

Processo nº 00100.000273/2020-88

1. INTRODUÇÃO

1.1. A presente análise tem por objetivo demonstrar a viabilidade técnica e econômica da solução para proteção de perímetro e conectividade de redes de dados e armazenamento, com suporte, treinamento e garantia, subsidiando o planejamento da contratação com informações de caráter técnico e cenários de resolução das necessidades de negócio do ITI.

2. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

2.1. Histórico do órgão

2.1.1. A infraestrutura do ITI é composta por ambientes de rede diversos, contemplando ambientes cabeado e sem fios, em múltiplas localidades.

2.1.2. Os ambientes gerenciados pela Coordenação Tecnologia da Informação e Comunicações - COTIC utilizam tecnologias de proteção de perímetro de redes precários, baseados em sua maioria por *softwares* gratuitos, com limitação de visualização de ataques, alertas e técnicas de mitigação de ataques contra a infraestrutura cabeada e sem fios da autarquia. Não obstante, os equipamentos utilizados como firewall não são dedicados, o que onera recursos de processamento e rede para manter o ativo em funcionamento. Além disso, a infraestrutura da rede sem fios da autarquia é demasiadamente defasada, impossibilitando adotar as práticas mais adequadas para manter o perímetro de segurança de rede seguro.

2.1.3. Atualmente o ITI conta com aproximadamente 180 usuários - sem contas de serviços-, 150 máquinas virtuais e 2 ambientes de processamento de dados, além de 15 pontos de acesso (access points), controladora e *firewalls* lógicos. Na disposição atual, ambos os ativos de delimitação de perímetro de rede estão suscetíveis a falha, gerando assim o risco de descontinuidade da comunicação da rede do ITI para seus usuários internos e externos.

2.1.4. A Medida Provisória nº 983, de 16 de julho de 2020, que “dispõe sobre as assinaturas eletrônicas em comunicações com entes públicos e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos”, amplia a missão do Instituto Nacional de Tecnologia da Informação, incluindo sua atuação “em atividades dos órgãos e entidades da administração direta, autárquica e fundacional dos Poderes e órgãos constitucionalmente autônomos dos entes federativos relacionadas à criptografia, às assinaturas e identificações eletrônicas e às tecnologias correlatas, inclusive àquelas relativas às assinaturas eletrônicas simples e avançadas.” O parágrafo único do Art. 5º, diz ainda que essa atuação abrangerá:

I - a realização de pesquisas;

II - a execução de atividades operacionais;

III - a prestação de serviços no âmbito dos entes públicos de que trata o **caput**, ressalvadas as competências específicas de outros órgãos e entidades;

IV - o fornecimento de assinaturas eletrônicas avançadas a pessoas naturais e a pessoas jurídicas para uso nos sistemas de entes públicos de que trata o **caput**; e

V - a edição de normas em seu âmbito de atuação.

2.1.5. Nesse sentido, e sob demanda do Ministério da Economia, este instituto está também conduzindo projeto de implantação de uma nova infraestrutura específica, dedicada e segregada da AC Raiz da ICP-Brasil, para viabilizar o fornecimento e uso de assinaturas eletrônicas avançadas no âmbito das necessidades do Governo Federal.

2.2. Identificação das necessidades de negócio

2.2.1. O Instituto Nacional de Tecnologia da Informação – ITI é uma autarquia federal criada pelo art. 12 da Medida Provisória no 2.200-2, de 24 de agosto de 2001, com sede e foro no Distrito Federal, vinculada à Casa Civil da Presidência da República e que tem por missão manter e executar as políticas da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil. Ao ITI compete ainda ser a primeira autoridade da cadeia de certificação digital – AC Raiz.

2.2.2. Para dar cumprimento às suas competências, o ITI conta com as áreas de negócio que compõem a sua estrutura organizacional. Dentre estas, cabe à Diretoria de Infraestrutura de Chaves Públicas - DINFRA, através da Coordenação de Tecnologia da Informação e Comunicações – COTIC, a definição, o planejamento, a implantação e a disponibilização de soluções de infraestrutura de TIC para atendimento às necessidades corporativas do Instituto.

2.2.3. O ITI implementa um processo permanente de modernização visando o aperfeiçoamento na prestação dos serviços a seus usuários internos e externos. A melhoria contínua relacionada ao seu ambiente tecnológico e ao atendimento especializado às diversas áreas funcionais do Instituto, em especial às áreas fins, é fundamental.

2.2.4. Dessa forma, a COTIC identificou melhorias que podem ser implantadas ou incrementadas na infraestrutura de TIC do ITI, objetivando a elevação da qualidade dos serviços suportados e fornecidos aos servidores do órgão e à sociedade. Dentre essas melhorias, identificou-se a atualização dos seus ativos de perímetro de rede cabeada e *wireless*, por meio da aquisição de uma solução de firewall e atualização da rede sem fios, sendo objeto das necessidades listadas no Documento de Oficialização da Demanda –DOD.

2.2.5. A falta de visualização de eventos que ocorrem nas redes local (LAN) e sem fios (WLAN) e a respectiva falta de controles de segurança, colocam o ITI em exposição a ataques contra sua infraestrutura. Há diversas técnicas de invasão utilizadas a nível de aplicação e de redes sem fios que são utilizadas contra organizações e a autarquia está sujeita a sofrer danos de grande relevância caso seja alvo de alguma dessas técnicas.

2.2.6. Não há meios de mensurar o perfil de ataques realizados contra o ITI com as ferramentas utilizadas hoje, e os bloqueios são insuficientes para conter técnicas específicas de ataque em camadas de rede, transporte e aplicação. Com isso, há vulnerabilidades já mapeadas pelo ITI que estão sem respectivas contramedidas.

2.2.7. Quanto ao escopo do projeto de assinaturas avançadas, parte importante dessa infraestrutura é a segurança do perímetro do ambiente tecnológico, que será composto, inicialmente, de dois sítios geograficamente separados.

2.2.8. O cenário atual de ameaças tecnológicas vem tornando os sistemas tradicionais de proteção praticamente obsoletos. O nível de complexidade observado nas redes inclui tecnologias como *blockchain*, *machine learning*, *deepweb*, virtualização, containerização, criptografia ponto a ponto, *ransomware*, *deepfakes*, computação em nuvem, botnets, DDOS, IoT/BYOD e outras. Muitas, representam avanços tecnológicos significativos, mas também trazem desafios. Outras, representam claras ameaças. Todo esse contexto tecnológico exige das equipes de infraestrutura e segurança cada vez mais técnicas e recursos modernos e eficientes.

2.2.9. O ITI utilizará dois agrupamentos (*clusters*) de firewall, um em cada sítio (Florianópolis e Brasília), para entregar esse serviço à população. A solução, também, contemplará monitoramento ativo das

defesas dos perímetros da rede com recursos de prevenção à intrusão, Internet Prevention Systems- IPS, com procedimentos automatizados de identificação e bloqueio de tráfego malicioso.

2.2.10. Visto que o ambiente será gerenciado com critérios de segurança similares aos da Infraestrutura de Chaves Públicas do Brasil, os firewalls NG, proporcionarão maior interoperabilidade e facilidade na sua administração, inclusive, possibilitando a configuração de arranjos redundantes. Essa característica é muito importante para ambientes críticos de alta disponibilidade, como o que se pretende implantar, consideramos adequando um índice de 99,99% de operação. Em um ano, isso representa a uma indisponibilidade máxima de 52,56 minutos.

2.2.11. O parque de *switches* de rede e armazenamento da Autarquia tem equipamentos sem garantia e já descontinuados pelos fabricantes. Há ativos dos fabricantes H3C, HP e 3Com, ou seja, é inviável sustentar um ambiente com equipamentos com falha iminente, de tecnologias, fabricantes e gerações diferentes.

2.2.12. Essa heterogeneidade inviabiliza a adoção de padrões de segurança com eficiência, dado que os fabricantes utilizam técnicas próprias para implementar os padrões da indústria em seus equipamentos.

2.2.13. *Switches* e *access points* podem hoje ser gerenciados por uma ferramenta de gerenciamento de políticas de acesso de redes chamada NAC (*Network Access Control*). NACs são utilizados para controlar o acesso de redes, segregar *hosts* que não atendam a requisitos de acesso, forçam conformidade de ativos quanto a atualizações e configurações, além de facilitar a implementação de iniciativas de uso de equipamento próprio no ambiente corporativo, o BYOD (*Bring Your Own Device*).

2.2.14. Os *switches* de armazenamento já não comportam a vazão de dados demandada pela COTIC e CGISI. Uma vez em descontinuidade, não há mais suporte a atualizações corretivas, evolutivas e de segurança para as ferramentas, e o componente de acesso, baseado em Java, tem apresentado instabilidades que podem, a qualquer momento, comprometer a operação de todos os dados armazenados nas áreas de armazenamento (*storages*) da autarquia.

2.2.15. A COTIC não tem gerência sobre os acessos da rede sem fios, e tem capacidade limitada de gerenciamento nas redes cabeadas, dada a falta de ferramentas para monitoramento e *enforcement* dessas políticas de acesso.

2.2.16. De maneira análoga, a CGISI gerencia ativos em ambientes geograficamente apartados, com a necessidade de um rígido controle de acesso à Infraestrutura de Chaves Públicas, e carece de ferramentas que facilitem esse gerenciamento.

2.2.17. Sendo assim, esta demanda está alinhada com as seguintes diretrizes estratégicas:

Objetivos Estratégicos - Planejamento Estratégico 2019-2022	Ações do PDTIC 2019-2020	Metas associadas no PDTIC 2019-2020	Plano anual de contratação (PAC-2020)
RE-1 - Assegurar confiança a documentos e transações eletrônicas com eficiência e sustentabilidade RE-2 - Ter clientes, governo e demais partes interessadas satisfeitos	ACTI-18 - Implantação de solução para o balanceamento do acesso e para a alta disponibilidade das aplicações corporativas, incluindo ferramentas para monitoramento do desempenho de acesso às aplicações. ACTI-42 - Aquisição de equipamentos capazes de implementar mecanismos de controle às informações	NEI-01 - Aperfeiçoar a qualidade de atendimento à sociedade e ao público interno NEI-03 - Aperfeiçoar a segurança da informação NEI-04 - Aprimorar serviços e governança de TIC NEI-07 - Otimizar a gestão dos recursos de TIC do ITI NEI-08 - Aprimorar as ferramentas de comunicação	150100 - Aquisição de solução de firewall 3932777 - Aquisição de controladora de redes sem fios e pontos de acesso 463674 - Switch 24 portas Gigabit 110/220 para conexão de servidores e equipamentos de rede 396243 - Switch 24 SAN

<p>DI-1</p> <p>- Aperfeiçoar, simplificar e consolidar o processo de credenciamento</p> <p>DI-2 - Fortalecer a auditoria e a fiscalização, com foco no monitoramento, na prevenção e na melhoria da qualidade do serviço prestado</p> <p>DI-5 - Fomentar a pesquisa, o desenvolvimento e a inovação em soluções tecnológicas para segurança e confiança Digital</p> <p>AL-2 - Promover gestão organizacional que favoreça a integração e a inovação Tecnológica</p> <p>AL-3 - Melhorar as soluções de tecnologia da informação e comunicação mantendo-as compatíveis com as demandas institucionais</p>	<p>armazenadas na infraestrutura de TIC (firewall, IDS/IPS, antiDDos, balanceamento de enlaces e aplicações etc.)</p> <p>ACTI-46 - Substituição da atual infraestrutura de rede sem fio do ITI por equipamentos mais modernos, melhor adequados para as necessidades da instituição e cobertos por garantia.</p> <p>ACTI-57 - Implantação de solução de autenticação para a rede sem fio por meio do protocolo 802.1X (WPA2 - Enterprise) integrada ao domínio corporativo.</p>	<p>institucionais</p> <p>NEI-11 - Fornecer ferramentas e serviços de Tecnologia da Informação e Comunicação adequadas para as necessidades de negócio do ITI</p> <p>NEI-12 - Aperfeiçoar os processos de gestão da Autoridade Certificadora Raiz da ICP-Brasil</p>	
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

2.3. Requisitos Legais

2.3.1. Medida Provisória nº 2.200-2, de 24 de Agosto de 2001 - Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências.

2.3.2. Medida Provisória nº 983, de 16 de junho de 2020, que dispõe sobre as assinaturas eletrônicas em comunicações com entes públicos e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos.;

2.3.3. Lei 8.666, de 21 de junho de 1993: Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.

- 2.3.4. Decreto nº 8.985, de 8 de Fevereiro de 2017 - Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Instituto Nacional de Tecnologia da Informação - ITI, remaneja cargos em comissão e substitui cargos em comissão do Grupo, Direção e Assessoramento Superiores - DAS por Funções Comissionadas do Poder Executivo – FCPE.
- 2.3.5. Decreto nº 7.892, de 23 de janeiro de 2013: Regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993.
- 2.3.6. Decreto nº 7.174, de 12 de maio de 2010: Regulamenta a contratação de bens e serviços de informática e automação pela Administração Pública Federal;
- 2.3.7. Decreto 5.450 de 31 de maio de 2005: Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.
- 2.3.8. Instrução Normativa MP/SLTI Nº1/2019: Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP do Poder Executivo Federal. Disponível em: http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/70267659/do1-2019-04-05-instrucao-normativa-n-1-de-4-de-abril-de-2019-70267535.
- 2.3.9. Decreto nº 8.638/2016 - Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.
- 2.3.10. Planejamento Estratégico 2019-2022 - Planejamento Estratégico do ITI. Disponível em <https://www.iti.gov.br/images/repositorio/institucional/planejamentoestrategico/pe2019-2022.pdf>.
- 2.3.11. Plano Diretor de Tecnologia da Informação e Comunicações 2019-2020 - Plano Diretor de Tecnologia da Informação e Comunicações do ITI. Disponível em https://www.iti.gov.br/images/repositorio/institucional/pdti/Plano_0313488_ITI_PDTIC_2019_2020_Minuta.pdf.
- 2.3.12. Decreto nº 3.555, de 08 de agosto de 2000, que aprova o regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns;
- 2.3.13. Lei nº 10.520, de 17 de julho de 2002, que institui, no âmbito da União, Estados, Distrito Federal e Municípios a modalidade de licitação denominada pregão, para contratação de bens e serviços comuns;
- 2.3.14. Lei Complementar nº 123, de 14 de dezembro de 2006, que institui o Estatuto Nacional da microempresa e da Empresa de Pequeno Porte;
- 2.3.15. Decreto nº 7.174, de 12 de maio de 2010, que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;
- 2.3.16. Decreto nº 7.404, de 23 de dezembro de 2010 que estabelece normas para execução da Política Nacional de Resíduos Sólidos, de que trata a Lei nº 12.305, de 2 de agosto de 2010;
- 2.3.17. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);
- 2.3.18. Decreto nº 10.024, de 20 de setembro de 2019, que regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências;
- 2.3.19. Instrução Normativa SLTI/MPOG nº 1, de 19 de janeiro de 2010: Estabelece critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela APF;
- 2.3.20. Decreto nº 7.746, de 5 de junho de 2012: Estabelece critérios e práticas para a promoção do desenvolvimento nacional sustentável nas contratações.

2.4. Recursos Materiais

- 2.4.1. O ITI dispõe dos recursos estruturais para a implantação dos objetos desse Estudo Técnico. Os requisitos de instalação, conectorização e implantação dos equipamentos fazem parte da contratação,

conforme detalhado ao longo do Termo de Referência.

2.4.2. Não há necessidade de recursos materiais adicionais para se assegurar a continuidade do negócio.

2.5. Recursos Humanos

2.5.1. A contratada deverá prover pessoal qualificado em quantidade suficiente para a realização dos serviços.

2.5.2. Como apoio na implantação e na configuração dos softwares, o ITI dispõe de contrato com empresa terceirizada, a qual fornece serviços relativos à operação da infraestrutura de TIC do Instituto.

2.5.3. Deverá designar um responsável para contato direto com o ITI, sem custo adicional para a contratante. Além de ser o ponto focal da comunicação da contratante, ele deverá assumir as responsabilidades da contratada perante o ITI.

2.5.4. Deverá também indicar um substituto para o preposto que, na ausência deste, deverá assumir integralmente todas as responsabilidades perante à contratante.

2.6. Requisitos de Garantia e Continuidade Contratual

2.6.1. A contratada deverá prestar garantia às soluções de firewall, redes e switches fibre channel fornecidas, no local onde se encontrar instalado, por um período de 60 (sessenta) meses a contar da data de recebimento definitivo.

2.6.2. Caso ocorra algum evento que impeça a continuidade dos serviços de suporte e manutenção por parte da empresa contratada a empresa fabricante ou desenvolvedora da solução deverá se responsabilizar de forma solidária, dando continuidade à prestação dos serviços nos termos contratuais.

2.6.3. Com a antecedência mínima de 6 (seis) meses, as equipes técnicas responsáveis pela gestão das soluções deverão iniciar os estudos de prospecção tecnológica para analisar as soluções disponíveis e promover a contração de solução ou substituição por tecnologias adequadas e que garantam a conformidade e continuidade dos serviços.

2.6.4. A continuidade dos serviços durante a vigência da garantia, em caso de interrupção contratual, será mantida pelo fabricante. Após o vencimento, o ITI deverá providenciar a adaptação do ambiente às futuras tecnologias disponíveis.

2.7. Requisitos de Segurança

2.7.1. A contratada deverá respeitar as políticas de segurança estabelecidas pelo ITI durante a realização de atividades no ambiente do mesmo.

