

# Estudo Técnico Preliminar

## 1. Informações Básicas

Número do processo: 23292.030398/2022-96

## 2. Descrição da necessidade

Aquisição de equipamento e serviços para gerenciamento e segurança da rede LAN/WLAN.

Finalização do Projeto IFSC Conecta que contempla a substituição da rede sem fio do IFSC por uma nova solução com agregação de segurança de dados (switches e firewall).

## 3. Área requisitante

Área Requisitante	Responsável
Diretoria de Tecnologia da Informação e Comunicação	Evaristo Marcos de Quadros Júnior

## 4. Necessidades de Negócio

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).

No momento que este ETP está sendo elaborado, está sendo executado o Projeto IFSC Conecta. Este processo tem como objetivo a aquisição de equipamentos e serviços que permitam a finalização deste projeto, criando no IFSC um ambiente seguro para a gestão dos dados institucionais e utilização da rede sem fio por todos os usuários (alunos, professores e servidores).

## 5. Necessidades Tecnológicas

No momento que este ETP está sendo elaborado, está sendo executado o Projeto IFSC Conecta. 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 unid; para 06 unidades será necessário a aquisição de pontos de acesso, switches e injetores PoE).

Essa infraestrutura permitirá o gerenciamento local da rede sem fio, a gestão de segurança através da implementação de firewall. Esta estrutura permitirá a aquisição de solução de telefonia VoIP, que será atrelada ao firewall e permitirá um ambiente completo e seguro.

## **6. Demais requisitos necessários e suficientes à escolha da solução de TIC**

### **6.1. Requisitos de Negócio**

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).

### **6.2. Requisitos de Capacitação**

Repasse de conhecimento (hands on).

### **6.3. Requisitos Legais**

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).

### **6.4. Requisitos de Manutenção e Suporte Técnico**

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.

A CONTRATADA deverá disponibilizar suporte técnico em nível corporativo com, no mínimo, as seguintes características:

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.

### **6.5. Requisitos Temporais**

a) 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.

b) Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos.

### **6.6. Requisitos de Segurança e Privacidade**

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

### **6.7. Requisitos de Segurança da Informação**

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

### **6.8 - Requisitos de Sustentabilidade**

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

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);

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;

### **6.9. Requisitos de Segurança dos Dados e Informações**

a) É vedado o acesso da CONTRATADA aos dados hospedados na infraestrutura da CONTRATANTE, sem prévia e formal autorização desta;

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.

c) A CONTRATADA deverá assinar Termo de Compromisso de Manutenção de Sigilo, 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.

#### **6.10. Requisitos de Arquitetura Tecnológica**

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

#### **6.11. Requisitos de Implantação**

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.

#### **6.12. Requisitos de Garantia e Assistência Técnica**

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.

#### **6.13. Requisitos de Experiência Profissional**

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

#### **6.14. Requisitos de Capacidade Técnica**

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

#### **6.15. Requisitos de Compatibilidade Técnica**

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

## **7. Estimativa da demanda - quantidade de bens e serviços**

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

## **8. Levantamento de soluções**

O IFSC através do processo 23292.010214/2021-24 (PE 32/2021) fez a aquisição de solução de gerenciamento de rede e segurança, composta por switches, firewall/controladora, pontos de acesso, injetores PoE e software de gerenciamento e segurança. A solução adquirida foi da fabricante Fortinet. Através do processo 23292.010041/2022-36 (PE 31009/2022) esta solução foi ampliada através da aquisição de pontos de acesso e injetores PoE. Até o momento (24/10/2022) foram empenhados R\$ 2.973.765,00 em equipamentos e serviços.

Visando consolidar a implantação desta solução com a aquisição de equipamentos de firewall, switches e appliance de telefonia VoIP integrada à solução, é lançado este novo processo, mantendo a opção pela fabricante definida no processo 23292.010214/2021-24 (PE 32/2021).

LEI Nº 14.133, DE 1º DE ABRIL DE 2021 (Lei de Licitações e Contratos Administrativos)

Art. 40. O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:

V - atendimento aos princípios:

a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;

## 9. Análise comparativa de soluções

Não se aplica pela justificativa apresentada no item 8 - Levantamento de Soluções.

## 10. Registro de soluções consideradas inviáveis

Não se aplica pela justificativa apresentada no item 8 - Levantamento de Soluções.

