meses)	Marca	Modelo	Frequência de entrega	Qtd.	Valor unitário (R\$)	Valor total (R\$)
1,00 UNIDADE	120	0	FORTINET	-	Anual	8,0000	487,0400	3896,32

Valor total da autorização: R\$11.466,16

onze mil quatrocentos e sessenta e seis reais e dezesseis centavos

Valor da operação: _____

ICMS a recuperar: _____

SENHOR FORNECEDOR, não emitir cobrança bancária. Os nossos pagamentos são efetuados através de ordem de pagamento direto para sua conta corrente.

LEONARDO BRUNO POSSA ANDRADE:7000516005160

Assinado de forma digital por LEONARDO BRUNO POSSA ANDRADE:7000516005160
Dados: 2023.06.27 14:21:14 -03'00'

CONDIÇÕES GERAIS

As notas fiscais deverão ser emitidas em nome de:

Nome: Defensoria Pública do Estado de Minas Gerais

CNPJ: 05.599.094/0001-80 Telefones: 31 2522-8670

Endereço:
Rua dos Guajajaras, nº 1707, bairro Barro Preto, Belo Horizonte/MG

Observações:
-

Assistência técnica: -
Condições de pagamento: Integral - até 30 dias após o recebimento definitivo

A inadimplência por atraso na entrega do material acarretará, ao fornecedor, a aplicação de multa observados os seguintes limites:

- multa de 0.3% por dia, a partir do primeiro dia útil subsequente ao do vencimento do prazo para cumprimento da obrigação, até o trigésimo dia de atraso, sobre o valor do fornecimento não realizado;
- multa de 20% sobre o valor do fornecimento não realizado, a partir do primeiro dia útil subsequente ao do vencimento do prazo para cumprimento das obrigações, no caso de atraso superior a 30 (trinta) dias na entrega dos bens constantes do instrumento contratual, ou entrega de objeto com vícios ou defeitos ocultos que o torne impróprio ao uso a que é destinado, ou diminuam-lhe o valor ou, ainda, fora das especificações contratadas;
- multa de 0.3% por dia, pelo descumprimento de qualquer cláusula ou condição prevista no Edital ou instrumento equivalente e não discriminado nas alíneas anteriores, sobre o valor contratado, contada da comunicação da da Contratante (via internet, fax, correio etc.), até cessar a inadimplência.

Belo Horizonte, _____ de _____ de _____

LEONARDO BRUNO POSSA
ANDRADE:70005160

Assinado de forma digital por LEONARDO
BRUNO POSSA ANDRADE:70005160
Dados: 2023.06.27 14:20:51 -03'00'

Aprovação pela unidade responsável

Assinatura do fornecedor

Data: ____/____/____



Ordem de serviço

Ordem de serviço nº: 000091

Processo: 1441003 000068/2023 Procedimento de contratação: Registro de preços não realizado no SIRP

Órgão ou entidade: DEFENSORIA PUBLICA DO ESTADO DE MINAS GERAIS

CNPJ: 05.599.094/0001-80

Unidade de compra: 1441003 - DPMG / COMPRAS E CONTRATOS

Dados do empenho

Nº e ano do empenho	Data do empenho	Unid. contábil/executora	Unid. orçamentária	Nº do contrato
330/2023	27/06/2023	1440011	1441	0

Elemento-item de despesa: 4002 - SERVICO DE TECNOLOGIA DA INFORMACAO

Fornecedor: 03.232.670/0001-21
ADVANTA SISTEMAS DE TELECOMUNICACOES E SERVICOS DE INFORMATICA LTDA.

Endereço:
AVENIDA COPACABANA, 325 - 18º ANDAR - SALAS 1810 A 1814 - DEZOITO DO FORTE EMPRESARIAL/ALPHAVILLE. - BARUERI - SP CEP: 06472-001

Telefones: (11) 4504-5900; (11) 4504-5902 5912

Banco: -

Agência: - Conta corrente: -

Unidade de pedido: 1441003 DPMG / COMPRAS E CONTRATOS

Endereço de entrega:
Rua da Bahia, 2277, Lourdes

Item de serviço: 000046000

Especificação:
SERVICO DE MONTAGEM, INSTALACAO, CONFIGURACAO E PADRONIZACAODE SOFTWARE E EQUIPAMENTO DA SOLUCAO DE DATACENTER

Demais informações necessárias para contratação:
CONFORME ATA DE RP.

Unid. aquisição / fornecimento	Frequência de entrega	Quantidade	Valor unitário (R\$)	Valor total (R\$)
1,00 UNIDADE	Anual	0,0000	0,0000	41129,63

Localidade: Belo Horizonte

Valor total da ordem de serviço: R\$ 41.129,63
quarenta e um mil cento e vinte e nove reais e sessenta e três centavos

SENHOR FORNECEDOR, não emitir cobrança bancária. Os nossos pagamentos são efetuados através de ordem de pagamento direto para sua conta corrente.

CONDIÇÕES GERAIS

As notas fiscais deverão ser emitidas em nome de:

Nome: Defensoria Pública do Estado de Minas Gerais

CNPJ: 05.599.094/0001-80 Telefones: 31 2522-8670

Endereço:
Rua dos Guajajaras, nº 1707, bairro Barro Preto, Belo Horizonte/MG

Observações:
-

O atraso na prestação do serviço acarretará ao fornecedor a aplicação de multa observados os seguintes limites:

- multa de 0.3% por dia, a partir do primeiro dia útil subsequente ao do vencimento do prazo para cumprimento da obrigação, até o trigésimo dia de atraso, sobre o valor do serviço não realizado;
- multa de 20% sobre o valor do serviço não realizado, a partir do primeiro dia útil subsequente ao do vencimento do prazo para cumprimento das obrigações, no caso de atraso superior a 30 (trinta) dias na prestação dos serviços constantes do instrumento contratual;
- multa de 0.3% por dia, pelo descumprimento de qualquer cláusula ou condição prevista no Edital ou instrumento equivalente e não discriminado nas alíneas anteriores, sobre o valor contratado, contada da comunicação da da Contratante (via internet, fax, correio etc.), até cessar a inadimplência.

Belo Horizonte, _____ de _____ de _____

LEONARDO BRUNO POSSA
ANDRADE:70005160

Assinado de forma digital por LEONARDO
BRUNO POSSA ANDRADE:70005160
Dados: 2023.06.27 14:22:04 -03'00'

Aprovação pela unidade responsável

Assinatura do fornecedor

Data: ____/____/____