2.8. Requisitos Tecnológicos

SOLUÇÃO DE FIREWALL

FIREWALLS (PERFIS 1 E 2)

Requisitos Gerais

- 2.8.1. A solução deverá ser dimensionada para operar no ambiente com os seguintes parâmetros:
 - 2.8.1.1. 400 usuários simultâneos na instituição;
 - 2.8.1.2. 2 dispositivos por usuário, sendo 1 em rede sem fios (ex.: 1 desktop e 1 tablet por pessoa);
 - 2.8.1.3. Ocupar, no máximo, 2 unidades de *rack* (2Us).
- 2.8.2. As funcionalidades deverão ser disponíveis integralmente para os usuários e dispositivos do dimensionamento acima. Ou seja, é proibida a entrega de funcionalidades com atendimento parcial (Ex.: módulo "ABC" que atenda até 10 usuários, em vez dos 400 descritos acima);
- 2.8.3. Os equipamentos devem ter seu licenciamento completo e perpétuo;
 - 2.8.3.1. No caso de funcionalidades que são comercializadas unicamente na modalidade de assinatura, o tempo da subscrição será o mesmo da garantia junto ao fabricante, contatos juntamente com os prazos do *hardware*.
- 2.8.4. Os equipamentos serão entregues com todos os *tranceivers*, conectorização, trilhos e demais componentes necessários para a instalação física nos *racks* e conectividade na infraestrutura de rede do ITI .
- 2.8.5. Não serão aceitos equipamentos em modo *End of Support* durante a vigência da garantia e que estejam em modo *End of Life* no ato da assinatura da ata de registro de preços, não deixando de atender à vigência da garantia.
 - 2.8.5.1. Se o equipamento ofertado não atenda a este requisito, será aceito equipamento de capacidade técnica igual ou superior, da mesma série ou linha ou família, desde que atenda a todos os requisitos técnicos do edital.
 - 2.8.5.2. O fabricante do equipamento proposto deve possuir avaliação(ões) publicada(s) entre os anos de 2017 a 2019 pela NSS Labs, confirmando taxa de bloqueio de ataques ("efetividade de segurança") mínima de 95% (noventa e cinco por cento).
- 2.8.6. Todo e qualquer componente externo da solução (ex.: ferramenta de gerência, centralizador de *logs*, gerador de relatórios, sensor, etc) necessário para o atendimento dos requisitos técnicos deverá ser compatível com o *hypervisor VMWare*;
 - 2.8.6.1. Caso haja necessidade de licenciamentos quaisquer diversos aos citados acima, como sistema gerenciador de bancos de dados (Ex.: MS SQL, Oracle), sistema operacional (Windows Server, Suse Linux, Red Hat) ou outro tipo de dependência que enseje custos, deverão ser entregues pelo fornecedor como parte da solução.
- 2.8.7. O fornecedor entregará 2 instâncias de gerenciamento de firewall, sendo:
 - 2.8.7.1. Uma para o ambiente interno do ITI, com localização física dos equipamentos em 2 sites em Brasília;
 - 2.8.7.2. Uma para o ambiente de assinaturas avançadas, com localização física dos equipamentos em Brasília e em Florianópolis;

Características físicas

- 2.8.8. 1 interface console RJ45
- 2.8.9. Para o firewall perfil 1:
 - 2.8.9.1. No mínimo, 8 interfaces x 10/100/1000 BaseT
 - 2.8.9.2. No mínimo, 2 interfaces 10G SFP+;
- 2.8.10. Para o firewall perfil 2:
 - 2.8.10.1. No mínimo, 8 interfaces x 10/100/1000 BaseT;

- 2.8.11. Ao menos duas interfaces USB que podem ser utilizadas como:
 - 2.8.11.1. Acesso *failover* por Modem USB;
 - 2.8.11.2. Interface de *setup* inicial do *Firewall*.
 - 2.8.11.3. Caso o equipamento conte com apenas uma interface USB, deverá haver disponibilidade de ao menos mais uma interface de comunicação no padrão RJ-45 para acesso de gerenciamento.
- 2.8.12. Deve ser instalado pela contratada em bastidor padrão de 19", com tamanho máximo de 1 RU e acompanhado dos respectivos Kit's de fixação.
 - 2.8.12.1. A instalação consiste na colocação dos equipamentos em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos, e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de tecnologia da informação do contratante, incluindo: instalação física, conexão, configuração e integração, aplicação de licenças e atualização de firmware, se necessário;
 - 2.8.12.2. A instalação abrange a aplicação das políticas definidas no serviço de configuração da solução de firewall, disponível no módulo de gerenciamento da solução, preferencialmente por meio do padrão *Zero Touch Deploy*, bem como os devidos ajustes de cada equipamento (ex.: IP diferente, FQDN ou qualquer outra peculiaridade para terminar a implantação);
 - 2.8.12.3. A contratada deverá garantir os equipamentos, componentes, acessórios, *transceivers* e cabos de conexão (elétricos e lógicos) necessários para interligar fisicamente todos os componentes.
- 2.8.13. Fonte 100–240VAC, 50–60 Hz; e
- 2.8.14. Tomada padrão brasileiro.

Características funcionais

A solução deve:

Firewall

- 2.8.15. Suportar configurações de multi-WAN, permitindo, ao menos, 4 conexões externas com a internet simultaneamente;
- 2.8.16. Operar com interfaces em modo de failover;
- 2.8.17. Funcionalidade de failover para um modem USB diretamente conectado;
- 2.8.18. Configuração de um modem USB como uma interface a ser utilizada em *Failover* de WAN;
- 2.8.19. Interfaces externas configuradas em modo Round Robin, com pesos configuráveis;
- 2.8.20. Interfaces externas configuradas com a funcionalidade de "*overflow*", permitindo o uso de links externos secundários quando o principal for excedido;
- 2.8.21. Realizar agregação de links (802.3ad);
- 2.8.22. Detecção de falha de links;
- 2.8.23. Suportar balanceamento de *links*;
- 2.8.24. Controle de banda por usuário, grupo de usuários, políticas e protocolo;
- 2.8.25. Controle de banda por interface;
- 2.8.26. Controle de banda por endereço de IP e VLAN;
- 2.8.27. Consumo de banda e cota de tempo por usuário;

- 2.8.28. Suportar sua implementação como Rounting Mode; Drop-In Mode (mesmo endereço IP em todas as interfaces) e em Transparent Bridge Mode;
- 2.8.29. Suportar:
 - 2.8.29.1. NAT estático e dinâmico;
 - 2.8.29.2. NAT 1:1;
 - 2.8.29.3. PAT;
 - 2.8.29.4. IPSec NAT Traversal; e
 - 2.8.29.5. NAT baseado em política.
- 2.8.30. Operar em modo de alta-disponibilidade, podendo atuar como ATIVO-PASSIVO e ATIVO-ATIVO;
- 2.8.31. Capacidade de fazer *load balancing* entre pelo menos 10 servidores internos com pesos distintos;
- 2.8.32. Suportar IPv6 nativamente;
- 2.8.33. Possuir capacidade de atuar como um roteador multicast para encaminhamento de trafego multicast da origem até os destinos dentro da rede;
- 2.8.34. Suportar a detecção e mitigação de flood UDP;
- 2.8.35. Possuir mecanismo *antispoofing*;
- 2.8.36. Detectar e bloquear, no mínimo:
 - 2.8.36.1. *IP spoofing*
 - 2.8.36.2. *SYN flood*
 - 2.8.36.3. *UDP flood*
 - 2.8.36.4. *Port scanning*
 - 2.8.36.5. *ICMP flood*
 - 2.8.36.6. *ICMP sweep*
- 2.8.37. Suportar configuração de quatro zonas de segurança, sendo externa, privada, opcional (DMZ) e customizada.
- 2.8.38. Suportar endereçamento IP estático e dinâmico;
- 2.8.39. Possuir funcionalidades de DHCP relay que permitam a adição de servidores DHCP simultâneos.
- 2.8.40. Permitir DHCPv6 em interfaces externas.
- 2.8.41. Possuir no firewall de perfil 1:
 - 2.8.41.1. Throughput de 15 Gbps para firewall;
 - 2.8.41.2. Throughput de 4 Gbps para IPS;
 - 2.8.41.3. Throughput de 3 Gbps para UTM (combinando AV, VPN, firewall, Web Filter com *deep inspection*, antispam e IPS);
 - 2.8.41.4. Suportar 3.500.000 conexões simultâneas;
 - 2.8.41.5. Suportar um mínimo de 300 VLANs;
- 2.8.42. Possuir no firewall de perfil 2:
 - 2.8.42.1. Throughput de 8 Gbps para firewall;
 - 2.8.42.2. Throughput de 2 Gbps para IPS;

- 2.8.42.3. Throughput de 1,5 Gbps para UTM (combinando AV, VPN, firewall, Web Filter com *deep inspection*, antispam e IPS);
- 2.8.42.4. Suportar 2.000.000 conexões simultâneas;
- 2.8.42.5. Suportar um mínimo de 200 VLANs;
- 2.8.43. O equipamento de firewall deve possuir, no mínimo, funcionalidades de: firewall, filtro de conteúdo, controle de URL, controle de aplicação, *intrusion prevention system* (IPS), antivírus de rede, controle de ameaças avançadas, antispam/phishing, SD-WAN e geração de relatórios;
- 2.8.43.1. Caso haja alguma funcionalidade não disponibilizada nativamente pelo *appliance*, o licitante deverá disponibilizar a ferramenta complementar do mesmo fabricante;
- 2.8.44. Implementar políticas de segurança na camada de aplicação;
- 2.8.45. Possuir políticas na camada de aplicação pré-configuradas com proteção padrão para suportar os seguintes protocolos com inspeção de *malware*:
 - 2.8.45.1. HTTP / HTTPS;
 - 2.8.45.2. POP3 / POP3S;
 - 2.8.45.3. IMAP / IMAPS;
 - 2.8.45.4. SMTP / SMTPS;
 - 2.8.45.5. FTP;
 - 2.8.45.6. DNS;
 - 2.8.45.7. SIP; e
 - 2.8.45.8. H.323.
- 2.8.46. Suportar autenticação via RADIUS, SecureID, LDAP e Active Directory;
- 2.8.47. Suportar autenticação transparente de usuários (Single Sign On) de AD e RADIUS;
- 2.8.48. Suportar a configuração de regras de proxy explícito para aceitar solicitações de clientes e buscar informação em nome dos clientes;
- 2.8.49. Ter funcionalidade de proxy SMTP para analisar documentos com macros embutidas e o equipamento também deve possuir uma opção para remover estes macros antes de enviar o documento para seus destinatários;
- 2.8.50. Suportar certificados digitais autoassinados (*self-signed*) para executar *deep inspection* de pacotes via proxy SMTP sobre TLS;
- 2.8.51. Executar *deep content inspection* de dados em proxy HTTPS;
- 2.8.52. Limitar o acesso de usuários a contas Google pessoais;
- 2.8.53. Definir o intervalo de tempo entre tentativas de login incorretas em conexões FTP;
- 2.8.54. Possuir a funcionalidade de NTP server;
- 2.8.55. Detectar regras conflitantes;
- 2.8.56. Suportar DNS dinâmico dos seguintes provedores, como:
 - 2.8.56.1. DynDNS.org
 - 2.8.56.2. No-IP.com
 - 2.8.56.3. dynu.com
 - 2.8.56.4. duckdns.org

- 2.8.57. Possuir defesas de ataques fragmentados, permitindo que o firewall monte os pacotes fragmentados antes de encaminhá-los a redes internas;
- 2.8.58. Conseguir filtrar conteúdo nos protocolos mais comuns, assim como filtrar conteúdo tipo “MIME”;
- 2.8.59. Proteger e-mails internos contra open relay. Ele deve ser capaz e ser configurado para domínios de e-mail aceitos no ambiente;
- 2.8.60. Permitir a configuração de limites para detecção de ataques de flood e Denial of Service (DoS) além de distributed denial of service (DDoS);
- 2.8.61. Suportar Protocol Anomaly Detection (PAD) para DNS e outros tipos de protocolos;
- 2.8.62. Suportar Server Name Indication (SNI) para configurar domínios para funcionalidades de bloqueio, inspeção ou permissão;
- 2.8.63. Complementar capacidades e bloqueio de CN existentes com SNI com a finalidade de bloquear domínios específicos do Google;
- 2.8.64. Suportar bloqueio e gerenciamento de tráfego por domínios especificados por FQDNs (Fully Qualified Domain Names) a fim de bloquear sites disponibilizados por Content Delivery Networks (CDNs);
- 2.8.65. Suportar o bloqueio de domínios através de *wildcard*;
- 2.8.66. Permitir a criação de políticas por IP utilizando *wildcard*;
- 2.8.67. Suportar o a configuração por política de bloqueio de conexões *inbound* e *outbound* para um país (ou conjunto de países);
- 2.8.68. O equipamento de firewall deve oferecer integração a mecanismos de Autenticação Forte de Múltiplo Fator (MFA) através do Protocolo Radius para as formas de VPN suportadas, sendo no mínimo SSL VPN (cliente), através da implementação PAP, L2TP (clientless) através da implementação MSCHAPv2 e IKEv2 (clientless) através da implementação EAP-MSCHAPv2;
- 2.8.69. O Fabricante da solução deve disponibilizar uma plataforma de abertura de chamados para suporte sem limite de número de chamados enquanto o licenciamento do dispositivo estiver válido;
- 2.8.70. O Fabricante deve possuir estoque de RMA dentro do Brasil a fim de agilizar a entrega de produtos em caso de falha/quebra;
- 2.8.71. O equipamento de firewall deve aplicar políticas granulares para restringir o tráfego de países considerados arriscados de acordo com a política de segurança da empresa contratante de acordo com o tipo de tráfego, porta, protocolo, endereço, usuário ou grupo de origem assim como destino;
- 2.8.72. O equipamento de firewall deve permitir outros tipos de tráfego que não ofereçam ameaças semelhantes, como DNS ou Mail para / de países que tenham certos protocolos bloqueados quando considerados perigosos pela política de segurança da empresa;
- 2.8.73. Permitir que o administrador de rede realize uma configuração em modo “offline” para posteriormente ser injetada ao firewall;
- 2.8.74. Possuir ferramenta de diagnóstico de tráfego de rede, tipo *tcpdump*;
- 2.8.75. Efetuar captura e *download* de pacotes no formato PCAP;
- 2.8.76. Suportar a criação de políticas de controle de uso de largura de banda, limitando ou expandido individualmente, baseadas em: porta ou protocolo, endereço IP de origem ou destino, grupo de usuários do Microsoft Active Directory e LDAP e/ou aplicações (por exemplo, Youtube e WhatsApp);
- 2.8.77. A solução deve suportar *single sign-on* (SSO) para soluções RADIUS;
- 2.8.78. A solução deve rastrear as sessões de usuários via SSO para RADIUS;

- 2.8.79. A solução deve suportar o download e alteração de diferentes versões de configuração para equipamentos, possibilitando utilizar a mesma configuração para hardwares distintos e versões de SO distintas;
- 2.8.80. A solução deve suportar SSO redundantes;
- 2.8.81. Gerenciar via linha comando através de porta serial e via SSH;
- 2.8.82. Suportar *single sign-on* para logins via RDP.
- 2.8.83. Suportar via SSO diversos usuários em uma única máquina para sistemas operacionais Windows;
- 2.8.84. Deve suportar VPN Mobile;
- 2.8.85. Suportar pelo menos 250 VPNs Mobile usando IPSec;
- 2.8.86. Suportar ao menos 250 usuários mobile usando VPN SSL;
- 2.8.87. Ser compatível com clientes SSL para Windows 7, 8, 10, Mac OS, Android e iOS;
- 2.8.88. Suportar VPN *site-to-site*;
- 2.8.89. Deve suportar pelo menos 100 VPNs entre *sites* utilizando IPSec;
- 2.8.90. Suportar iterações com outros produtos e marcas que suportem o padrão IPSec;
- 2.8.91. A solução deve suportar os seguintes métodos de autenticação:
 - 2.8.91.1. DES;
 - 2.8.91.2. AES 128;
 - 2.8.91.3. AES 192; e
 - 2.8.91.4. AES 256.
- 2.8.92. A solução deve suportar os seguintes métodos de criptografia:
 - 2.8.92.1. SHA-2;
 - 2.8.92.2. MD5;
 - 2.8.92.3. IKE Pre-Shared Key;
 - 2.8.92.4. 3rd Party Cert; e
 - 2.8.92.5. AES with CBC and GCM.
- 2.8.93. Deve suportar Dead Peer Detection (DPD);
- 2.8.94. Deve suportar VPN *site-to-site* e *client-to-site* com IKEv2;
- 2.8.95. Deve suportar Perfect Forward Secrecy (PFS) com chaves Diffie-Hellman (ou Diffie-Hellman-Merkle) em pacotes web e email;
- 2.8.96. Realizar VPN Failover (reestabelecer a VPN através de um segundo link em caso de falha do link primário);
- 2.8.97. Suportar VPN IPSEC com um throughput igual ou maior que 1 Gbps;
- 2.8.98. Permitir criar interfaces virtuais para VPNs e rotear tráfego utilizando VPNs *site-to-site* com protocolos de roteamento dinâmico;
- 2.8.99. A solução deve permitir visualizar estatísticas de VPN em interfaces virtuais, gateways e tunnel types para qualquer tipo de usuário;
- 2.8.100. Deve permitir visualizar mensagens de diagnóstico de VPN para ajudar a remediar e realizar o *troubleshooting* pelos administradores do sistema;

- 2.8.101. A solução deve suportar tuneis VPN site-to-site estáticos (políticas) e dinâmicas (roteadas) para *Microsoft Azure* e *AWS*; e
- 2.8.102. A solução deve suportar VPN em interfaces virtuais e realizar Failover entre elas.