## 11. Análise comparativa de custos (TCO)

Não se aplica pela justificativa apresentada no item 8 - Levantamento de Soluções.

## 12. Descrição da solução de TIC a ser contratada

Item	Descrição	
<b>LOTE/GRUPO 1: Solução de Gerenciamento de Rede, Telefonia e Segurança</b>		
1	<p>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.</p>	426731
	<p>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 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</p>	

2

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 2.4 GHz 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

393277

	<p>relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.</p>	
<p>3</p>	<p><b>SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE REDE E SEGURANÇA</b></p> <p>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 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 802.1 X, 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</p>	<p>27456</p>

	<p>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.</p>	
<p>4</p>	<p>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 esta 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 período de garantia.</p>	<p>27456</p>
	<p>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</p>	

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 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 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

5

393277

	<p>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.</p>	
<p>6</p>	<p>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 devera 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 devera 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 devera 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</p>	<p>27090</p>

	<p>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 horaria mínima de 8 horas;</p>	
<p>7</p>	<p>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 devera 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 devera 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 devera 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 horaria mínima de 8 horas;</p>	<p>27090</p>
	<p>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 devera 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</p>	

<p>8</p>	<p>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;</p>	<p>27090</p>
	<p>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. 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</p>	

<p>9</p>	<p>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 RIs 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;</p>	<p>27090</p>
<p>10</p>	<p>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-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</p>	<p>27090</p>

	<p>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 RLI 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;</p>	
<p>11</p>	<p>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 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 RLI 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;</p>	<p>27090</p>
	<p>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</p>	

<p>12</p>	<p>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 devera 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 devera 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 devera 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 horaria mínima de 8 horas;</p>	<p>27090</p>
<p>13</p>	<p>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,</p>	<p>27090</p>

	<p>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.</p>	
<p>14</p>	<p>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.</p>	<p>27090</p>
<p>15</p>	<p>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 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 – 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.</p>	<p>27090</p>

	<p>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.</p>	
<p>16</p>	<p>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. 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 disará apenas o número do ramal e o sistema proposto disará um número local ou celular. 56. O sistema proposto deve ser capaz de gerar</p>	<p>474397</p>

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.

**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

17	<p>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. 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</p>	474397
----	---	--------

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 (dezesseis) 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.

**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, suprindo 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)

<p>18</p>	<p>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 r RTP; 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;</p>	<p>474397</p>
<p>19</p>	<p>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 r RTP; 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;</p>	<p>474397</p>
	<p>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</p>	

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. 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

20

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

27456

/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.

**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 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

21

27456

(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 exporta-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.

**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 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 (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

22

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;

150100

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 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). 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.

**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 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

23

150100

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 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 exporta-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.

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 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

24

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

150100

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 suportar 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.

**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 (dezesseis) 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 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; 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

25

150100

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 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 compoñham 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

	<p>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.</p>	
<p>26</p>	<p>SWITCH TIPO 1 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA Características Mínimas:</p> <ol style="list-style-type: none"> <li>1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;</li> <li>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);</li> <li>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;</li> <li>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;</li> <li>5. Deve possuir 1 (uma) interface USB;</li> <li>6. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo);</li> <li>7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;</li> <li>8. Deve possuir tabela MAC com suporte a 32.000 endereços;</li> <li>9. Deve operar com latência igual ou inferior à 1us (microsegundo);</li> <li>10. 8. Deve implementar Flow Control baseado no padrão IEEE 802.3X;</li> <li>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);</li> <li>12. 10. Deve suportar a comutação de Jumbo Frames;</li> <li>13. 11. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;</li> <li>14. 12. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;</li> <li>15. 10.13. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;</li> <li>16. 14. Deve implementar serviço de DHCP Relay;</li> <li>17. 15. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (um mil) entradas na tabela;</li> <li>18. 16. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);</li> <li>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;</li> <li>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;</li> <li>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;</li> <li>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 umBPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;</li> <li>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;</li> <li>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;</li> <li>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;</li> <li>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;</li> <li>27. 25. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;</li> <li>28. 26. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);</li> <li>29. 27. Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;</li> <li>28. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;</li> <li>30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;</li> <li>31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;</li> <li>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;</li> <li>33. 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;</li> <li>34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;</li> <li>35. Deve suportar MAC Authentication Bypass (MAB);</li> <li>36. Deve implementar RADIUS CoA (Change of Authorization);</li> <li>37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;</li> <li>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</li> </ol>	<p>463274</p>

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.