Web Filter

- 2.8.103. Ter a funcionalidade de filtro de conteúdo Web e de URL com licenciamento incluso;
- 2.8.104. Permitir que o filtro trabalhe por categorias, ajustado por grupos de usuário e possuir um mínimo de 120 categorias;
- 2.8.105. Permitir exceções no filtro de conteúdo por meio de whitelist;
- 2.8.106. Apresentar ao usuário uma tela de aviso indicando que a categoria do website acessado não está de acordo com as políticas da empresa, permitindo ao mesmo seguir adiante após clicar em um “aceite”;
- 2.8.107. Suportar customização da mensagem de bloqueio;
- 2.8.108. Suportar uma base de dados atualizada dinamicamente localizada na nuvem ou disponível em uma solução de máquina virtual compatível com VMWare;
- 2.8.109. Filtrar conteúdo em múltiplas línguas, incluindo mas não limitado a: português, inglês, alemão, espanhol, japonês, chinês tradicional e simplificado;
- 2.8.110. Identificar e bloquear mais de 1000 aplicações diferentes, incluindo controle granular de aplicação, como telas de login e metodologias específicas de transferência de arquivo;
- 2.8.111. Suportar *updates* automáticos de assinaturas de aplicação;
- 2.8.112. Ter capacidade de atualização *offline* de suas assinaturas de aplicação;
- 2.8.113. Reconhecer pelo menos as seguintes aplicações:
1. active directory;
 2. appletalk echo;
 3. bittorrent;
 4. 4shared;
 5. cs game;
 6. call of duty;
 7. citrix;
 8. db2
 9. diablo3;
 10. dropbox;
 11. edonkey;
 12. evernote;
 13. emule;
 14. facebook;
 15. facebook chat;
 16. google drive;
 17. google-docs;
 18. gnutella;
 19. gmail;
 20. gmail chat;
 21. http-proxy;
 22. http-tunnel;
 23. skype;
 24. linked-in;
 25. logme in;
 26. ms-rdp;

- 27. mysql;
- 28. msft-store;
- 29. netflix;
- 30. spotify;
- 31. skydrive;
- 32. teamviewer;
- 33. twitter;
- 34. vnc;
- 35. youtube;
- 36. oracle;
- 37. kerberos;
- 38. ldap;
- 39. radius;
- 40. itunes;
- 41. dhcp;
- 42. ftp;
- 43. dns;
- 44. wins;
- 45. msrpc;
- 46. ntp;
- 47. snmp;
- 48. rpc over http;
- 49. gotomeeting;
- 50. twitch.tv;
- 51. vevo;
- 52. webex;
- 53. winamp;
- 54. zoom;
- 55. sftp;
- 56. sql-net;
- 57. vmnet;
- 58. quic;
- 59. cisco tdp;
- 60. openvpn;
- 61. tinyvpn;
- 62. dotvpn;
- 63. tor;
- 64. yammer;
- 65. fortnite;
- 66. LoL;
- 67. second life;
- 68. netscout;
- 69. whatsapp;
- 70. telegram;
- 71. klogin.

2.8.114. Suportar validação de URL com *content filtering*;

2.8.115. Disponibilizar bases de dados de *blacklists* do fabricante;

2.8.116. Bloquear tráfego vindo de IPs maliciosos reconhecidos por base de dados de *blacklists* disponíveis no mercado (no mínimo, a do próprio fabricante).

2.8.117. Bloquear tráfego de botnets reconhecidas por base de dados de *blacklist* disponíveis no mercado (no mínimo, a do próprio fabricante);

- 2.8.118. Suportar a filtro de aplicação no próprio hardware da solução através de subscrição inclusa por tempo integral da garantia; e
- 2.8.119. Suportar a configuração de exceções para filtro de aplicação.

Antivírus

- 2.8.120. Ter a funcionalidade de antivírus de borda com licenciamento incluso;
- 2.8.121. Receber atualizações de assinaturas de antivírus automaticamente;
- 2.8.122. Permitir o acesso a *updates* de assinatura de manualmente e instalar estas assinaturas a partir de um ambiente *offline*;
- 2.8.123. Suportar a opção de quarentena para e-mails recebidos
- 2.8.124. Suportar *whitelists* para e-mails a fim de receber mensagens de domínios confiáveis em seu ambiente
- 2.8.125. Ter a capacidade de detectar e bloquear *malwares* diversos, como: *spyware*, *Potentially Unwanted Programs* (PUPs), trojans, bots e backdoors;
- 2.8.126. Ser capaz de escanear todos os arquivos comprimidos (.zip, .tar, .rar, .gzip) com pelo menos 3 níveis de compressão;
- 2.8.127. Ser capaz de tratar arquivos criptografados;
- 2.8.128. Suportar os pelo menos os protocolos: HTTP, FTP, SMTP, POP3;
- 2.8.129. Possuir pontuação de reputação para cada URL/IP acessado;
- 2.8.130. Permitir o *by-pass* da varredura do AV, com base na pontuação;
- 2.8.131. Permitir o bloqueio de endereços com reputação baixa devido a histórico de vírus e/ou outros tipos de *malware*. O score deve ser estipulado baseado em informação recebida por repositório do fabricante;
- 2.8.132. Possuir engine de antivírus;
- 2.8.133. Possuir um engine de análise heurística avançada;
- 2.8.134. Possuir um engine de AV de inteligência artificial;
- 2.8.135. Desenvolver perfis de arquivos maliciosos e benignos. Esses perfis incluem comportamentos e características de arquivos para fornecer uma visão abrangente da ameaça em potencial;
- 2.8.136. Avaliar a ameaça em potencial;
- 2.8.137. Identificar uma ameaça, e bloquear o *malware* automaticamente, impedindo que a carga mal-intencionada entre em sua rede.

Antispam

- 2.8.138. Ter a funcionalidade de Antispam com licenciamento incluso;
- 2.8.139. Possuir capacidades de Anti-Spam ativadas a partir de uma assinatura adicional no mesmo hardware, ou solução do mesmo fabricante que seja integrável com o *firewall*;
- 2.8.140. Trabalhar com tecnologia de anti-spam baseada em Recurrent Pattern Detection (RPD) ou similar;
- 2.8.141. Possuir em sua solução de anti-spam uma opção de quarentena;
- 2.8.142. Ser capaz de bloquear mensagens com links maliciosos;
- 2.8.143. Ter integração entre análise de antivírus e anti-spam (detecção e surto de vírus);

- 2.8.144. Possuir capacidade para bloquear spam em idiomas estrangeiros;
- 2.8.145. Possuir capacidade para bloquear spam baseado em texto;
- 2.8.146. Identificar e bloquear *e-mails* falsificados (*email spoofing*);
- 2.8.147. Ter integração com MS Exchange 2019 e Exchange Online (Azure);
- 2.8.148. Ser compatível com Zimbra.

IPS

- 2.8.149. Ter a funcionalidade de IPS com licenciamento incluso;
- 2.8.150. Receber atualizações automáticas de assinaturas de IPS
- 2.8.151. Oferecer suporte para o IPS conduzir análises na camada de aplicação, definir o nível de severidade do ataque e gerar alarmes remotos para notificações de eventos
- 2.8.152. Oferecer suporte para bloqueio automático de fontes conhecidas de ataque
- 2.8.153. Suportar todos os principais protocolos: HTTP, FTP, SMTP, POP3, IMAP
- 2.8.154. Oferecer suporte para acessar atualizações de assinatura e, manualmente, instalar assinaturas em modo *offline*;
- 2.8.155. Possuir a capacidade de realizar os escaneamentos em modo FAST SCAN e FULL SCAN
- 2.8.156. Permitir que cada ameaça de IPS seja tratada de forma específica, de acordo com seu nível de ameaça;
- 2.8.157. Prevenir, no mínimo, os seguintes ataques:
 - 2.8.157.1. *SQL injection*;
 - 2.8.157.2. Cross-site scripting (XSS);
 - 2.8.157.3. Travessia de diretórios (*directory traversal*);
 - 2.8.157.4. Execução remota de código;
 - 2.8.157.5. *Portscans*;
 - 2.8.157.6. *Exploits*;
 - 2.8.157.7. *Backdoors*;
 - 2.8.157.8. *Spoofing*;
 - 2.8.157.9. *Flooding*;
 - 2.8.157.10. Tráfego mal formado;
 - 2.8.157.11. Cabeçalhos inválidos de protocolos;
 - 2.8.157.12. Elevação de privilégios;
 - 2.8.157.13. *Local File Inclusion*;
 - 2.8.157.14. Buffer overflows;
 - 2.8.157.15. Evasão de IPS:
 - 1. *IP Packet Fragmentation*;
 - 2. *Stream Segmentation*;
 - 3. *RPC Fragmentation*;
 - 4. *URL Obfuscation*;
 - 5. *HTML Obfuscation*;

- 6. *Payload Encoding*;
- 7. *FTP Evasion*; e
- 8. *Layered Evasions*.

- 2.8.158. Permitir desativar a análise de ataques a partir de endereços/faixa de IP específicos; e
- 2.8.159. Permitir desativar a análise de assinaturas e protocolos.

DLP

- 2.8.160. Suportar recursos de prevenção contra perda de dados (DLP)
- 2.8.161. Oferecer suporte DLP para iniciativas de conformidade com PCI, HIPAA e GDPR;
- 2.8.162. Suportar regras predefinidas de DLP para números de identidade nacionais/internacionais, dados de cartão de crédito, dados de endereço, informações pessoais identificáveis (PII) e informações sobre saúde;
- 2.8.163. Fornecer regras predefinidas de DLP para o Brasil;
- 2.8.164. Suportar atualizações de assinatura de DLP e/ou a instalação manual de assinaturas de DLP em modo *offline*;
- 2.8.165. Funcionar em conjunto com as demais ferramentas da solução, para mitigar ameaças.

APT

- 2.8.166. Ter recurso de detecção de ameaças persistentes avançadas (APT);
- 2.8.167. Suportar emulação completa de sistema para detectar *malware* avançado durante o tempo de execução da execução em uma Next Generation Sandbox na nuvem para, no mínimo, 25 artefatos simultâneos;
- 2.8.168. Suportar APT para todos os executáveis de Windows, zip, PDF, objeto do Microsoft Office, Mac OS, Javascript e tipos de arquivo APK do Android;
- 2.8.169. Fornecer relatórios detalhados com análises acionáveis que identificam um arquivo como *malware*;
- 2.8.170. Incluir uma lista sumária de indicadores de ameaças que informam porque o arquivo foi bloqueado como *malware*.

Firewall de DNS e Phishing

- 2.8.171. Ter a funcionalidade de Firewall de DNS e proteção contra *phishing* com licenciamento incluso;
- 2.8.172. Fornecer proteção anti-malware de blacklists de domínios por firewall de DNS
- 2.8.173. Fornecer filtro de conteúdo a nível de domínio
- 2.8.174. Prover detalhes de contexto da ameaça em cada alerta
- 2.8.175. Proteger o ambiente de ameaças de comando e controle e outras conexões maliciosas;
- 2.8.176. Utilizar bases de inteligência da solução para otimizar a proteção;
- 2.8.177. Permitir a comunicação individualizada e personalizada entre a vítima do ataque e o fornecedor do sistema de análise de ameaças
- 2.8.178. Fornecer relatórios com dados detalhados e análise aprofundada identificando o arquivo como *malware*

Access Portal

- 2.8.179. Permitir que administradores realizem o suporte de implementação e acesso centralizado à aplicações na nuvem e recursos internos via RDP e SSH, com integração com soluções de SSO;
- 2.8.180. Habilitar a funcionalidade de Access Portal no mesmo hardware através de licenciamento adicional incluso;
- 2.8.181. Incluir no suporte a SAML no Access Portal para a integração com SSO e provedores de MFA, que atuem como identity provider (IDP);
- 2.8.182. Integrar a autenticação do Access Portal com mecanismos de autenticação do firewall, incluindo RADIUS

SD-WAN

- 2.8.183. Ter a funcionalidade de SD-WAN com licenciamento incluso;
- 2.8.184. Suportar roteamento baseado por política de SD-WAN, permitindo que administradores especifiquem parâmetros para definir por qual interface certo tipo de trafego será enviado.
- 2.8.185. Permitir a configuração da funcionalidade de SD-WAN em qualquer interface WAN de forma agnóstica, independente se a mesma for MPLS, internet, 4G/LTE, entre outras;
- 2.8.186. Ser compatível com o componente de da solução, permitindo que suas características e análises sejam realizadas nas VPNs assim como em links WAN;
- 2.8.187. Conter mecanismo de detecção de melhor circuito de roteamento (algoritmos de melhor caminho);
- 2.8.188. Possuir roteamento Baseado em Políticas e múltiplas saídas (e tipos de saídas) WANs;
- 2.8.189. Deve selecionar o melhor caminho baseado em tipo de tráfego e do host de origem;
- 2.8.190. Ser configurada para realizar *failover* entre links principais e secundários caso os links utilizados ultrapassem os limites previamente definidos de *jitter*, latência e perda de pacotes;
- 2.8.191. Deve verificar *jitter*, latência e perda de pacotes de cada link externo com endereços distintos na internet;
- 2.8.192. Ser configurável via implantação *Zero-Touch Deploy*;
- 2.8.193. Ser compatível com VPNs montadas em interfaces virtuais com roteamento dinâmico;
- 2.8.194. Realizar o gerenciamento de tráfego por tipo de aplicação;
- 2.8.195. A solução de SD-WAN UTM deve suportar atualizações automáticas de endereço IP via serviço de DNS Dinâmico
- 2.8.196. Suportar o monitoramento de link com *ping*, TCP e DNS;
- 2.8.197. Suportar o monitoramento de links VPN; e
- 2.8.198. Permitir a exportação de informações via Netflow.

Gerenciamento

- 2.8.199. A solução será entregue com sua ferramenta de gerência de firewalls com licenciamento incluso.

- 2.8.199.1. Haverão duas instâncias licenciadas de gerência apartadas a serem providas pela contratada: uma com 4 firewalls do perfil 1, outra com 2 equipamentos de cada perfil.
- 2.8.200. Prover administração em tempo real de, no mínimo, 4 firewalls, inclusive de modelos diferentes do fabricante, através de uma única interface de gerência;
- 2.8.201. Suportar monitoramento em tempo real de logs de tráfego, alarmes, eventos, diagnósticos e estatísticas;
- 2.8.202. Enviar diversos alertas via SNMP ou email;
- 2.8.203. Permitir o uso de NAT para conexões via *gateway* de aplicação SNMP;
- 2.8.204. Permitir ser gerenciado através de múltiplos computadores simultaneamente;
- 2.8.205. Permitir a criação de templates para configurações de VPN;
- 2.8.206. Permitir a criação de templates para configurações compartilhadas entre firewalls de diversos locais remotos;
- 2.8.207. Suportar o agendamento para a aplicação de configurações compartilhadas de um ou diversos *firewalls* simultaneamente;
- 2.8.208. Suportar a função de *rollback* para configurações anteriores;
- 2.8.209. Permitir a edição de políticas através de Windows GUI, interface Web e CLI;
- 2.8.210. Suportar a configuração de acessos distintos para administradores
- 2.8.211. Suportar gerenciamento via Web Browser ou via cliente;
- 2.8.212. Suportar comparação de versões de configurações;
- 2.8.213. Possuir a capacidade de criação de políticas de firewall;

Relatórios e logs

- 2.8.214. A solução será entregue com licenciamento de sua ferramenta de gerência de gráficos e geração de relatórios, do tipo *virtual appliance*, incluso.
- 2.8.215. Possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário;
- 2.8.216. Permitir a implementação de servidores externos ao firewall para centralizar os logs e relatórios;
- 2.8.217. A solução de armazenamento de logs e relatórios não deve ter custo adicional;
- 2.8.218. Permitir o envio de logs para, no mínimo, 2 servidores simultaneamente;
- 2.8.219. Criptografar a transmissão dos logs sem que seja necessária a criação de uma VPN para tal;
- 2.8.220. A solução de logs e relatórios deve possuir ao menos 90 relatórios pré-configurados, sem qualquer custo adicional;
- 2.8.221. Suportar a extração de relatórios no formato de PDF e CSV;
- 2.8.222. Possuir relatórios:
 - 2.8.222.1. Executivo;
 - 2.8.222.2. de *compliance* com padrões internacionais como HIPAA, PCI e GDPR;
 - 2.8.222.3. de ameaças;
 - 2.8.222.4. maiores consumidores de aplicações web;
 - 2.8.222.5. ativos em exposição (representação de quais ativos representam maior risco na rede)

- 2.8.223. Gerar relatórios contendo dados do ultimo dia, semana ou mês, automaticamente e envia-los por e-mail e FTP
- 2.8.224. Permitir em seu dashboard o pivotamento ou aprofundamento para maiores detalhes dos logs;
- 2.8.225. Suportar o envio de todos os relatórios por e-mail para períodos específicos
- 2.8.226. Suportar acessos distintos de administração e somente leitura para acessos a logs da solução;
- 2.8.227. Ser compatível com solução VMWare;
- 2.8.228. Indicar os tipos de trafego passando pelo firewall em layout gráfico;
- 2.8.229. Prover uma visão de mapa mundi, indicando a origem e destino do trafego de aplicação, pacotes negados e eventos de ameaças (no mínimo IPS e conexões);
- 2.8.230. Possuir relatórios de IPS que detalhem as informações e CVE de cada ameaça;
- 2.8.231. Suportar a agregação de diversos firewalls a fim de criar relatórios unificados da solução;
- 2.8.232. Suportar eventos de SSO;
- 2.8.233. Apresentar os FQDNs de clientes do Firewall em relatórios por usuário;
- 2.8.234. Possuir dashboard para bloqueio de IPs de origens de ataques;
- 2.8.235. Possuir um dashboard indicando o uso de cada política, inclusive informando as políticas não utilizadas no firewall;
- 2.8.236. Possuir um *dashboard* indicando geograficamente o fluxo do trafego do firewall, politicas acionadas assim como o IP de origem e destino do tráfego.

Garantia e atualização de versão do fabricante da solução de firewall

- 2.8.237. O serviço de garantia será do Fabricante, pelo período de 60 (sessenta) meses contados a partir do recebimento definitivo do produto, na modalidade 24x7, sem prejuízo de qualquer política de garantia adicional oferecido pelo fabricante;
- 2.8.238. Deverá fornecer direito de atualização contínua dos produtos licenciados - novas versões e *patches* de atualização.
- 2.8.239. O atendimento será em horário integral, telefônico e eletrônico, na modalidade 24x7x365;
- 2.8.240. Deverá ser disponibilizada pelo fabricante uma central de atendimento, 24 horas por dia, 7 dias por semana, todos os dias do ano;
- 2.8.241. A abertura de chamados na central de atendimento poderá ser feita através de telefone 0800, e-mail e portal web;
- 2.8.242. Deverá ser disponibilizado acesso a base de conhecimento do site do fabricante e fóruns de discussão.
- 2.8.243. Em caso de equipamento defeituoso, o envio de equipamento(s), componente(s), acessório(s) e dispositivo(s) novo(s), de primeiro uso e de modelo igual ou superior ao(s) danificado(s), desde que compatível com os equipamentos adquiridos, às expensas do fabricante, às dependências da CONTRATANTE;
- 2.8.244. O contrato de reposição de peças deverá ser na modalidade 8x5xNBD, com acionamento em horário comercial e devendo o equipamento substituto ser entregue na CONTRATADA até o próximo dia útil (Next Business Day - NBD) após a abertura do chamado;
- 2.8.245. Para determinação do horário de início de cada chamado referente a substituição de equipamento defeituoso devem ser levadas em consideração as seguintes condições:

- 2.8.245.1. Caso a determinação de falha do hardware pela fabricante tenha ocorrido antes das 15h, horário local da Brasília-DF, de segunda a sexta-feira (excluindo os feriados), o equipamento deverá ser enviado no mesmo dia para chegar no próximo dia útil.
- 2.8.245.2. Para as solicitações feitas depois das 15h, o fabricante deverá entregar o equipamento substituto até o segundo dia útil após o a determinação da falha;
- 2.8.246. A CONTRATADA deverá disponibilizar e colocar em operação em até 2 horas um equipamento de igual configuração e modelo para suprir o equipamento defeituoso, até que o substituto seja entregue e instalado;
- 2.8.247. O equipamento substituto passará à propriedade da contratante, devendo o mesmo ser imediatamente incluído no contrato de manutenção vigente em substituição ao equipamento danificado;
- 2.8.248. O equipamento substituído deverá ser devolvido ao fabricante às expensas do mesmo, em até 5 (cinco) dias úteis.
- 2.8.249. A CONTRATANTE deverá ter acesso direto ao centro de assistência técnica da fabricante dos equipamentos para abertura dos chamados, bem como para acompanhar e gerenciar os casos quando necessário. Esse acesso deverá ser provido 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de login/senha individual;
- 2.8.250. A CONTRATANTE deverá ter a opção de abrir os chamados junto a fabricante com o intermédio da CONTRATADA;
- 2.8.251. Não será aceita garantia para reposição de equipamentos da empresa revendedora;
- 2.8.252. Caso haja deslocamento do equipamento para outro *rack*, sala ou prédio da CONTRATANTE, a CONTRATADA deverá realizar a movimentação e reinstalação dos equipamentos para o novo ambiente, a critério da contratante.

SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE FIREWALL (POR SITE)

- 2.8.253. Configurar a ferramenta de gerência em ambiente VMWare, preparando para aceitar os ativos da solução;
- 2.8.254. Aplicar e tornar disponíveis as políticas a serem sincronizadas com os *firewalls* da solução;
- 2.8.255. Disponibilizar acesso à contratante;
- 2.8.256. Habilitar e disponibilizar perfil de leitura e geração de relatórios gerenciais da solução;
- 2.8.257. Integrar a solução com os serviços de diretório e autenticação da CONTRATANTE;
- 2.8.258. Aplicar, no mínimo, as políticas de segurança na CONTRATANTE pertinentes ao equipamento:
- 2.8.258.1. Firewall;
- 2.8.258.2. Antispam/Antiphishing;
- 2.8.258.3. Antivírus de rede;
- 2.8.258.4. VPN;
- 2.8.258.5. Filtros de conteúdos (*web filter, app control, etc*);
- 2.8.258.6. Logs.
- 2.8.258.7. IPS;
- 2.8.258.8. APT;
- 2.8.258.9. *Firewall* de DNS;

2.8.258.10. Relatórios; e

2.8.258.11. Demais incluídas na solução.

2.8.259. Caso a funcionalidade ainda não exista no ambiente da CONTRATANTE, a CONTRATADA deverá estabelecer uma linha de base, a partir de regras de monitoramento (ex.: utilização do IPS em modo de detecção), antes da efetivação das regras para bloqueio;

2.8.260. A CONTRATADA deverá apoiar a contratante na instalação, reinstalação, configuração ou reconfiguração dos módulos adquiridos/contratados a qualquer tempo durante a garantia da solução.

Treinamento para os *firewalls*

2.8.261. Oferecer treinamento para operacionalização dos *firewalls* (planejamento, instalação, configuração, operação, suporte e *troubleshooting*) com conteúdo teórico e atividades práticas, utilizando interfaces gráficas e linhas de comando (comand-line interface - CLI). A duração mínima de será de 40 (quarenta) horas e atenderá a 10 pessoas.

2.8.262. Os treinamentos deverão ser realizados em local situado na cidade de Brasília, nas dependências da CONTRATADA.

2.8.263. A CONTRATADA deverá fornecer o treinamento no período de vigência do contrato, no máximo até 30 (trinta) dias após pedido da CONTRATANTE.

2.8.264. A Contratada deverá fornecer material de treinamento e deverá ser ministrado por profissional certificado pelo fabricante do equipamento.

TREINAMENTO OFICIAL DO FABRICANTE DA SOLUÇÃO DE FIREWALL

2.8.265. O treinamento oficial do fabricante será de, no mínimo, 40 horas, em português.

2.8.266. O treinamento será realizado preferencialmente no modelo presencial, em instalações providas pela CONTRATADA.

2.8.266.1. Os treinamentos só serão aceitos na modalidade à distância se:

1. Por impossibilidade logística devido à pandemia de COVID-19;
2. Por interesse e oportunidade da Administração.

2.8.267. Deve ser ministrado por profissional certificado pelo fabricante dos equipamentos como instrutor.

2.8.268. A ementa do curso deve abranger conteúdos que vão desde instalação, configuração, gerenciamento, operação a *troubleshooting* dos equipamentos de hardware e de softwares que compõem a solução de redes sem fios.

2.8.269. Os treinamentos deverão ser realizados no Brasil, em português, na modalidade presencial, em local fornecido pela CONTRATADA.

2.8.270. O local de treinamento deverá possuir todas as facilidades para um perfeito desempenho das atividades, incluindo os recursos áudio visuais e laboratórios necessários, sem ônus à contratante.

2.8.271. A empresa disponibilizará material em formato digital (PDF) aos participantes e quaisquer conteúdos e ferramentas adicionais que venham a ser necessárias para o treinamento.

2.8.272. Os cursos referentes a equipamentos e softwares que façam parte do objeto deverão usar o material oficial de treinamento do respectivo fabricante por meio de qualquer um dos seus respectivos centros autorizados de treinamento.

2.8.273. Caso não haja disponibilidade para realização em Brasília, a empresa custeará os gastos de passagens e estadia para o centro de treinamento mais próximo de Brasília.

2.8.274. Deverá ser fornecido certificado de conclusão oficial do fabricante da solução aos participantes.

SOLUÇÃO DE REDES SEM FIOS E CABEADA

SISTEMA DE GERENCIAMENTO E CONTROLE DE ACESSO DE REDES SEM FIOS E CABEADA

Requisitos Gerais

2.8.275. A solução deverá ser dimensionada para operar no ambiente com os seguintes parâmetros:

2.8.275.1. A solução deverá operar para atender simultaneamente 400 usuários na instituição, sendo mandatória a solução permitir a autenticação destes usuários simultâneos, fornecendo, caso necessário, licenças para este processo de autenticação, conforme especificações do mecanismo de controle de acesso;

2.8.275.2. *Access points* devem ter funcionalidade de gerenciar outros *access points*, trabalhando em modo auto controlado (*cluster*);

2.8.275.3. Licenciamento contemplando o quantitativo mínimo de 100 (cem) dispositivos de rede, por meio de licença para autenticação de usuários no servidor TACACS+ interno;

2.8.276. Os equipamentos devem ter seu licenciamento completo e perpétuo;

2.8.277. O(s) sistema(s) de gerência e controle de acesso da rede sem fio deverão atender as especificações, a exemplo de, e não limitado a: serviço de autenticação, ferramenta de relatórios, software de gestão e inventário de ativos, sistema de prevenção de intrusões em redes sem fios (Wireless Intrusion Prevention System - WIPS). Caso necessário, a fim de atender aos requisitos, poderá o fornecedor entregar controladora física ou virtual.

2.8.277.1. Os eventuais módulos adicionais providos para o atendimento das especificações técnicas serão do mesmo fabricante, por questão de integração e compatibilidade completa da solução.

2.8.277.2. As licenças entregues deverão ser bidirecionais sempre que aplicável. Ou seja, caso haja necessidade de que o fornecedor entregue a licença "ABC" na controladora e a "XYZ" no *access point* para o funcionamento adequado da funcionalidade, ambas serão entregues.

2.8.278. A gerência da rede wireless será provida na forma de solução virtualizada (*virtual appliance*), compatível com o *hypervisor* VMWare;

2.8.279. As funcionalidades deverão ser disponíveis integralmente para os usuários e dispositivos do dimensionamento acima. Ou seja, é proibida a entrega de funcionalidades com atendimento parcial (Ex.: módulo "ABC" que atenda até 10 usuários, em vez dos 400 descritos acima);

2.8.280. Não serão aceitos equipamentos em modo *End of Support* durante a vigência da garantia e que estejam em modo *End of Life* no ato da assinatura da ata de registro de preços, não deixando de atender à vigência da garantia.

2.8.280.1. Se o equipamento ofertado não atenda a este requisito, será aceito equipamento de capacidade técnica igual ou superior, da mesma série ou linha ou família, desde que atenda a todos os requisitos técnicos do edital.

2.8.281. Todo e qualquer componente da solução (ex.: ferramenta de gerência, centralizador de *logs*, gerador de relatórios, sensor, etc) necessário para o atendimento dos requisitos técnicos deverá ser compatível com o *hypervisor* VMWare;

2.8.281.1. Caso haja necessidade de licenciamentos quaisquer diversos aos citados acima, como sistema gerenciador de bancos de dados (Ex.: MS SQL, Oracle), sistema operacional (Windows Server, Suse Linux, Red

Hat) ou outro tipo de dependência que enseje custos, deverão ser entregues pelo fornecedor como parte da solução.

Software de gerência/controladora WLAN

2.8.282. Solução local (*appliance virtual*), responsável pelas seguintes funções na rede sem fio: administração, configuração e gerenciamento completo centralizado dos pontos de acesso *wifi* também descritos na solução.

2.8.283. A controladora/ software de gerência deverá ser do mesmo fabricante do ponto de acesso a fim de garantir uma perfeita interoperabilidade.

2.8.284. Seja por meio da controladora ou por meio do software de gerenciamento, deve ser fornecida solução que comporte o gerenciamento de no mínimo 50 (cinquenta) pontos de acesso e gerenciar no mínimo 800 (oitocentos) usuários simultâneos.

2.8.285. Deverá ser fornecido o licenciamento para gerenciamento de 20 pontos de acesso, conforme quantitativo de Access points exigidos;

2.8.286. Caso a licitante esteja fornecendo controladora, e seja necessária uma expansão futura das capacidade da controladora WLAN (física ou virtual), o licenciamento para gerenciamento dos pontos de acesso deverá ser reaproveitado, adicionando a diferença de licença dos novos quantitativos exigidos de pontos de acesso e licenciamento/troca de hardware para comportar o aumento de capacidade de gerenciamento das controladoras.

2.8.287. Oferecer recursos de mobilidade entre VLANs para *roaming* de camada 2;

2.8.288. Implementar roaming (deslocamento) baseado nos protocolos IEEE 802.11r, 802.11k e 802.11v;

2.8.289. A Controladora WLAN poderá estar diretamente e/ou remotamente conectada aos Ponto de Acesso Sem Fio por ela gerenciadas, inclusive via roteamento nível 3 da camada OSI;

2.8.290. Se a Controladora WLAN falhar, os *access points* relacionados deverão se associar a uma Controladora WLAN alternativa de forma automática, não permitindo que a rede sem fio se torne inoperante;

2.8.291. Deve realizar o *upgrade* de *softwares* dos pontos de acesso *wifi*.

2.8.292. Deve implementar agendamento automático de upgrades de firmware dos Access Points (APs).

2.8.293. Deve efetuar backups automáticos das configurações e arquivos.

2.8.294. Deve disponibilizar uma console de gerenciamento web acessível através de protocolo HTTPS, compatível com os principais browsers do mercado (Firefox e Chrome).

Requisitos de autenticação de usuários e visitantes (captive portal)

2.8.295. Caso seja necessário componente externo à controladora, ele deverá ser baseado nas mesmas características de virtualização e licenciamento descritas acima, devendo ser do mesmo fabricante da solução ofertada;

2.8.296. Deve ser capaz de ocultar o rótulo de identificação (SSID) de redes;

2.8.297. Deve permitir a limitação de banda para uma rede;

2.8.298. Deve disponibilizar pelo menos 03 (três) níveis de acesso à Console de Gerenciamento Web, sendo:

2.8.298.1. Administrador: acesso de leitura e escrita às configurações para o gerenciamento do sistema.

2.8.298.2. Operador: acesso de apenas leitura às configurações para a monitoria, sem permissão para alterar configurações.

- 2.8.298.3. Organizador de Visitantes: acesso e permissão exclusiva para criação de usuários temporários e visitantes para acesso a rede Wi-Fi.
- 2.8.299. Deve permitir a criação de múltiplas redes distintas e segregadas, mas administradas na mesma console.
- 2.8.300. Deve permitir que as contas de usuários visitantes sejam armazenadas internamente na solução, não havendo necessidade de criação de usuários temporários em bases externas;
- 2.8.301. Implementar protocolo de autenticação para controle do acesso administrativo ao equipamento com mecanismos de AAA;
 - 2.8.301.1. Deve implementar recursos que permitam mecanismo de autenticação através de portal Web customizável (captive portal customizável) para clientes visitantes.
 - 2.8.301.2. Este mecanismo deve permitir ainda que o cliente visitante crie a sua própria conta de usuário, cuja validação deve ser realizada por meio de mensagem a ser enviada ao visitante durante o cadastro.
 - 2.8.301.3. No caso de a solução gerar um usuário e/ou senha automaticamente, estes dados devem ser informados ao visitante através de e-mail, SMS, ou captive portal.
 - 2.8.301.4. Todo o processo deve ser realizado sem a intervenção do administrador da solução que controla a solução wireless (self-service).
- 2.8.302. Deve possuir captive portal web de autenticação do tipo splash page.
 - 2.8.302.1. Caso não haja possibilidade de integração, serão aceitas soluções integradas com outros softwares de acesso, do mesmo fabricante, sem custos extras ao ITI.
- 2.8.303. A solução deve suportar no mínimo os seguintes métodos de autenticação:
 - 2.8.303.1. WEP
 - 2.8.303.2. WPA
 - 2.8.303.3. WPA2-PSK
 - 2.8.303.4. WPA2-Enterprise with 802.1X
 - 2.8.303.5. WPA3
 - 2.8.303.6. EAP-TLS
 - 2.8.303.7. Autenticação por *MAC address* (para dispositivos não compatíveis com o padrão 802.1x).
- 2.8.304. Deve exigir que o usuário visitante aceite o “Termo de uso da rede” a cada login ou apenas no primeiro login;
- 2.8.305. Deve permitir que a customização da página de registro de visitantes para campos relacionados a confirmação de *sponsorship*;
- 2.8.306. Deve permitir o gerenciamento das credenciais de visitantes;
- 2.8.307. Deve permitir a configuração de contas de usuários visitantes com prazo de validade e largura de banda;
- 2.8.308. Deve realizar o caching de endereço MAC dos usuários visitantes;
- 2.8.309. Deve permitir o login automático de usuários que realizem o auto-registro;
- 2.8.310. Deve permitir a autenticação de usuário anônimo sem necessidade de prover usuário e senha;
- 2.8.311. Deve permitir a criação de token de acesso;
- 2.8.312. Deve permitir a criação e gerenciamento de múltiplas contas de usuários visitantes;
- 2.8.313. Deve permitir autenticação através de social login nativa na solução;

- 2.8.314. Implantar o padrão 802.1x.
- 2.8.315. A ferramenta deverá fornecer servidor RADIUS e servidor TACACS+ para o serviço de AAA;
- 2.8.316. A ferramenta deverá implementar mecanismos de análise de dispositivos, caracterizando o tipo do dispositivo e infraestrutura com critérios pre definidos (device fingerprint);

Requisitos de gerenciamento e controle de acesso do ambiente

- 2.8.317. A controladora deve permitir a visualização de um conjunto de informações de análise dos Access Points que fazem parte da rede wireless, disponibilizando pelo menos as seguintes informações:
 - 2.8.317.1. Relação dos Access Points conectados, disponibilizando no mínimo as informações de Nome, MAC Address, Modelo de equipamento e endereço IP.
 - 2.8.317.2. Ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em performance;
 - 2.8.317.3. Quantidade de dispositivos conectados em cada Access Point, volume de dados utilizado, tempo de disponibilidade e SSIDs.
 - 2.8.317.4. Localização dos Access Points em planta baixa inserida no sistema, incorporando informações sobre os equipamentos gerenciados.
- 2.8.318. Deve dispor de alarmes e eventos acerca das configurações dos pontos de acesso para auditoria;
- 2.8.319. Deve permitir a visualização de um conjunto de informações dos dispositivos conectados à rede wireless, disponibilizando pelo menos os dados abaixo especificados:
 - 2.8.319.1. Endereço IP, MAC Address, Hostname, Usuário;
 - 2.8.319.2. Sistema Operacional do dispositivo utilizado;
 - 2.8.319.3. Tempo de conexão;
 - 2.8.319.4. Informação do SSID e Ponto de Acesso utilizados;
 - 2.8.319.5. Gráficos ou Dados de utilização dos Usuários;
 - 2.8.319.6. Últimos alertas do sistema;
 - 2.8.319.7. Informações de destinos acessados.
- 2.8.320. Deve possibilitar o agrupamento dos Access Point suportando a criação e o gerenciamento de grupos de Access Point simultâneos.
- 2.8.321. Deve guardar os logs por um período de no mínimo 3 (três) meses ou suportar envio dos logs no formato Syslog;
- 2.8.322. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- 2.8.323. Possuir suporte a MIB II, conforme RFC 1213.