**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 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

27	<p>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</p>	463274
----	--	--------

<p>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.</p>	
<p><b>SWITCH TIPO 4 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA</b> Características Mínimas:</p> <ol style="list-style-type: none"> <li>1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;</li> <li>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);</li> <li>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;</li> <li>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;</li> <li>5. Deve possuir 1 (uma) interface USB;</li> <li>6. Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo);</li> <li>7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;</li> <li>8. Deve possuir tabela MAC com suporte a 32.000 endereços;</li> <li>9. Deve operar com latência igual ou inferior à 1us (microsegundo);</li> <li>10. Deve implementar Flow Control baseado no padrão IEEE 802.3X;</li> <li>11. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);</li> <li>12. Deve suportar a comutação de Jumbo Frames;</li> <li>13. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;</li> <li>14. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;</li> <li>15. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;</li> <li>16. Deve implementar serviço de DHCP Relay;</li> <li>17. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;</li> <li>18. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);</li> <li>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;</li> <li>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;</li> <li>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;</li> <li>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;</li> <li>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;</li> <li>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;</li> <li>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;</li> <li>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;</li> <li>27. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;</li> <li>28. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);</li> <li>29. Deverá implementar priorização de tráfego baseada nos valores do campo</li> </ol>	

<p>28</p>	<p>"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; 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 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).</p>	<p>463274</p>
	<p>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</p>	

29

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 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

448242

	<p>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.</p>	
30	<p>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. 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</p>	27456

	<p>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;</p>	
31	<p>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 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 entrado. 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;</p>	453584
32	<p>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).</p>	150812
33	<p>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).</p>	150812
34	<p>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</p>	150812

	desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).	
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

### 13. Estimativa de custo total da contratação

**Valor (R\$):** 9.525.948,98

As cotações a seguir foram selecionadas com base na diferença de 35% entre o maior e o menor preço, considerando o intervalo de preços. O valor de 35% é uma orientação do Departamento de Compras do IFSC.

- Checklist das cotações:
  - Período de realização da pesquisa de mercado: 05/10/2022 a 14/10/2022;
  - Fontes de cotação: Painel de Preços, Internet e fornecedor;
  - Empresas consultadas:
    - Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. - CNPJ: 03.232.670/0001-21;
    - Sigmafone Telecomunicações LTDA. - CNPJ: 78.766.151/0001-42;
    - Clear Tecnologia da Informação LTDA. - CNPJ: 30.088.923/0001-08.
- Foram utilizados preços públicos e privados para referência atualizada de preço e/ou por não apresentar o mesmo objeto licitado no Painel de Preços (preço público).
- As cotações foram realizadas pela área requisitante representada por Benoni de Oliveira Pires – Analista de TIC, lotado e em exercício na Diretoria de Tecnologia da Informação e Comunicação. No momento da elaboração deste ETP o mesmo é ocupante do cargo de Diretor de TIC.
  
- Foram utilizados como requisitos de busca (Serviços/Ponto de Acesso Indoor/Outdoor):
  - Ano: 2021/2022
  - Serviço: 27090
  - Nome do material (PDM): PONTO DE ACESSO

Fonte	Item 1	Item 2	Item 3
Painel de Preços Fornecedor	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 1.281,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 8.205,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 240.914,00 - 05/10/2022
	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 1.332,24 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 8.451,15 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 250.550,56 - 11/10/2022
	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 1.310,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 8.370,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 248.600,00 - 14/10/2022
		UASG 290002 – PE 101/2021 – R\$ 7.454,00 Relatório gerado dia: 13/10/2022 às 14:59 Fonte: paineldeprecos.planejamento.gov.br	
		UASG 925125 – PE 43/2021 – R\$ 9.300,00 Relatório gerado dia: 13/10/2022 às 14:59 Fonte: paineldeprecos.planejamento.gov.br	
		UASG 158143 – PE 13/2021 – R\$ 11.256,00	

	Relatório gerado dia: 13/10/2022 às 14:59 Fonte: paineldeprecos.planejamento.gov.br	
<b>R\$ 1.307,74</b>	<b>R\$ 8.839,36</b>	<b>R\$ 246.688,18</b>