Análise de perfil de dispositivo

- 2.8.324. Deve implementar funcionalidade de classificação automática criando perfis de dispositivos, de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;
- 2.8.325. Deve categorizar os dispositivos em pelo menos 3 níveis:
 - 2.8.325.1. Por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.);

- 2.8.325.2. Por sistema operacional (ex. Windows, Linux, MacOS, etc.);
- 2.8.325.3. Versão do sistema operacional (ex. Windows 7, Windows 2008 Server, etc.);
- 2.8.326. Deve ser capaz de gerar gráficos das categorias separando os dispositivos conforme suas características;
- 2.8.327. Deve suportar a coleta de informações, para classificação, usando no mínimo:
 - 2.8.327.1. DHCP;
 - 2.8.327.2. HTTP User-Agent;
 - 2.8.327.3. MAC OUI;
 - 2.8.327.4. ActiveSync plugin;
 - 2.8.327.5. SNMP;
 - 2.8.327.6. Subnet Scanner;
 - 2.8.327.7. IF-MAP;
 - 2.8.327.8. MDM;
 - 2.8.327.9. TCP Fingerprinting.
- 2.8.328. Deve possuir dicionário de categorias de dispositivos pré-configurado e mecanismo de atualização do mesmo;
- 2.8.329. Deve suportar a integração com, no mínimo, as seguintes soluções de MDM de mercado AirWatch, MobileIron, SAP Afaria, MaaS 360 devendo comprovar a compatibilidade em documentação oficial do fabricante;
- 2.8.330. Deve permitir priorização na ordem de criação dos perfis com no mínimo as seguintes características:
 - 2.8.330.1. Agente proprietário;
 - 2.8.330.2. HTTP User-Agent;
 - 2.8.330.3. SNMP;
 - 2.8.330.4. DHCP;
 - 2.8.330.5. MAC OUI.
- 2.8.331. A solução de análise de perfil de usuários deverá permitir consultas a sua base, pela solução de controle de acesso para validação de dispositivos com base no seu perfil.

Controle de acesso de dispositivos e usuários

- 2.8.332. A Solução deverá dar suporte a no mínimo as seguintes bases de dados:
 - 2.8.332.1. Microsoft Active Directory;
 - 2.8.332.2. Diretórios LDAP;
 - 2.8.332.3. PostgreSQL;
 - 2.8.332.4. MSSQL;
 - 2.8.332.5. Servidores de Token;
 - 2.8.332.6. Lista interna estática de hosts.
- 2.8.333. Deve suportar "Single Sign-on" (SSO) através de SAML;

2.8.334. Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

2.8.334.1. Atributos do usuário autenticado;

2.8.334.2. Hora do dia, dia da semana;

2.8.334.3. Tipo de dispositivo utilizado;

2.8.334.4. Localização do usuário;

2.8.334.5. Tipo de autenticação utilizada.

2.8.335. Deve permitir a visualização de todas informações relativas a cada transação e autenticação, a solução deverá trazer no mínimo as seguintes informações:

2.8.335.1. Data e Hora;

2.8.335.2. Mac Address do dispositivo;

2.8.335.3. Classificação do dispositivo;

2.8.335.4. Usuário;

2.8.335.5. Método de autenticação utilizado;

2.8.335.6. Fonte de autenticação utilizada para validação;

2.8.335.7. Perfil de acesso aplicado;

2.8.335.8. Atributos de entrada do protocolo utilizados na requisição (ex. RADIUS);

2.8.335.9. Informações de resposta da solução para o elemento de rede;

2.8.335.10. Alertas em caso de falha;

2.8.336. Deve possuir Dashboard customizável, onde deve permitir a visualização de no mínimo as seguintes informações:

2.8.336.1. Lista com últimos Alertas do sistema;

2.8.336.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Autenticações Web;

2.8.336.3. Gráfico com o status das autenticações aceitas e rejeitadas nos últimos 7 dias;

2.8.336.4. Gráfico com a categorização dos dispositivos classificados pela solução, divididos de acordo com as categorias de classificação;

2.8.336.5. Últimas falhas de autenticação;

2.8.336.6. Gráfico com as requisições de avaliação de postura dos dispositivos, divididos em:

1. Saudáveis (dentro das políticas estabelecidas);

2. Não saudáveis (que estão fora das políticas estabelecidas);

2.8.336.7. Lista com as últimas autenticações;

2.8.336.8. Lista com as últimas autenticações com sucesso;

2.8.336.9. Utilização de CPU do sistema, no mínimo nos últimos 30 minutos;

2.8.337. Deve possuir base de regras e categorias de dispositivos pré-configurada e mecanismo de atualização da mesma;

2.8.338. Deve suportar a integração com no mínimo as seguintes soluções de MDM de mercado AirWatch, MobileIron, SAP Afaria, MaaS 360 devendo comprovar a compatibilidade em documentação oficial

do fabricante;

- 2.8.339. Deve suportar autenticações via OAuth2 e Facebook;
- 2.8.340. Deve possuir recursos integrados de AAA: RADIUS, TACACS+ e Kerberos;
- 2.8.341. Deve possuir suporte aos seguintes recursos:
 - 2.8.341.1. RADIUS;
 - 2.8.341.2. RADIUS CoA;
 - 2.8.341.3. TACACS+;
 - 2.8.341.4. Web authentication;
 - 2.8.341.5. SAML;
 - 2.8.341.6. EAP-TLS;
 - 2.8.341.7. MAC address authentication (dispositivos sem suporte a 801X);
- 2.8.342. Deve suportar verificação de vulnerabilidade através de varredura de portas;
- 2.8.343. Deve suportar à aplicação de políticas em ambiente com múltiplos fornecedores de Wireless, cabeado e VPN;
- 2.8.344. Deve possuir CA integrada, para geração de certificados para os dispositivos que forem se autenticar na rede;
- 2.8.345. Deve suportar à integração com plataforma de terceiros usando HTTP/RESTful API;
- 2.8.346. Deve permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários;
- 2.8.347. Deve possuir suporte a administração através de IPv6;
- 2.8.348. Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilização de usuários visitantes através de portal web seguro;
- 2.8.349. Deve implementar a criação de grupos de autorizadores com privilégios distintos de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;
- 2.8.350. Deve permitir realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;
- 2.8.351. Deve permitir a configuração do tempo de validade das credenciais, baseando-se na criação da conta ou no primeiro login da conta;
- 2.8.352. Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais e números para compor a senha.

SISTEMA DE CONTROLE DE ACESSO A REDES CABEADAS

Requisitos gerais

- 2.8.353. A solução deverá ser dimensionada para operar no ambiente com os seguintes parâmetros:
 - 2.8.353.1. A solução deverá operar para atender simultaneamente 20 usuários da instituição, sendo mandatória a solução permitir a autenticação destes usuários simultâneos, fornecendo, caso necessário, licenças para este processo de autenticação, conforme especificações do mecanismo de controle de acesso;

- 2.8.353.2. Licenciamento contemplando o quantitativo mínimo de 30 (trinta) dispositivos de rede, por meio de licença para autenticação de usuários no servidor TACACS+ interno;
- 2.8.354. Os equipamentos devem ter seu licenciamento completo e perpétuo;
- 2.8.355. O(s) sistema(s) de gerência e controle de acesso da rede deverão atender as especificações, a exemplo de, e não limitado a: serviço de autenticação, ferramenta de relatórios, software de gestão e inventário de ativos, sistema de controle de acesso a redes. Caso necessário, a fim de atender aos requisitos, poderá o fornecedor entregar controladora física ou virtual.
- 2.8.355.1. Os eventuais módulos adicionais providos para o atendimento das especificações técnicas serão do mesmo fabricante, por questão de integração e compatibilidade completa da solução.
- 2.8.355.2. As licenças entregues deverão ser bidirecionais sempre que aplicável. Ou seja, caso haja necessidade de que o fornecedor entregue a licença "ABC" na controladora e a "XYZ" nos *switches* para o funcionamento adequado da funcionalidade, ambas serão entregues.
- 2.8.356. A gerência da rede wireless será provida na forma de solução virtualizada (*virtual appliance*), compatível com o *hypervisor* VMWare;
- 2.8.357. As funcionalidades deverão ser disponíveis integralmente para os usuários e dispositivos do dimensionamento acima. Ou seja, é proibida a entrega de funcionalidades com atendimento parcial (Ex.: módulo "ABC" que atenda até 10 usuários, em vez dos 20 descritos acima);
- 2.8.358. Os equipamentos devem ter seu licenciamento completo e perpétuo;
- 2.8.359. Não serão aceitos equipamentos em modo *End of Support* durante a vigência da garantia e que estejam em modo *End of Life* no ato da assinatura da ata de registro de preços, não deixando de atender à vigência da garantia.
- 2.8.359.1. Se o equipamento ofertado não atenda a este requisito, será aceito equipamento de capacidade técnica igual ou superior, da mesma série ou linha ou família, desde que atenda a todos os requisitos técnicos do edital.
- 2.8.360. Todo e qualquer componente da solução (ex.: ferramenta de gerência, centralizador de *logs*, gerador de relatórios, sensor, etc) necessário para o atendimento dos requisitos técnicos deverá ser compatível com o *hypervisor* VMWare;
- 2.8.360.1. Caso haja necessidade de licenciamentos quaisquer diversos aos citados acima, como sistema gerenciador de bancos de dados (Ex.: MS SQL, Oracle), sistema operacional (Windows Server, Suse Linux, Red Hat) ou outro tipo de dependência que enseje custos, deverão ser entregues pelo fornecedor como parte da solução.

Análise de perfil de dispositivo

- 2.8.361. Deve implementar funcionalidade de classificação automática criando perfis de dispositivos, de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;
- 2.8.362. Deve categorizar os dispositivos em pelo menos 3 níveis:
- 2.8.362.1. Por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.);
- 2.8.362.2. Por sistema operacional (ex. Windows, Linux, MacOS, etc.);
- 2.8.362.3. Versão do sistema operacional (ex. Windows 7, Windows 2008 Server, etc.);
- 2.8.363. Deve ser capaz de gerar gráficos das categorias separando os dispositivos conforme suas características;
- 2.8.364. Deve suportar a coleta de informações, para classificação, usando no mínimo:
- 2.8.364.1. DHCP;

- 2.8.364.2. HTTP User-Agent;
- 2.8.364.3. MAC OUI;
- 2.8.364.4. ActiveSync plugin;
- 2.8.364.5. SNMP;
- 2.8.364.6. Subnet Scanner;
- 2.8.364.7. IF-MAP;
- 2.8.364.8. MDM;
- 2.8.364.9. TCP Fingerprinting.
- 2.8.365. Deve possuir dicionário de categorias de dispositivos pré-configurado e mecanismo de atualização do mesmo;
- 2.8.366. Deve suportar a integração com, no mínimo, as seguintes soluções de MDM de mercado AirWatch, MobileIron, SAP Afaria, MaaS 360 devendo comprovar a compatibilidade em documentação oficial do fabricante;
- 2.8.367. Deve permitir priorização na ordem de criação dos perfis com no mínimo as seguintes características:
 - 2.8.367.1. Agente proprietário;
 - 2.8.367.2. HTTP User-Agent;
 - 2.8.367.3. SNMP;
 - 2.8.367.4. DHCP;
 - 2.8.367.5. MAC OUI.
- 2.8.368. A solução de análise de perfil de usuários deverá permitir consultas a sua base, pela solução de controle de acesso para validação de dispositivos com base no seu perfil.

Controle de acesso de dispositivos e usuários

- 2.8.369. A Solução deverá dar suporte a no mínimo as seguintes bases de dados:
 - 2.8.369.1. Microsoft Active Directory;
 - 2.8.369.2. Diretórios LDAP;
 - 2.8.369.3. PostgreSQL;
 - 2.8.369.4. MSSQL;
 - 2.8.369.5. Servidores de Token;
 - 2.8.369.6. Lista interna estática de hosts.
- 2.8.370. Deve suportar "Single Sign-on" (SSO) através de SAML;
- 2.8.371. Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:
 - 2.8.371.1. Atributos do usuário autenticado;
 - 2.8.371.2. Hora do dia, dia da semana;
 - 2.8.371.3. Tipo de dispositivo utilizado;
 - 2.8.371.4. Localização do usuário;

- 2.8.371.5. Tipo de autenticação utilizada.
- 2.8.372. Deve permitir a visualização de todas informações relativas a cada transação e autenticação, a solução deverá trazer no mínimo as seguintes informações:
 - 2.8.372.1. Data e Hora;
 - 2.8.372.2. Mac Address do dispositivo;
 - 2.8.372.3. Classificação do dispositivo;
 - 2.8.372.4. Usuário;
 - 2.8.372.5. Método de autenticação utilizado;
 - 2.8.372.6. Fonte de autenticação utilizada para validação;
 - 2.8.372.7. Perfil de acesso aplicado;
 - 2.8.372.8. Atributos de entrada do protocolo utilizados na requisição (ex. RADIUS);
 - 2.8.372.9. Informações de resposta da solução para o elemento de rede;
 - 2.8.372.10. Alertas em caso de falha;
- 2.8.373. Deve possuir Dashboard customizável, onde deve permitir a visualização de no mínimo as seguintes informações:
 - 2.8.373.1. Lista com últimos Alertas do sistema;
 - 2.8.373.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Autenticações Web;
 - 2.8.373.3. Gráfico com o status das autenticações aceitas e rejeitadas nos últimos 7 dias;
 - 2.8.373.4. Gráfico com a categorização dos dispositivos classificados pela solução, divididos de acordo com as categorias de classificação;
 - 2.8.373.5. Últimas falhas de autenticação;
 - 2.8.373.6. Gráfico com as requisições de avaliação de postura dos dispositivos, divididos em:
 - 1. Saudáveis (dentro das políticas estabelecidas);
 - 2. Não saudáveis (que estão fora das políticas estabelecidas);
 - 2.8.373.7. Lista com as últimas autenticações;
 - 2.8.373.8. Lista com as últimas autenticações com sucesso;
 - 2.8.373.9. Utilização de CPU do sistema, no mínimo nos últimos 30 minutos;
- 2.8.374. Deve possuir base de regras e categorias de dispositivos pré-configurada e mecanismo de atualização da mesma;
- 2.8.375. Deve suportar a integração com no mínimo as seguintes soluções de MDM de mercado AirWatch, MobileIron, SAP Afaria, MaaS 360 devendo comprovar a compatibilidade em documentação oficial do fabricante;
- 2.8.376. Deve suportar autenticações, no mínimo, via OAuth2 e Facebook;
- 2.8.377. Deve possuir recursos integrados de AAA: RADIUS, TACACS+ e Kerberos;
- 2.8.378. Deve possuir suporte aos seguintes recursos:
 - 2.8.378.1. RADIUS;
 - 2.8.378.2. RADIUS CoA;

- 2.8.378.3. TACACS+;
- 2.8.378.4. Web authentication;
- 2.8.378.5. SAML;
- 2.8.378.6. EAP-TLS;
- 2.8.378.7. MAC address authentication (dispositivos sem suporte a 801X);
- 2.8.379. Deve suportar verificação de vulnerabilidade através de varredura de portas;
- 2.8.380. Deve suportar à aplicação de políticas em ambiente com múltiplos fornecedores de Wireless, cabeado e VPN;
- 2.8.381. Deve possuir CA integrada, para geração de certificados para os dispositivos que forem se autenticar na rede;
- 2.8.382. Deve suportar à integração com plataforma de terceiros usando HTTP/RESTful API;
- 2.8.383. Deve permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários;
- 2.8.384. Deve possuir suporte a administração através de IPv6;
- 2.8.385. Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilização de usuários visitantes através de portal web seguro;
- 2.8.386. Deve implementar a criação de grupos de autorizadores com privilégios distintos de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;
- 2.8.387. Deve permitir realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;
- 2.8.388. Deve permitir a configuração do tempo de validade das credenciais, baseando-se na criação da conta ou no primeiro login da conta;
- 2.8.389. Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais e números para compor a senha.