- Foram utilizados como requisitos de busca (Serviços/Ponto de Acesso Outdoor):
  - Ano: 2021/2022
  - Serviço: 27090
  - Nome do material (PDM): PONTO DE ACESSO

Fonte	Item 4	Item 5	Item 6
Painel de Preços Fornecedor	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 320,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 12.416,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 16.240,00 - 05/10/2022
	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 336,00 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 12.664,32 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 16.727,20 - 11/10/2022
	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 327,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 12.560,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 16.585,00 - 14/10/2022
		UASG 925125 – PE 43/2021 – R\$ 11.000,00 Relatório gerado dia: 13/10/2022 às 15:38 Fonte: paineldeprecos.planejamento.gov.br	UASG 070019 – PE 35/2021 – R\$ 16.000,00 Relatório gerado dia: 13/10/2022 às 17:11 Fonte: paineldeprecos.planejamento.gov.br
		UASG 160070 – PE 28/2021 – R\$ 17.249,00 Relatório gerado dia: 13/10/2022 às 15:38 Fonte: paineldeprecos.planejamento.gov.br	UASG 194007 – PE 06/2021 – R\$ 17.564,00 Relatório gerado dia: 13/10/2022 às 17:11 Fonte: paineldeprecos.planejamento.gov.br
			UASG 153137 – PE 20/2021 – R\$ 17.600,00 Relatório gerado dia: 13/10/2022 às 17:11 Fonte: paineldeprecos.planejamento.gov.br
	<b>R\$ 327,67</b>	<b>R\$ 13.128,2</b>	<b>R\$ 16.786,03</b>

- Foram utilizados como requisitos de busca (Serviços):
  - Ano: 2021/2022
  - Serviço: 27090

Fonte	Item 7	Item 8	Item 9
Painel de Preços Fornecedor	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 25.678,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 4.243,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 6.669,00 - 05/10/2022
	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 26.705,12 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 4.370,29 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 7.002,45 - 11/10/2022
	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 26.270,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 4.305,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 6.894,00 - 14/10/2022
	UASG 158516 – PE 105/2021 – R\$ 22.555,09 Relatório gerado dia: 13/10/2022 às 17:14 Fonte: paineldeprecos.planejamento.gov.br	UASG 158132 – PE 42/2021 – R\$ 4.150,00 Relatório gerado dia: 13/10/2022 às 17:17 Fonte: paineldeprecos.planejamento.gov.br	UASG 160020 – PE 02/2022 – R\$ 6.125,00 Relatório gerado dia: 13/10/2022 às 17:17 Fonte: paineldeprecos.planejamento.gov.br
	UASG 155341 – PE 13/2021 – R\$ 24.190,40 Relatório gerado dia: 13/10/2022 às 17:14 Fonte: paineldeprecos.planejamento.gov.br	UASG 070019 – PE 35/2021 – R\$ 5.000,00 Relatório gerado dia: 13/10/2022 às 17:17 Fonte: paineldeprecos.planejamento.gov.br	UASG 240127 – PE 72/2021 – R\$ 6.470,00 Relatório gerado dia: 13/10/2022 às 17:17 Fonte: paineldeprecos.planejamento.gov.br
	UASG 160091 – PE 11/2021 – R\$ 30.000,00 Relatório gerado dia: 13/10/2022 às 17:14 Fonte: paineldeprecos.planejamento.gov.br		UASG 070019 – PE 35/2021 – R\$ 7.000,00 Relatório gerado dia: 13/10/2022 às 17:17 Fonte: paineldeprecos.planejamento.gov.br
	<b>R\$ 25.899,76</b>	<b>R\$ 4.413,66</b>	<b>R\$ 6.693,41</b>

- Foram utilizados como requisitos de busca (Serviços):
  - Ano: 2021/2022
  - Serviço: 27090

Fonte	Item 10	Item 11	Item 12
Painel de Preços Fornecedor	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 16.783,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 51.888,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 15.141,00 - 05/10/2022
	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 17.622,15 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 53.963,52 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 15.595,23 - 11/10/2022
	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 18.320,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 52.530,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 16.320,00 - 14/10/2022
	UASG 740014 – PE 07/2021 – R\$ 18.664,00 Relatório gerado dia: 13/10/2022 às 17:22 Fonte: paineldeprecos.planejamento.gov.br	UASG 120195 – PE 336/2021 – R\$ 44.990,00 Relatório gerado dia: 13/10/2022 às 17:25 Fonte: paineldeprecos.planejamento.gov.br	UASG 120195 – PE 336/2021 – R\$ 15.000,00 Relatório gerado dia: 13/10/2022 às 17:31 Fonte: paineldeprecos.planejamento.gov.br
	UASG 070019 – PE 35/2021 – R\$ 20.100,00 Relatório gerado dia: 13/10/2022 às 17:22 Fonte: paineldeprecos.planejamento.gov.br	UASG 765700 – PE 03/2021 – R\$ 62.200,00 Relatório gerado dia: 13/10/2022 às 17:25 Fonte: paineldeprecos.planejamento.gov.br	UASG 070019 – PE 35/2021 – R\$ 16.000,00 Relatório gerado dia: 13/10/2022 às 17:31 Fonte: paineldeprecos.planejamento.gov.br
		UASG 120633 – PE 88/2021 – R\$ 77.683,32 Relatório gerado dia: 13/10/2022 às 17:25 Fonte: paineldeprecos.planejamento.gov.br	UASG 194007 – PE 06/2021 – R\$ 17.564,00 Relatório gerado dia: 13/10/2022 às 17:31 Fonte: paineldeprecos.planejamento.gov.br
	<b>R\$ 18.297,83</b>	<b>R\$ 57.209,14</b>	<b>R\$ 15.936,70</b>

- Foram utilizados como requisitos de busca (Serviços):
  - Ano: 2021/2022
  - Serviço: 27090

Fonte	Item 13	Item 14	Item 15
Painel de Preços Fornecedor	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 24.126,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 13.371,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 22.723,00 - 05/10/2022
	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 25.091,04 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 13.905,84 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 23.631,92 - 11/10/2022
	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 24.800,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 13.500,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 25.600,00 - 14/10/2022
	UASG 160486 – DL 113/2021 – R\$ 20.199,00 Relatório gerado dia: 13/10/2022 às 17:40 Fonte: paineldeprecos.planejamento.gov.br	UASG 150182 – DL 201/2021 – R\$ 11.980,00 Relatório gerado dia: 13/10/2022 às 17:46 Fonte: paineldeprecos.planejamento.gov.br	UASG 070019 – PE 35/2021 – R\$ 20.100,00 Relatório gerado dia: 13/10/2022 às 17:49 Fonte: paineldeprecos.planejamento.gov.br
	UASG 158516 – PE 105/2021 – R\$ 22.555,09 Relatório gerado dia: 13/10/2022 às 17:40 Fonte: paineldeprecos.planejamento.gov.br	UASG 741000 – DL 128/2022 – R\$ 12.000,00 Relatório gerado dia: 13/10/2022 às 17:46 Fonte: paineldeprecos.planejamento.gov.br	UASG 160486 – DL 113/2021 – R\$ 20.199,00 Relatório gerado dia: 13/10/2022 às 17:49 Fonte: paineldeprecos.planejamento.gov.br
	UASG 155341 – DL 13/2021 – R\$ 24.190,40 Relatório gerado dia: 13/10/2022 às 17:40 Fonte: paineldeprecos.planejamento.gov.br	UASG 090011 – PE 15/2021 – R\$ 13.474,40 Relatório gerado dia: 13/10/2022 às 17:46 Fonte: paineldeprecos.planejamento.gov.br	UASG 155341 – DL 13/2021 – R\$ 24.190,40 Relatório gerado dia: 13/10/2022 às 17:49 Fonte: paineldeprecos.planejamento.gov.br
	<b>R\$ 23.493,59</b>	<b>R\$ 13.038,54</b>	<b>R\$ 22.740,72</b>

Fonte	Item 16	Item 17	Item 18
Fornecedor	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 39.795,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 31.398,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 37.754,00 - 05/10/2022
	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 40.988,85 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 32.967,90 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 40.019,24 - 11/10/2022
	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08

R\$ 40.660,00 - 14/10/2022	R\$ 32.080,00 - 14/10/2022	R\$ 39.780,00 - 14/10/2022
<b>R\$ 40.481,28</b>	<b>R\$ 32.148,63</b>	<b>R\$ 39.184,41</b>