ACCESS POINT

- 2.8.390. Deve implementar, no mínimo, as tecnologias 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac e 802.11ax, compatíveis as frequências de rádio 2,4Ghz e 5Ghz com irradiação omnidirecional, com as seguintes características:
 - 2.8.390.1. IEEE 802.11b: 11, 5.5, 2 e 1 Mbps;
 - 2.8.390.2. IEEE 802.11a e IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps;
 - 2.8.390.3. 802.11n (2.4GHz): 6.5 to 300 (MCS0 to MCS15, HT20 to HT40)
 - 2.8.390.4. 802.11n (5GHz): 6.5 to 600 (MCS0 to MVC31, HT20 to HT40)
 - 2.8.390.5. IEEE 802.11ac: 6,5 a 860 Mbps (MCS0 a MCS9, NSS=1 a 2 e VHT20 a VHT80);
 - 2.8.390.6. 802.11ax: 3,6 a 570 Mbps em 2,4 GHz;
 - 2.8.390.7. 802.11ax: 3.6 a 4,803 (MCS0 to MCS11, NSS = 1 to 4, HE20 to HE160)
 - 2.8.390.8. Deve possuir integração ZIGBEE e rádio bluetooth BLE 5.0 para utilização em serviços de localização com maior precisão. Não se faz necessária a entrega do software de localização, ficando a cargo da infraestrutura a compatibilidade e recurso disponíveis para futuras aquisições de software;

- 2.8.391. Implementar DFS (Dynamic Frequency Selection) para otimização do espectro de rádio frequência;
- 2.8.392. Implementar TWT (Target Wake Time);
- 2.8.393. Deverá conter todas as licenças necessárias para utilização conjunta das funcionalidades descritas na controladora, como: firewall, WIPS, autenticação, gerenciamento, relatórios e quaisquer outras para atendimento pleno dos requisitos da solução;
- 2.8.394. Deverão ser fornecidos pontos de acesso Wi-Fi idênticos, novos e sem uso anterior;
- 2.8.395. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento, na data de entrega da proposta;
- 2.8.396. Deve ser apresentado certificado válido fornecido pela Wi-Fi Alliance na categoria Wi-Fi CERTIFIED 6 na data do pregão contendo, no mínimo, as funcionalidades:
- 2.8.396.1. DL OFDMA;
- 2.8.396.2. UL OFDMA;
- 2.8.396.3. DL MU-MIMO; e
- 2.8.396.4. Target Wake Time (TWT).
- 2.8.397. A configuração dos seus parâmetros operacionais, o gerenciamento das políticas de segurança e de radiofrequência devem ser gerenciadas pela solução;
- 2.8.398. Deve possuir garantia de no mínimo 60 (sessenta) meses, pelo fabricante ou CONTRATADA.
- 2.8.399. Deve possibilitar a fixação do equipamento em teto e parede. Devem ser fornecidos todos os acessórios necessários para que possa ser feita a fixação.
- 2.8.400. Não deve haver restrição de licença que limite o número de usuários por Ponto de Acesso.
- 2.8.401. O modelo do equipamento ofertado deve possuir, na data da entrega da proposta, homologação junto à ANATEL.
- 2.8.402. Deve possuir no mínimo 01 (uma) porta Ethernet 2.5 multigigabit Ethernet BASE-T autosense, UTP RJ45;
- 2.8.403. Deve permitir ser alimentado através da tecnologia PoE.
- 2.8.403.1. Caso o aparelho seja compatível apenas com o padrão PoE+, a contratada deverá fornecer, sem custos adicionais, todos os recursos para o perfeito funcionamento do aparelho, como: injetores compatíveis com o modelo do *access point* ofertado (bivolt), cabos de força e de dados Cat6a e adaptadores.
- 2.8.404. Deverá ser fornecida e instalada a versão mais recente do software interno do ponto de acesso Wi-Fi.
- 2.8.405. Deve possuir captive portal web de autenticação do tipo splash page local ou em conjunto com a ferramenta de gerência.
- 2.8.406. Deve implementar recursos de *firewall*.
- 2.8.407. Deve suportar, no mínimo, 200 usuários conectados/autenticados por rádio.
- 2.8.408. Deve localmente ou em conjuntos com a solução de controladora wireless, implementar análise de espectro de RF em 2.4GHz e 5GHz para identificação de outros pontos de acesso intrusos e não autorizados (rogues), além de interferências no canal habilitado no ponto de acesso e nos demais canais configurados na rede Wi-Fi. A análise de espectro deve ser realizada de forma simultânea ao atendimento dos clientes do ponto de acesso, sem que estes sejam desconectados.
- 2.8.409. Deve localmente ou em conjunto com a solução de controladora wireless, realizar o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF.

- 2.8.410. Ajustar automaticamente os canais 802.11 e realizar a detecção de interferências e reajustar os parâmetros de Rádio Frequência visando evitar problemas de cobertura e performance.
- 2.8.411. Deve permitir, simultaneamente, usuários configurados, no mínimo, nos padrões IEEE 802.11a, 802.11n, 801.11ac e 802.11ax;
- 2.8.412. Deve operar nas frequências de 2.4GHz e 5GHz;
- 2.8.413. Deve Operar com DFS (802.11h) e OFDMA;
- 2.8.414. Deve implementar protocolo CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance).
- 2.8.415. Ser compatível com os padrões WMM e 802.1p para priorização de tráfego.
- 2.8.416. Deve possuir capacidade para operação em modo "repetidor", permitindo a comunicação entre pontos de acesso Wi-Fi sem a necessidade de cabeamento adicional permitindo desta forma o atendimento de usuários em locais isolados da localidade.
- 2.8.417. Deve possuir cliente DHCP, para configuração automática do endereço IP.
- 2.8.418. Deve permitir a conexão à rede de usuários em IPv4, IPv6 e suportar dual-stack (clientes IPv4 e IPv6 no mesmo ponto de acesso Wi-Fi).
- 2.8.419. Deve possuir a capacidade de criação de no mínimo 12 (doze) SSIDs.
- 2.8.420. Permitir habilitar e desabilitar a divulgação do SSID.
- 2.8.421. Deverá possuir mecanismo de rádio com suporte à MIMO 4x4, com 4 *Spatial Streams*, no mínimo para o rádio de 5GHz;
- 2.8.422. Possuir LED's indicativos do estado de operação e da atividade do rádio;
- 2.8.423. O software interno e os arquivos de configuração devem ser armazenados em memória não-volátil, permitindo a sua atualização via solução de controladora wireless.
- 2.8.424. Permitir o uso do protocolo de autenticação IEEE 802.1X para no mínimo EAP-TLS e EAP-PEAP.
- 2.8.425. Deve implementar WPA2 com AES.
- 2.8.426. Deve ser compatível com o padrão IEEE 802.11i.
- 2.8.427. Deve implementar WPA3 Enterprise.
- 2.8.428. Deve permitir a implantação de VLANs segundo o padrão IEEE 802.1Q;
- 2.8.429. Deve permitir a configuração de no mínimo 8 (oito) VLANs.
- 2.8.430. Deve implementar a técnica de direcionamento de banda, permitindo que clientes com suporte a faixa de frequência de 5 GHz se conectem aos Pontos de Acesso utilizando, preferencialmente, a faixa de 5 GHz.
- 2.8.431. Deve implementar o protocolo NTP (Network Time Protocol) ou o protocolo SNTP (Simple Network Time Protocol) em modo cliente.
- 2.8.432. Deve implementar o envio de eventos por meio do protocolo Syslog.
- 2.8.433. Deve implementar controle de limite de uso de banda.

Instalação dos *access points*

- 2.8.434. Os Pontos de Acesso deverão ser renomeados de acordo com o ambiente onde será instalado, conforme definição da contratante;
- 2.8.435. Antes da fixação, o técnico da contratada deverá registrar os equipamentos que serão instalados, para controle dos equipamentos (número de série e MAC address);

- 2.8.436. A contratada é responsável pela fixação do *access point*;
- 2.8.437. A contratada deverá realizar a passagem de cabos entre o ponto onde os *access points* serão instalados e a porta de comunicação do *switch* de distribuição indicado pela contratante para conexão física na rede;
- 2.8.437.1. O ponto de rede será entregue certificado pela contratada;
- 2.8.438. A contratante disponibilizará o ambiente computacional para a instalação dos componentes da infraestrutura de rede *wifi*, respeitados os requisitos técnicos a serem entregues pela contratada;
- 2.8.439. A contratada deverá instalar e energizar o Ponto de Acesso *wifi* em local indicado pela contratante fixando-o no local determinado;
- 2.8.440. a contratada deverá aplicar nos *access points* as políticas configuradas na gerência da solução; o técnico da contratada deverá conectar o Ponto de Acesso ao ponto lógico indicado. Após a fixação do AP com o kit de instalação, o técnico deverá tirar fotos da instalação para finalizar o serviço. As fotos deverão ser encaminhadas para validação final da equipe de fiscalização.
- 2.8.441. Ao final do processo, a contratada deverá entrar em contato com a equipe da contratante para validação da instalação.
- 2.8.442. A infraestrutura de cabeamento será de responsabilidade da contratada.
- 2.8.442.1. Todos os cabos de dados *Ethernet* da solução entregues pela contratada serão todos do padrão Cat6 ou superior, e atender ao padrão TIA/EIA 568-A.

Treinamento da rede sem fios

- 2.8.443. Oferecer treinamento para operacionalização do ambiente de rede sem fios (planejamento, instalação, configuração, operação, suporte e *troubleshooting*) com conteúdo teórico e atividades práticas, utilizando interfaces gráficas e linhas de comando (comand-line interface - CLI). A duração mínima de será de 40 (quarenta) horas e atenderá a 10 pessoas.
- 2.8.444. Os treinamentos deverão ser realizados em local situado na cidade de Brasília, nas dependências da CONTRATADA.
- 2.8.445. A CONTRATADA deverá fornecer o treinamento no período de vigência do contrato, no máximo até 30 (trinta) dias após pedido da CONTRATANTE.
- 2.8.446. A Contratada deverá fornecer material de treinamento e deverá ser ministrado por profissional certificado pelo fabricante do equipamento.

SERVIÇO DE CONFIGURAÇÃO DO SISTEMA DE GERENCIAMENTO E CONTROLE DE ACESSO DE REDES SEM FIOS E CABEADA

- 2.8.447. A instalação será feita em qualquer um dos prédios de lotação da contratante em Brasília;
- 2.8.448. A contratada deverá executar Site Survey via software ou Indoor no prédio da contratante, conforme solicitação, podendo ser solicitada inspeção física do ambiente.
- 2.8.449. A instalação dos Ponto de Acesso Sem Fio deverá ser posterior a este Site Survey, apoiada por software adequado, que indique:
- 2.8.449.1. O melhor posicionamento dos dispositivos para a maximização da cobertura do sinal de radiofrequência nos espectros 802.11 a/b/g/n/ac/ax;
- 2.8.449.2. A quantidade exata de pontos de acesso a serem instalados por ambiente;

- 2.8.449.3. As zonas de interferência;
- 2.8.449.4. A frequência a ser utilizada por cada ponto de acesso;
- 2.8.449.5. As áreas de cobertura;
- 2.8.449.6. As taxas de transmissão ou faixas de níveis de recepção de sinal de RF em desenho colorido.
- 2.8.450. A potência mínima aceita para o dimensionamento do quantitativo de *access points* é de -65 dBm.
- 2.8.450.1. A instalação não será aceita se houver pontos de sombras ou com sinal fraco nas instalações da contratada.
- 2.8.451. A empresa licitante interessada deverá solicitar as plantas de referência do prédio para endereço eletrônico cotic@iti.gov.br e realizar *site survey* preditivo, a fim de estimar a qualidade do sinal e quantitativo de equipamentos propostos;
- 2.8.451.1. O *site survey* preditivo fará parte da proposta de preços para a solução de *wifi*, tendo o sinal mínimo de -65dBm;
- 2.8.451.2. Por questões de eventuais mudanças nos *layouts* das salas, a CONTRATADA deverá realizar novo levantamento durante o planejamento da implantação;
- 2.8.452. As atividades contempladas pelo serviço de instalação incluem: planejamento, instalação física e configuração lógica dos pontos de acesso e da controladora wireless;
- 2.8.453. Deverá ser elaborado pela contratada um plano de implantação contendo todo o detalhamento de implantação dos produtos;
- 2.8.454. O plano deverá contemplar o diagrama lógico da rede com todos os equipamentos envolvidos na solução e as configurações lógicas que serão realizadas em cada equipamento e software;
- 2.8.455. A CONTRATADA deverá criar e disponibilizar o cronograma das atividades para aprovação da CONTRATANTE;
- 2.8.456. A CONTRATADA terá o prazo de 90 (noventa) dias após a abertura da ordem de serviços para implantar e deixar o projeto de redes sem fios em pleno funcionamento.
- 2.8.457. Deverá configurar na contratada redes ao menos:
- 2.8.457.1. Rede para usuários internos, utilizando o algoritmo WPA2 com a base de autenticação ou certificados digitais, a critério da CONTRATANTE;
- 2.8.457.2. Rede para dispositivos corporativos, autenticado utilizando certificados digitais;
- 2.8.457.3. Rede para visitantes, utilizando cadastro do cidadão via registro local.
- 2.8.458. Configurar o portal de acesso (captive portal) de visitantes e elaborar manuais de utilização para o cadastrador de usuários e para o usuário final.
- 2.8.459. Para a rede cabeada, os equipamentos serão configurados e implantados para gerenciar os ativos corporativos mediante autenticação forte, postura (conformidade) com rede segregada para quarentena, 802.1x dos *switches*, habilitação dos dashboards de monitoramento, implantação do serviço TACACS da solução e da CA (se aplicável).

Treinamento para o sistema de controle de acessos

- 2.8.460. Oferecer treinamento para operacionalização do sistema de controle de acesso para redes sem fios e cabeadas (planejamento, instalação, configuração, operação, suporte e *troubleshooting*) com conteúdo teórico e atividades práticas, utilizando interfaces gráficas e linhas de comando (comand-line interface - CLI). A duração mínima de será de 40 (quarenta) horas e atenderá a 10 pessoas.

2.8.461. Os treinamentos deverão ser realizados em local situado na cidade de Brasília, nas dependências da CONTRATADA.

2.8.462. A CONTRATADA deverá fornecer o treinamento no período de vigência do contrato, no máximo até 30 (trinta) dias após pedido da CONTRATANTE.

2.8.463. A Contratada deverá fornecer material de treinamento e deverá ser ministrado por profissional certificado pelo fabricante do equipamento.

SERVIÇO DE CONFIGURAÇÃO DO SISTEMA DE CONTROLE DE ACESSO A REDES CABEADAS

2.8.464. Para a rede cabeada, os equipamentos serão configurados e implantados para gerenciar os ativos corporativos mediante autenticação forte, postura (conformidade) com rede segregada para quarentena, 802.1x dos *switches*, habilitação dos dashboards de monitoramento, implantação do serviço TACACS da solução e da CA (se aplicável).

TREINAMENTO OFICIAL DO FABRICANTE DA SOLUÇÃO DE CONTROLE DE ACESSO

2.8.465. O treinamento oficial do fabricante do sistema de controle de acesso (sem fios e cabeada) será de, no mínimo, 40 horas, em português.

2.8.466. O treinamento será realizado preferencialmente no modelo presencial, em instalações providas pela CONTRATADA.

2.8.466.1. Os treinamentos só serão aceitos na modalidade à distância se:

1. Por impossibilidade logística devido à pandemia de COVID-19;
2. Por interesse e oportunidade da Administração.

2.8.467. Deve ser ministrado por profissional certificado pelo fabricante dos equipamentos como instrutor.

2.8.468. A ementa do curso deve abranger conteúdos que vão desde instalação, configuração, gerenciamento, operação a *troubleshooting* dos equipamentos de hardware e de softwares que compõem a solução de redes sem fios.

2.8.469. Os treinamentos deverão ser realizados no Brasil, em português, na modalidade presencial, em local fornecido pela CONTRATADA.

2.8.470. O local de treinamento deverá possuir todas as facilidades para um perfeito desempenho das atividades, incluindo os recursos áudio visuais e laboratórios necessários, sem ônus à CONTRATANTE.

2.8.471. A empresa disponibilizará material em formato digital (PDF) aos participantes e quaisquer conteúdos e ferramentas adicionais que venham a ser necessárias para o treinamento.

2.8.472. Os cursos referentes a equipamentos e softwares que façam parte do objeto deverão usar o material oficial de treinamento do respectivo fabricante por meio de qualquer um dos seus respectivos centros autorizados de treinamento.

2.8.473. Caso não haja disponibilidade para realização em Brasília, a empresa custeará os gastos de passagens e estadia para o centro de treinamento mais próximo de Brasília.