Fonte	Item 19	Item 20	Item 21
Fornecedor	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 29.543,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 81.683,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 229.755,00 - 05/10/2022
	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 30.724,72 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 84.133,49 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 236.647,65 - 11/10/2022
	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 31.230,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 82.324,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 233.160,00 - 14/10/2022
	<b>R\$ 30.499,24</b>	<b>R\$ 82.713,49</b>	<b>R\$ 23.3187,55</b>

- Foram utilizados como requisitos de busca (Solução de Gerenciamento de Redes e Segurança):
  - Ano: 2021/2022
  - Nome do material (PDM): FIREWALL

Fonte	Item 22	Item 23	Item 24
Painel de Preços Fornecedor	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 34.091,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 79.506,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 241.702,00 - 05/10/2022
	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 35.113,73 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 81.891,18 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 251.370,08 - 11/10/2022
	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 34.800,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 82.900,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 248.300,00 - 14/10/2022
	UASG 927045 – PE 01/2021 – R\$ 35.000,00 Relatório gerado dia: 13/10/2022 às 15:57 Fonte: paineldeprecos.planejamento.gov.br	UASG 925473 – PE 01/2021 – R\$ 61.300,00 Relatório gerado dia: 13/10/2022 às 16:06 Fonte: paineldeprecos.planejamento.gov.br	UASG 158515 – PE 09/2021 – R\$ 194.666,68 Relatório gerado dia: 13/10/2022 às 16:23 Fonte: paineldeprecos.planejamento.gov.br
	UASG 168003 – PE 04/2022 – R\$ 35.500,00 Relatório gerado dia: 13/10/2022 às 15:57 Fonte: paineldeprecos.planejamento.gov.br	UASG 168003 – PE 04/2022 – R\$ 62.000,00 Relatório gerado dia: 13/10/2022 às 16:06 Fonte: paineldeprecos.planejamento.gov.br	UASG 925473 – PE 01/2022 – R\$ 238.515,00 Relatório gerado dia: 13/10/2022 às 16:23 Fonte: paineldeprecos.planejamento.gov.br
	UASG 030100 – PE 42/2021 – R\$ 40.000,00 Relatório gerado dia: 13/10/2022 às 15:57 Fonte: paineldeprecos.planejamento.gov.br	UASG 158154 – PE 5712/2022 – R\$ 66.000,00 Relatório gerado dia: 13/10/2022 às 16:06 Fonte: paineldeprecos.planejamento.gov.br	UASG 926426 – PE 11/2021 – R\$ 239.780,48 Relatório gerado dia: 13/10/2022 às 16:23 Fonte: paineldeprecos.planejamento.gov.br
	UASG 070021 – PE 20/2021 – R\$ 43.480,21 Relatório gerado dia: 13/10/2022 às 15:57 Fonte: paineldeprecos.planejamento.gov.br	UASG 030100 – PE 42/2021 – R\$ 90.000,00 Relatório gerado dia: 13/10/2022 às 16:06 Fonte: paineldeprecos.planejamento.gov.br	UASG 451116 – PE 16/2022 – R\$ 282.647,10 Relatório gerado dia: 13/10/2022 às 16:23 Fonte: paineldeprecos.planejamento.gov.br
	<b>R\$ 36.854,99</b>	<b>R\$ 74.799,59</b>	<b>R\$ 242.425,90</b>

- Foram utilizados como requisitos de busca (Solução de Gerenciamento de Redes e Segurança/switches):
  - Ano: 2021/2022
  - Nome do material (PDM): FIREWALL
  - Nome do material (PDM): SWITCH

Fonte	Item 25	Item 26	Item 27
Painel de Preços Fornecedor	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 551.300,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 8.479,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 19.296,00 - 05/10/2022
	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 567.839,00 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 9.072,53 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 20.260,80 - 11/10/2022

Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 555.945,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 9.730,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 19.730,00 - 14/10/2022
UASG 154080 – PE 05/2021 – R\$ 580.000,00 Relatório gerado dia: 13/10/2022 às 16:29 Fonte: paineldeprecos.planejamento.gov.br	UASG 254445 – PE 86/2021 – R\$ 8.573,75 Relatório gerado dia: 13/10/2022 às 12:35 Fonte: paineldeprecos.planejamento.gov.br	UASG 742050 – PE 80/2021 – R\$ 17.996,99 Relatório gerado dia: 13/10/2022 às 12:42 Fonte: paineldeprecos.planejamento.gov.br
UASG 030100 – PE 42/2022 – R\$ 625.000,00 Relatório gerado dia: 13/10/2022 às 16:29 Fonte: paineldeprecos.planejamento.gov.br	UASG 158154 – PE 2712/2021 – R\$ 8.951,93 Relatório gerado dia: 13/10/2022 às 12:35 Fonte: paineldeprecos.planejamento.gov.br	UASG 160219 – PE 07/2021 – R\$ 18.000,00 Relatório gerado dia: 13/10/2022 às 12:42 Fonte: paineldeprecos.planejamento.gov.br
UASG 926426 – PE 11/2021 – R\$ 643.461,54 Relatório gerado dia: 13/10/2022 às 16:29 Fonte: paineldeprecos.planejamento.gov.br	UASG 110322 – PE 21/2021 – R\$ 9.000,00 Relatório gerado dia: 13/10/2022 às 12:35 Fonte: paineldeprecos.planejamento.gov.br	UASG 160098 – PE 24/2021 – R\$ 19.438,00 Relatório gerado dia: 13/10/2022 às 12:42 Fonte: paineldeprecos.planejamento.gov.br
UASG 158143 – PE 08/2022 – R\$ 729.300,22 Relatório gerado dia: 13/10/2022 às 16:29 Fonte: paineldeprecos.planejamento.gov.br	UASG 158195 – PE 12/2021 – R\$ 9.620,00 Relatório gerado dia: 13/10/2022 às 12:35 Fonte: paineldeprecos.planejamento.gov.br	
<b>R\$ 607.549,39</b>	<b>R\$ 9.061,03</b>	<b>R\$ 19.120,30</b>

- Foram utilizados como requisitos de busca (serviço de instalação e configuração):

- Ano: 2021/2022
- Nome do material (PDM): SWITCH

Fonte	Item 28	Item 29	Item 30
Painel de Preços Fornecedor	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 14.691,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 25.151,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 3.347,00 - 05/10/2022
	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 15.572,46 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 26.660,06 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 3.614,76 - 11/10/2022
	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 15.260,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 25.990,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 3.840,00 - 14/10/2022
	UASG 459931 – PE 03/2021 – R\$ 13.900,00 Relatório gerado dia: 13/10/2022 às 12:42 Fonte: paineldeprecos.planejamento.gov.br	UASG 925387 – PE 43/2022 – R\$ 24.500,00 Relatório gerado dia: 13/10/2022 às 12:42 Fonte: paineldeprecos.planejamento.gov.br	
	UASG 160098 – PE 24/2020 – R\$ 14.696,00 Relatório gerado dia: 13/10/2022 às 12:42 Fonte: paineldeprecos.planejamento.gov.br	UASG 925603 – PE 20/2021 – R\$ 25.000,00 Relatório gerado dia: 13/10/2022 às 12:42 Fonte: paineldeprecos.planejamento.gov.br	
	UASG 926208 – PE 02/2022 – R\$ 15.000,00 Relatório gerado dia: 13/10/2022 às 12:42 Fonte: paineldeprecos.planejamento.gov.br	UASG 113601 – PE 08/2021 – R\$ 26.000,00 Relatório gerado dia: 13/10/2022 às 12:42 Fonte: paineldeprecos.planejamento.gov.br	
		UASG 200331 – PE 01/2022 – R\$ 26.550,00 Relatório gerado dia: 13/10/2022 às 12:42 Fonte: paineldeprecos.planejamento.gov.br	
	<b>R\$ 14.853,24</b>	<b>R\$ 25.693,00</b>	<b>R\$ 3.600,58</b>

- Foram utilizados como requisitos de busca (serviço de instalação e configuração):

- Ano: 2021/2022
- Nome do material (PDM): TRANSCEIVER
- Nome do material (PDM): TELEFONE VOIP - sem retorno da busca.

Fonte	Item 31	Item 32	Item 33
Painel de Preços Fornecedor	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 1.772,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 864,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 2.644,00 - 05/10/2022
	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 1.825,16 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 898,56 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 2.723,32 - 11/10/2022
	Clear Tecnologia da Informação LTDA.	Clear Tecnologia da Informação LTDA.	Clear Tecnologia da Informação LTDA.