2.8.474. Deverá ser fornecido certificado de conclusão oficial do fabricante da solução aos participantes.

SWITCHES CORE

Características gerais

- 2.8.475. Deverão ser fornecidos 2 (dois) equipamentos para compor o *Cluster* da camada *core*;
- 2.8.476. Deve possuir no mínimo 48 portas 1/10GbE padrão SFP/SFP+;
- 2.8.476.1. Todas as portas óticas deverão conter *transceivers* compatíveis (10G Base-SR) com as especificações das portas para distância mínima de 300 metros;
- 2.8.477. Deve possuir no mínimo 4 portas 40 GbE padrão QSFP+;
- 2.8.477.1. Deve ser entregue com cabos do tipo DAC de no mínimo 1 metro de comprimento de 40Gbps de velocidade de conexão suficientes para todas as portas 40GbE dos equipamentos;
- 2.8.478. Caso a solução utilize KeepAlive, deve ser entregue com 01(um) cabo adicional do tipo DAC de no mínimo 3 metros de comprimento de 10Gbps de velocidade de conexão;
- 2.8.479. Qualquer que seja o equipamento ofertado, mesmo que este possua número superior de portas exigidas, deverá ter todas as portas de comunicação (downlink e uplink) habilitadas e licenciadas.
- 2.8.480. Deve possuir fontes de alimentação e ventiladores do tipo hot-swappable que possam ser trocados sem que seja necessário desligar o equipamento ou interromper seu funcionamento.
- 2.8.481. A arquitetura deve permitir “Cluster” de Switches (par de switches) em que dois (02) switches interligados operem em conjunto.
- 2.8.482. Deve implementar a solução de MC-LAG (Multi Chassis Link Aggregation Group) ou tecnologia semelhante que possibilite funcionalidade idêntica, em que mesmo havendo conexões entre diferentes equipamentos pertencentes ao mesmo par de switches, seja disponibilizado somente um único caminho lógico e agregado de comunicação, eliminando desta forma a necessidade do uso do protocolo STP (Spanning Tree Protocol).
- 2.8.482.1. Não serão aceitas soluções em condição de empilhamento ou em cascadeamento;
- 2.8.483. O par de switches deve operar em alta-disponibilidade e possibilitar o upgrade de software sem que haja a parada do ambiente, com a mudança de tráfego entre os switches, caso necessário;
- 2.8.484. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
- 2.8.485. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;
- 2.8.486. Deverá ser fornecido um jogo de manuais originais dos equipamentos fornecidos, preferencialmente em língua portuguesa, contendo informações sobre as suas características técnicas, configurações, programação, montagem, instalação, manutenção, operação e gerenciamento de todas as funcionalidades fornecidas. Toda documentação dos equipamentos fornecidos será fornecida tanto na forma impressa como também em mídia digital, na forma de arquivos eletrônicos;
- 2.8.487. Os equipamentos, materiais e produtos a serem fornecidos deverão atender a todas as Normas e Resoluções da Agência Nacional de Telecomunicações - ANATEL de acordo com a Resolução nº 242 ou superior;
- 2.8.488. Todas as versões de sistema operacional ou software armazenado no equipamento deverão ser fornecidos nos releases mais atualizados, adequadas às necessidades requeridas nesta especificação, fornecidas se disponíveis na mídia CD-ROM. Durante a vigência da garantia / suporte técnico será prevista a atualização do Sistema Operacional do equipamento dentro da mesma versão por outra mais atualizada visando manter o equipamento atualizado e livre de bugs, falhas de segurança etc;
- 2.8.489. Deverão ser fornecidos todos os softwares, cabos de força e lógicos, conectores, adaptadores, acessórios de fixação, necessários para o pleno funcionamento do equipamento;
- 2.8.490. Os equipamentos fornecidos deverão ser novos, estar em produção (não serão aceitos equipamentos já descontinuados pelo fabricante) e estar nas condições originais de fabricação, ou seja, sem

modificação, retirada ou acréscimo de componentes externos e / ou internos à montagem original do fabricante;

2.8.491. Todos os equipamentos e seus acessórios deverão estar na embalagem original do fabricante. Todos os acessórios básicos que acompanham os equipamentos deverão ser fornecidos;

2.8.492. Deve vir acompanhado do kit de suporte específico para montagem em Rack de 19";

2.8.493. Operar nas temperaturas de 0 a 40 °C;

2.8.494. Deverá possuir fontes de alimentação internas com alimentação através de circuitos elétricos de entrada distintos, para tensão de 110/220 VAC a 60 Hz, com capacidade para implementar a configuração máxima do chassi, e redundância n+1 instalada- 01(uma) fonte extra de redundância;

Desempenho

2.8.495. Deve possuir capacidade de comutação de, no mínimo, 2 Tbps;

2.8.496. Deve possuir capacidade de encaminhamento de, no mínimo, 900 MPPS;

Disponibilidade

2.8.497. Deve possuir interface de Console Serial ou USB;

2.8.498. Deve possuir uma porta para gerenciamento out-of-band com conector RJ-45;

2.8.499. Deve implementar 803ad Agregação de Links com mínimo de 54 grupos de 8 portas;

2.8.500. Deve possuir buffers de, no mínimo, 16MB;

Switching

2.8.501. Deve implementar funcionalidade que permita a detecção de links unidirecionais;

2.8.502. Deve implementar funcionalidade que permita a detecção de falhas de uplink;

2.8.503. Deve implementar, no mínimo, 4.000(quatro mil) VLANs, conforme padrão IEEE 801q;

2.8.504. Deve implementar os seguintes padrões IEEE 801D, 801W, 801S, 801P

2.8.505. Deve Implementar JUMBO FRAME (mínimo de 9k) em todas as interfaces Gigabit Ethernet

2.8.506. Tabela de endereços MAC com capacidade para no mínimo 80.000 endereços MAC;

2.8.507. Deve implementar LLDP (IEEE 801ab)

2.8.508. Deve implementar o padrão IEEE801AK

2.8.509. Deve implementar MRVP

2.8.510. Deve implementar PVST+, RPVST+ ou protocolo compatível;

2.8.511. Deve implementar MSTP (IEEE 801s) com suporte a 64 instâncias;

2.8.512. Suportar tabela para pelo menos 90.000 hosts IPV4 e 45.000 Hosts IPV6.

Roteamento

2.8.513. Deve possuir tabela de roteamento com no mínimo 13.000 rotas IPv4 e 3.000 rotas IPv6;

2.8.514. Deve implementar roteamento estático;

2.8.515. Deve Implementar roteamento OSPFv2 e OSPFv3;

2.8.516. Deve implementar roteamento OSPFv2 NSSA;

- 2.8.517. Deve implementar roteamento OSPF com suporte a autenticação MD5 ou texto claro;
- 2.8.518. Deve implementar roteamento OSPF com ECMP (Equal Cost Multi Path) de no mínimo, 8 grupos;
- 2.8.519. Deve implementar OSPF com “Graceful Restart”, que permita o encaminhamento de pacotes mesmo que o software de OSPF seja reiniciado;
- 2.8.520. Deve implementar BGP;
- 2.8.521. Deve implementar PRB (Policy Based Routing)
- 2.8.522. Deve implementar VRRP (Virtual Router Redundancy Protocol);
- 2.8.523. Deve implementar DHCP Client e DHCP Relay
- 2.8.524. Deve suportar VRF (Virtual Routing and Forwarding) até 3 VRFs Routing
- 2.8.525. Deve implementar VRF Ipv4 e Ipv6;
- 2.8.526. Deve implementar funcionalidade que especifica o número máximo de entradas no ARP;
- 2.8.527. Deve implementar funcionalidade de proteção contra frames de BPDUs (spanning tree), no caso de recebimento de BPDUs, a porta deve ser colocada no estado de “down”

Multicast

- 2.8.528. Deve implementar PIM-SM;
- 2.8.529. Deve implementar IGMP nas versões v1 e v2 e Snooping
- 2.8.530. Deve implementar MLD Snooping;

Software Defined Networking

- 2.8.531. Deve possuir tecnologia que permite a separação do plano de dados (encaminhamento de pacotes) e do plano de controle;
- 2.8.532. Deve permitir a automação de tarefas de reconfiguração da rede mediante eventos que impactem o seu comportamento através de scripts internos ou ferramentas externas que neste caso devão ser fornecidas;
- 2.8.533. Deve ser totalmente programável em REST API
- 2.8.534. Deve permitir a automação de tarefas de reconfiguração da rede mediante eventos que impactem o seu comportamento através de scripts internos ou ferramentas externas que neste caso deverão ser fornecidas;
- 2.8.535. Deve possuir interface REST API e scripting via Python;
- 2.8.536. Deve possuir embarcado ferramenta customizável e programável para monitoração e análise de eventos que possa auxiliar na identificação e correção de problemas de redes, aplicações e eventos de segurança da informação. Caso não possua este recurso é possível entregar uma ferramenta similar, podendo ser composto por hardware ou software adicional;

QoS

- 2.8.537. Deve permitir a configuração do volume de broadcast, Multicast e unicast desconhecido aceito por porta, o excesso deve ser descartado;
- 2.8.538. Deve implementar rate-limiting;
- 2.8.539. Deve suportar espelhamento de portas;

- 2.8.540. Deve possuir algoritmos de enfileiramento SP e WRR ou WFQ;
- 2.8.541. Deve suportar no mínimo, 8 (oito) filas de prioridade por porta.

Segurança

- 2.8.542. Deve implementar ACL's Ipv4 e Ipv6;
- 2.8.543. Deve possuir RADIUS e TACACS+ para controle de gerenciamento do switch;
- 2.8.544. Deve suportar RADIUS/TACACS+

Gerenciamento

- 2.8.545. Deve suportar duas imagens de software na memória flash (IOS, Firmware);
- 2.8.546. Deve possuir capacidade de armazenar múltiplos arquivos de configuração;
- 2.8.547. Deve implementar sFlow (IPv4 e IPv6) ou similar;
- 2.8.548. Deve implementar TFTP, SFTP ou SCP para gerenciamento de software e configuração
- 2.8.549. Deve implementar SNMP v1, v2c e v3;
- 2.8.550. Deve possuir sincronização de horário (clock) do equipamento com servidor de tempo através do protocolo NTP ou SNTP
- 2.8.551. Deve suportar Self Signed Certificate Management
- 2.8.552. Deve suportar SSH v2
- 2.8.553. Deve Suportar AAA (TACACS+ & RADIUS)
- 2.8.554. Deve implementar CLI com gerência por meio de linhas de comando;

SWITCH TOPO DE RACK 48 PORTAS

Características gerais

- 2.8.555. Deve possuir no mínimo 48 portas 1/10GbE padrão UTP Base-T;
- 2.8.556. Deve possuir no mínimo 4 portas 40 GbE padrão QSFP+;
- 2.8.557. Deve ser entregue com cabos do tipo DAC de no mínimo 3 metros de comprimento de 40Gbps de velocidade de conexão suficientes para todas as portas 40GbE dos equipamentos;
- 2.8.558. Qualquer que seja o equipamento ofertado, mesmo que este possua número superior de portas exigidas, deverá ter todas as portas de comunicação (downlink e uplink) habilitadas e licenciadas.
- 2.8.559. Deve possuir fontes de alimentação e ventiladores do tipo hot-swappable que possam ser trocados sem que seja necessário desligar o equipamento ou interromper seu funcionamento
- 2.8.560. A arquitetura deve permitir "Cluster" de Switches (par de switches) em que dois (02) switches interligados operem em conjunto. Deve implementar a solução de MC-LAG (Multi Chassis Link Aggregation Group) ou tecnologia semelhante que possibilite funcionalidade idêntica, em que mesmo havendo conexões entre diferentes equipamentos pertencentes ao mesmo par de switches, seja disponibilizado somente um único caminho lógico e agregado de comunicação, eliminando desta forma a necessidade do uso do protocolo

STP (Spanning Tree Protocol). Não serão aceitas soluções em condição de empilhamento ou em cascadeamento;

2.8.561. Caso opere em cluster, deverá o par de switches operar em alta-disponibilidade e possibilitar o upgrade de software sem que haja a parada do ambiente, com a mudança de tráfego entre os switches, caso necessário;

2.8.562. Deve vir acompanhado do kit de suporte específico para montagem em Rack de 19";

2.8.563. Operar nas temperaturas de 0 a 40 °C;

2.8.564. Deverá possuir fontes de alimentação internas com alimentação através de circuitos elétricos de entrada distintos, para tensão de 110/220 VAC a 60 Hz, com capacidade para implementar a configuração máxima do chassi, e redundância n+1 instalada- 01(uma) fonte extra de redundância;

2.8.565. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;

2.8.566. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;

2.8.567. Deverá ser fornecido um jogo de manuais originais dos equipamentos fornecidos, preferencialmente em língua portuguesa, contendo informações sobre as suas características técnicas, configurações, programação, montagem, instalação, manutenção, operação e gerenciamento de todas as funcionalidades fornecidas. Toda documentação dos equipamentos fornecidos será fornecida tanto na forma impressa como também em mídia digital, na forma de arquivos eletrônicos;

2.8.568. Os equipamentos, materiais e produtos a serem fornecidos deverão atender a todas as Normas e Resoluções da Agência Nacional de Telecomunicações - ANATEL de acordo com a Resolução nº 242 ou superior;

2.8.569. Todas as versões de sistema operacional ou software armazenado no equipamento deverão ser fornecidos nos releases mais atualizados, adequadas às necessidades requeridas nesta especificação, fornecidas se disponíveis na mídia CD-ROM. Durante a vigência da garantia / suporte técnico será prevista a atualização do Sistema Operacional do equipamento dentro da mesma versão por outra mais atualizada visando manter o equipamento atualizado e livre de bugs, falhas de segurança etc;

2.8.570. Deverão ser fornecidos todos os softwares, cabos de força e lógicos, conectores, adaptadores, acessórios de fixação, necessários para o pleno funcionamento do equipamento;

2.8.571. Os equipamentos fornecidos deverão ser novos, estar em produção (não serão aceitos equipamentos já descontinuados pelo fabricante) e estar nas condições originais de fabricação, ou seja, sem modificação, retirada ou acréscimo de componentes externos e / ou internos à montagem original do fabricante;

2.8.572. Todos os equipamentos e seus acessórios deverão estar na embalagem original do fabricante. Todos os acessórios básicos que acompanham os equipamentos deverão ser fornecidos;

Desempenho

2.8.573. Deve possuir capacidade de comutação de, no mínimo, 2 Tbps;

2.8.574. Deve possuir capacidade de encaminhamento de, no mínimo, 900 MPPS;

Disponibilidade

2.8.575. Deve possuir interface de Console Serial ou USB;

- 2.8.576. Deve possuir uma porta para gerenciamento out-of-band com conector RJ-45;
- 2.8.577. Deve implementar 803ad Agregação de Links com mínimo de 54 grupos de 8 portas;
- 2.8.578. Deve possuir buffers de, no mínimo, 16MB;

Switching

- 2.8.579. Deve implementar funcionalidade que permita a detecção de links unidirecionais;
- 2.8.580. Deve implementar funcionalidade que permita a detecção de falhas de uplink;
- 2.8.581. Deve implementar, no mínimo, 4.000(quatro mil) VLANs, conforme padrão IEEE 801q;
- 2.8.582. Deve implementar os seguintes padrões IEEE 801D, 801W, 801S, 801P
- 2.8.583. Deve Implementar JUMBO FRAME (mínimo de 9k) em todas as interfaces Gigabit Ethernet
- 2.8.584. Tabela de endereços MAC com capacidade para no mínimo 80.000 endereços MAC;
- 2.8.585. Deve implementar LLDP (IEEE 801ab)
- 2.8.586. Deve implementar o padrão IEEE801AK
- 2.8.587. Deve implementar MRVP
- 2.8.588. Deve implementar PVST+, RPVST+ ou protocolo compatível;
- 2.8.589. Deve implementar MSTP (IEEE 801s) com suporte a 64 instâncias;
- 2.8.590. Suportar tabela para pelo menos 90.000 hosts IPV4 e 45.000 Hosts IPV6

Roteamento

- 2.8.591. Deve possuir tabela de roteamento com no mínimo 13.000 rotas IPv4 e 3.000 rotas IPv6;
- 2.8.592. Deve implementar roteamento estático;
- 2.8.593. Deve Implementar roteamento OSPFv2 e OSPFv3;
- 2.8.594. Deve implementar roteamento OSPFv2 NSSA;
- 2.8.595. Deve implementar roteamento OSPF com suporte a autenticação MD5 ou texto claro;
- 2.8.596. Deve implementar roteamento OSPF com ECMP (Equal Cost Multi Path) de no mínimo, 8 grupos;
- 2.8.597. Deve implementar OSPF com “Graceful Restart”, que permita o encaminhamento de pacotes mesmo que o software de OSPF seja reiniciado;
- 2.8.598. Deve implementar BGP;
- 2.8.599. Deve implementar PRB (Policy Based Routing)
- 2.8.600. Deve implementar VRRP (Virtual Router Redundancy Protocol);
- 2.8.601. Deve implementar DHCP Client e DHCP Relay
- 2.8.602. Deve suportar VRF (Virtual Routing and Forwarding) até 3 VRFs Routing
- 2.8.603. Deve implementar VRF Ipv4 e Ipv6;
- 2.8.604. Deve implementar funcionalidade que especifica o número máximo de entradas no ARP;
- 2.8.605. Deve implementar funcionalidade de proteção contra frames de BPDUs (spanning tree), no caso de recebimento de BPDUs, a porta deve ser colocada no estado de “down”

Multicast

- 2.8.606. Deve implementar PIM-SM;
- 2.8.607. Deve implementar IGMP nas versões v1 e v2 e Snooping
- 2.8.608. Deve implementar MLD Snooping ;

Software Defined Networking

- 2.8.609. Deve possuir tecnologia que permite a separação do plano de dados (encaminhamento de pacotes) e do plano de controle;
- 2.8.610. Deve permitir a automação de tarefas de reconfiguração da rede mediante eventos que impactem o seu comportamento através de scripts internos ou ferramentas externas que neste caso devão ser fornecidas;
- 2.8.611. Deve ser totalmente programável em REST API
- 2.8.612. Deve permitir a automação de tarefas de reconfiguração da rede mediante eventos que impactem o seu comportamento através de scripts internos ou ferramentas externas que neste caso deverão ser fornecidas;
- 2.8.613. Deve possuir interface REST API e scripting via Python;
- 2.8.614. Deve possuir embarcado ferramenta customizável e programável para monitoração e análise de eventos que possa auxiliar na identificação e correção de problemas de redes, aplicações e eventos de segurança da informação. Caso não possua este recurso é possível entregar uma ferramenta similar, podendo ser composto por hardware ou software adicional;

QoS

- 2.8.615. Deve permitir a configuração do volume de broadcast, Multicast e unicast desconhecido aceito por porta, o excesso deve ser descartado;
- 2.8.616. Deve implementar rate-limiting;
- 2.8.617. Deve suportar espelhamento de portas;
- 2.8.618. Deve possuir algoritmos de enfileiramento SP e WRR ou WFQ;
- 2.8.619. Deve suportar no mínimo, 8 (oito) filas de prioridade por porta;

Segurança

- 2.8.620. Deve implementar ACL's Ipv4 e Ipv6;
- 2.8.621. Deve possuir RADIUS e TACACS+ para controle de gerenciamento do switch;
- 2.8.622. Deve suportar RADIUS/TACACS+ servers.