CNPJ: 30.088.923/0001-08 R\$ 1.825,16 - 14/10/2022	CNPJ: 30.088.923/0001-08 R\$ 881,00 - 14/10/2022	CNPJ: 30.088.923/0001-08 R\$ 2.765,00 - 14/10/2022
	UASG 927248 – PE 34/2021 – R\$ 1.220,00 Relatório gerado dia: 13/10/2022 às 12:01 Fonte: paineldeprecos.planejamento.gov.br	UASG 090019 – PE 15/2021 – R\$ 2.217,00 Relatório gerado dia: 13/10/2022 às 12:08 Fonte: paineldeprecos.planejamento.gov.br
	UASG 158516 – PE 32/2021 – R\$ 1.000,00 Relatório gerado dia: 13/10/2022 às 12:01 Fonte: paineldeprecos.planejamento.gov.br	UASG 113601 – PE 08/2021 – R\$ 2.250,00 Relatório gerado dia: 13/10/2022 às 12:08 Fonte: paineldeprecos.planejamento.gov.br
		UASG 080025 – PE 23/2021 – R\$ 2.280,00 Relatório gerado dia: 13/10/2022 às 12:08 Fonte: paineldeprecos.planejamento.gov.br
<b>R\$ 1.807,44</b>	<b>R\$ 972,71</b>	<b>R\$ 2.479,88</b>

- Foram utilizados como requisitos de busca (serviço de instalação e configuração):
  - Ano: 2021/2022
  - Nome do material (PDM): TRANSCEIVER

Fonte	Item 34	Item 35
Painel de Preços Fornecedor	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 420,00 - 05/10/2022	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA. CNPJ: 03.232.670/0001-21 R\$ 934,00 - 05/10/2022
	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 432,60 - 11/10/2022	Sigmafone Telecomunicações LTDA. CNPJ: 78.766.151/0001-42 R\$ 980,70 - 11/10/2022
	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 458,00 - 14/10/2022	Clear Tecnologia da Informação LTDA. CNPJ: 30.088.923/0001-08 R\$ 965,00 - 14/10/2022
	UASG 158516 – PE 32/2021 – R\$ 530,00 Relatório gerado dia: 13/10/2022 às 12:16 Fonte: paineldeprecos.planejamento.gov.br	UASG 925045 – PE 92/2021 – R\$ 786,42 Relatório gerado dia: 13/10/2022 às 12:53 Fonte: paineldeprecos.planejamento.gov.br
	UASG 926306 – PE 32/2021 – R\$ 600,00 Relatório gerado dia: 13/10/2022 às 12:16 Fonte: paineldeprecos.planejamento.gov.br	UASG 158516 – PE 32/2021 – R\$ 1.100,00 Relatório gerado dia: 13/10/2022 às 12:53 Fonte: paineldeprecos.planejamento.gov.br
	<b>R\$ 488,12</b>	<b>R\$ 953,22</b>

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
<b>LOTE/GRUPO 1: Solução de Gerenciamento de Rede, Telefonia e Segurança</b>					
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		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 SEGURANÇA PARA CAMPUS TIPO 3	UNIDADE	15	36.854,99	552.824,85
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

#### 14. Justificativa técnica da escolha da solução

Não se aplica pela justificativa apresentada no item 8 - Levantamento de Soluções.

#### 15. Justificativa econômica da escolha da solução

- Eficácia: Atendimento às normas de segurança no tratamento de dados;
- Eficiência: Infraestrutura de dados protegida;
- Efetividade: Redundância na proteção de dados;
- Economicidade: Economia a partir de compra planejada.

## 16. Parcelamento da Solução

A solução será agrupada em lote único 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;) Os equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste processo.

## 17. Benefícios a serem alcançados com a contratação

Implantação de infraestrutura de dados e telefonia integrada, segura e com redundância.

## 18. Providências a serem Adotadas

Dar prosseguimento à contratação com a licitação dos materiais e serviços deste projeto.

## 19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

### 19.1. Justificativa da Viabilidade

O projeto é viável tecnologicamente e financeiramente. Faz parte da conclusão do projeto "Conecta IFSC".

## 20. Responsáveis

EVARISTO MARCOS DE QUADROS JUNIOR

Integrante Requisitante

KARI DE SOUZA SOARES

Integrante Técnico

BENONI DE OLIVEIRA PIRES

Diretor de TIC