Gerenciamento

- 2.8.623. Deve suportar duas imagens de software na memória flash (IOS, Firmware);
- 2.8.624. Deve possuir capacidade de armazenar múltiplos arquivos de configuração;
- 2.8.625. Deve implementar sFlow (IPv4 e IPv6) ou similar;
- 2.8.626. Deve implementar TFTP, SFTP ou SCP para gerenciamento de software e configuração

- 2.8.627. Deve implementar SNMP v1, v2c e v3;
- 2.8.628. Deve possuir sincronização de horário (clock) do equipamento com servidor de tempo através do protocolo NTP ou SNTP;
- 2.8.629. Deve suportar Self Signed Certificate Management;
- 2.8.630. Deve suportar SSH v2;
- 2.8.631. Deve Suportar AAA (TACACS+ & RADIUS);
- 2.8.632. Deve implementar CLI com gerência por meio de linhas de comando;

SWITCH DE ACESSO 48 PORTAS

Características Gerais

- 2.8.633. Deve possuir 48 (quarenta e oito) portas POE+ 10/100/1000Mbps do tipo RJ45;
- 2.8.634. Deve possuir 4 (quatro) portas 1/10Gbps SFP+;
- 2.8.634.1. Todas as portas óticas deverão conter *transceivers* compatíveis (10G Base-SR) com as especificações das portas para distância mínima de 300 metros;
- 2.8.634.2. O fornecedor deverá entregar 4 *patch cords* óticos padrão OM4 compatíveis, de 3 (três) metros cada;
- 2.8.635. Deve possuir capacidade de encaminhamento de, no mínimo, 110Mpps;
- 2.8.636. Deve possuir capacidade de comutação de, no mínimo, 176Gbps;
- 2.8.637. Deve implementar IEEE 802.3az para as portas 10/100/1000Mbps;
- 2.8.638. Deve possuir uma interface de console USB;
- 2.8.639. Deve suportar empilhamento de no mínimo 8 (oito) switches;
- 2.8.640. Deve suportar agregação de link através de LACP com no mínimo 20 grupos distribuídos através da pilha, com cada grupo permitindo até 8 portas;
- 2.8.641. Deve suportar a agregação de links entre diferentes membros da pilha;
- 2.8.642. Deve possuir no mínimo 15.000 endereços MAC;
- 2.8.643. Deve possuir latência máxima de 4µs, considerando pacotes de 64 bytes;
- 2.8.644. Deve possuir buffers de, no mínimo, 6 MB;
- 2.8.645. Deve implementar funcionalidade que permita a detecção de links unidirecionais;
- 2.8.646. Deve implementar funcionalidade que permita a detecção de falhas de uplink;
- 2.8.647. Deve implementar no mínimo 2000 VLANs simultaneamente;
- 2.8.648. Deve implementar MVRP (Multiple VLAN Registration Protocol);
- 2.8.649. Deve implementar LLDP (IEEE 802.1ab);
- 2.8.650. Deve implementar LLDP-MED;
- 2.8.651. Deve implementar PVST+, RPVST+ ou protocolo compatível;
- 2.8.652. Deve implementar MSTP (IEEE 802.1s);
- 2.8.653. Deve implementar túneis VxLAN (VTEP).

Roteamento

- 2.8.654. Deve possuir tabela de roteamento com no mínimo 2.000 rotas IPv4 e 1.000 rotas IPv6;
- 2.8.655. Deve implementar roteamento estático;
- 2.8.656. Deve implementar RIP v2, com suporte a autenticação MD5 (RIPv2);
- 2.8.657. Deve implementar RIPng;
- 2.8.658. Deve implementar OSPF;
- 2.8.659. Deve implementar OSPFv3;
- 2.8.660. Deve implementar Policy-based Routing;
- 2.8.661. Deve implementar VRRP;
- 2.8.662. Deve implementar VRRPv3;
- 2.8.663. Deve implementar servidor DHCP;
- 2.8.664. Deve implementar DHCP snooping (IPv4 e IPv6);
- 2.8.665. Deve implementar DHCP relay (IPv4 e IPv6);
- 2.8.666. Deve implementar Gateway mDNS, com suporte a Apple Bonjour

Multicast

- 2.8.667. Deve implementar PIM-SM;
- 2.8.668. Deve implementar PIM-DM;
- 2.8.669. Deve implementar MLD snooping;
- 2.8.670. Deve implementar IGMP v3.

Software Defined Networking

- 2.8.671. Deve implementar OpenFlow 1.3 ou superior;
- 2.8.672. Deve implementar a separação lógica do tráfego sem suporte a OpenFlow do tráfego com suporte a OpenFlow através de instâncias. O tráfego OpenFlow não pode influenciar o tráfego não openflow no equipamento;
- 2.8.673. Deve permitir configurar cada instância como modo ativo (pacotes referentes a fluxos que o switch não conhece são enviados para a controladora) ou modo passivo (pacotes que não se referem a um fluxo na tabela do switch não são enviados para a controladora);
- 2.8.674. Deve implementar 16 instâncias de OpenFlow;
- 2.8.675. As instâncias de OpenFlow devem suportar a associação de múltiplas VLANs;
- 2.8.676. Cada instância OpenFlow configurada no equipamento deve suportar, pelo menos, a configuração de 3 controladores SDN;
- 2.8.677. Deve permitir utilizar intervalo de portas TCP/UDP e flags de TCP como parâmetros nas regras de OpenFlow;
- 2.8.678. Deve suportar no mínimo 16.000 regras openflow;
- 2.8.679. Deve possuir interface REST API;

2.8.680. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE;

2.8.681. Deve suportar a criação de VLANs e ACLs no equipamento através de REST.

QoS

2.8.682. Deve implementar controle de broadcast;

2.8.683. Deve implementar rate limiting para pacotes ICMP;

2.8.684. Deve implementar rate limiting para tráfego broadcast e multicast;

2.8.685. Deve implementar rate limiting baseado em tráfego classificado por uma ACL;

2.8.686. Deve suportar espelhamento de portas;

2.8.687. Deve suportar espelhamento de tráfego para um switch remoto.

Segurança

2.8.688. Deve implementar controle de acesso baseado em perfis (Role Based Access Control);

2.8.689. Deve implementar VLANs privadas, de forma que permita o isolamento de tráfego de uma porta de acesso das demais portas de acesso de uma mesma VLAN, permitindo acesso apenas para as portas de Uplink (porta promíscua);

2.8.690. Deve implementar 802.1x;

2.8.691. Deve implementar autenticação baseada em web;

2.8.692. Deve implementar autenticação baseada em endereço MAC;

2.8.693. Deve permitir a utilização simultânea de autenticação 802.1x e MAC em uma mesma porta;

2.8.694. Deve implementar TACACS+. Não serão aceitas soluções similares;

2.8.695. Deverá suportar o download de políticas ou ACLs a partir de um software de Controle de Acesso à Rede (NAC), sem necessidade de pré-configuração das regras no switch, permitindo a centralização das políticas;

2.8.696. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam à rede (device profiling) sem a necessidade de agentes instalados nos dispositivos;

2.8.697. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, Mac OS e Linux.

Gerenciamento

2.8.698. Deve implementar NTP com autenticação MD5;

2.8.699. Deve implementar Time Domain Reflectometry (TDR) para testes de cabos UTP, permitindo identificar falhas e verificar a distância do cabo;

2.8.700. Deve suportar duas imagens de software na flash;

2.8.701. Deve suportar múltiplos arquivos de configuração na flash;

- 2.8.702. Deve permitir o agendamento de tarefas, permitindo executar um comando em um dia e horário específicos;
- 2.8.703. Deve suportar a autoconfiguração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);
- 2.8.704. Deve suportar gerenciamento através de plataforma de nuvem do mesmo fabricante, com funcionalidades de gerenciamento de configuração, alertas e notificações e gerenciamento de firmware, sem necessidade de instalação de nenhum software ou dispositivo on-site;
- 2.8.705. Deve suportar IPSec para comunicação com o sistema de gerenciamento;
- 2.8.706. Deve implementar sFlow (IPv4 e IPv6) ou similar;
- 2.8.707. Deve possuir interface web para configuração;
- 2.8.708. Deve implementar TR-69 (CPE WAN Management Protocol) ou similar;
- 2.8.709. Deve suportar diagnóstico de transceivers ópticos;
- 2.8.710. Deve implementar Syslog sobre TLS ou similar;
- 2.8.711. Deve implementar Secure SFTP (SFTP);
- 2.8.712. Deve implementar SNMP v1/v2/v3;
- 2.8.713. Deve implementar funcionalidade que permita monitorar o SLA (Service Level Agreement) de conexões IP. Deve suportar os seguintes testes: ICMP Echo, UDP-Echo (em porta configurável) e TCP-Connect (em porta configurável) e Jitter UDP para voz;
- 2.8.714. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
- 2.8.715. Deve implementar a configuração automática de Access Point wireless do mesmo fabricante quando conectado ao switch. Devem ser suportados os seguintes parâmetros para a configuração automática: VLAN, CoS, largura de banda máxima;
- 2.8.716. Deve suportar o encaminhamento de tráfego para controladora wireless do mesmo fabricante para inspeção e controle de acesso.

Licenciamento

- 2.8.717. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
- 2.8.718. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.

SWITCH DE ACESSO 48 PORTAS MULTIGIGABIT

Características Gerais

- 2.8.719. Deve possuir, no mínimo, 48 (quarenta e oito) portas POE+ 10/100/1000Mbps do tipo RJ45 (Base-T)
- 2.8.719.1. No mínimo 8 (oito) portas serão padrão Ethernet Base-T com capacidade de fluxo Multigigabit (IEEE 802.3bz) 1/2.5/5GBaseT ports PoE+;
- 2.8.719.2. Caso não seja possível as portas Multigigabit dentre as 48 portas acima, poderá ser entregue slot adicional para este fim.
- 2.8.720. As portas padrão Gigabit Ethernet devem possuir a funcionalidade de transmissão de energia via cabo Ethernet (Power over Ethernet).
- 2.8.721. Possuir no mínimo 2 (duas) portas SFP+.

- 2.8.721.1. Poderão também serem entregues mediante modulo adicional, caso necessário.
- 2.8.721.2. Todas as portas óticas deverão conter *tranceivers* compatíveis (10G Base-SR) com as especificações das portas para distância mínima de 300 metros;
- 2.8.721.3. O fornecedor deverá entregar 2 *patch cords* óticos padrão OM4 compatíveis, de 3 (três) metros cada;
- 2.8.722. Deve possuir capacidade de encaminhamento de, no mínimo, 100Mpps;
- 2.8.723. Deve possuir capacidade de comutação de, no mínimo, 200Gbps;
- 2.8.724. Deve implementar IEEE 802.3az para as portas 10/100/1000Mbps;
- 2.8.725. Deve possuir uma interface de console USB;
- 2.8.726. Deve suportar empilhamento de no mínimo 8 (oito) switches;
- 2.8.727. Deve suportar agregação de link através de LACP com no mínimo 20 grupos distribuídos através da pilha, com cada grupo permitindo até 8 portas;
- 2.8.728. Deve suportar a agregação de links entre diferentes membros da pilha;
- 2.8.729. Deve possuir no mínimo 15.000 endereços MAC;
- 2.8.730. Deve possuir latência máxima de 4µs, considerando pacotes de 64 bytes;
- 2.8.731. Deve possuir buffers de, no mínimo, 6 MB;
- 2.8.732. Deve implementar funcionalidade que permita a detecção de links unidirecionais;
- 2.8.733. Deve implementar funcionalidade que permita a detecção de falhas de uplink;
- 2.8.734. Deve implementar no mínimo 2000 VLANs simultaneamente;
- 2.8.735. Deve implementar MVRP (Multiple VLAN Registration Protocol);
- 2.8.736. Deve implementar LLDP (IEEE 802.1ab);
- 2.8.737. Deve implementar LLDP-MED;
- 2.8.738. Deve implementar PVST+, RPVST+ ou protocolo compatível;
- 2.8.739. Deve implementar MSTP (IEEE 802.1s);
- 2.8.740. Deve implementar túneis VxLAN (VTEP).

Roteamento

- 2.8.741. Deve possuir tabela de roteamento com no mínimo 2.000 rotas IPv4 e 1.000 rotas IPv6;
- 2.8.742. Deve implementar roteamento estático;
- 2.8.743. Deve implementar RIP v2, com suporte a autenticação MD5 (RIPv2);
- 2.8.744. Deve implementar RIPng;
- 2.8.745. Deve implementar OSPF;
- 2.8.746. Deve implementar OSPFv3;
- 2.8.747. Deve implementar Policy-based Routing;
- 2.8.748. Deve implementar VRRP;
- 2.8.749. Deve implementar VRRPv3;
- 2.8.750. Deve implementar servidor DHCP;

- 2.8.751. Deve implementar DHCP snooping (IPv4 e IPv6);
- 2.8.752. Deve implementar DHCP relay (IPv4 e IPv6);
- 2.8.753. Deve implementar Gateway mDNS, com suporte a Apple Bonjour;

Multicast

- 2.8.754. Deve implementar PIM-SM;
- 2.8.755. Deve implementar PIM-DM;
- 2.8.756. Deve implementar MLD snooping;
- 2.8.757. Deve implementar IGMP v3.

Software Defined Networking

- 2.8.758. Deve implementar OpenFlow 1.3 ou superior;
- 2.8.759. Deve implementar a separação lógica do tráfego sem suporte a OpenFlow do tráfego com suporte a OpenFlow através de instâncias. O tráfego OpenFlow não pode influenciar o tráfego não openflow no equipamento;
- 2.8.760. Deve permitir configurar cada instância como modo ativo (pacotes referentes a fluxos que o switch não conhece são enviados para a controladora) ou modo passivo (pacotes que não se referem a um fluxo na tabela do switch não são enviados para a controladora);
- 2.8.761. Deve implementar 16 instâncias de OpenFlow;
- 2.8.762. As instâncias de OpenFlow devem suportar a associação de múltiplas VLANs;
- 2.8.763. Cada instância OpenFlow configurada no equipamento deve suportar, pelo menos, a configuração de 3 controladores SDN;
- 2.8.764. Deve permitir utilizar intervalo de portas TCP/UDP e flags de TCP como parâmetros nas regras de OpenFlow;
- 2.8.765. Deve suportar no mínimo 16.000 regras openflow;
- 2.8.766. Deve possuir interface REST API;
- 2.8.767. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE;
- 2.8.768. Deve suportar a criação de VLANs e ACLs no equipamento através de REST.

QoS

- 2.8.769. Deve implementar controle de broadcast;
- 2.8.770. Deve implementar rate limiting para pacotes ICMP;
- 2.8.771. Deve implementar rate limiting para tráfego broadcast e multicast;
- 2.8.772. Deve implementar rate limiting baseado em tráfego classificado por uma ACL;
- 2.8.773. Deve suportar espelhamento de portas;
- 2.8.774. Deve suportar espelhamento de tráfego para um switch remoto.

Segurança

- 2.8.775. Deve implementar controle de acesso baseado em perfis (Role Based Access Control);
- 2.8.776. Deve implementar VLANs privadas, de forma que permita o isolamento de tráfego de uma porta de acesso das demais portas de acesso de uma mesma VLAN, permitindo acesso apenas para as portas de Uplink (porta promíscua);
- 2.8.777. Deve implementar 802.1x;
- 2.8.778. Deve implementar autenticação baseada em web;
- 2.8.779. Deve implementar autenticação baseada em endereço MAC;
- 2.8.780. Deve permitir a utilização simultânea de autenticação 802.1x e MAC em uma mesma porta;
- 2.8.781. Deve implementar TACACS+. Não serão aceitas soluções similares;
- 2.8.782. Deverá suportar o download de políticas ou ACLs a partir de um software de Controle de Acesso à Rede (NAC), sem necessidade de pré-configuração das regras no switch, permitindo a centralização das políticas;
- 2.8.783. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam à rede (device profiling) sem a necessidade de agentes instalados nos dispositivos;
- 2.8.784. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, Mac OS e Linux.

Gerenciamento

- 2.8.785. Deve implementar NTP com autenticação MD5;
- 2.8.786. Deve implementar Time Domain Reflectometry (TDR) para testes de cabos UTP, permitindo identificar falhas e verificar a distância do cabo;
- 2.8.787. Deve suportar duas imagens de software na flash;
- 2.8.788. Deve suportar múltiplos arquivos de configuração na flash;
- 2.8.789. Deve permitir o agendamento de tarefas, permitindo executar um comando em um dia e horário específicos;
- 2.8.790. Deve suportar a autoconfiguração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);
- 2.8.791. Deve suportar gerenciamento através de plataforma de nuvem do mesmo fabricante, com funcionalidades de gerenciamento de configuração, alertas e notificações e gerenciamento de firmware, sem necessidade de instalação de nenhum software ou dispositivo on-site;
- 2.8.792. Deve suportar IPSec para comunicação com o sistema de gerenciamento;
- 2.8.793. Deve implementar sFlow (IPv4 e IPv6) ou similar;
- 2.8.794. Deve possuir interface web para configuração;
- 2.8.795. Deve implementar TR-69 (CPE WAN Management Protocol) ou similar;
- 2.8.796. Deve suportar diagnóstico de transceivers ópticos;
- 2.8.797. Deve implementar Syslog sobre TLS ou similar;
- 2.8.798. Deve implementar Secure SFTP (SFTP);

- 2.8.799. Deve implementar SNMP v1/v2/v3;
- 2.8.800. Deve implementar funcionalidade que permita monitorar o SLA (Service Level Agreement) de conexões IP. Deve suportar os seguintes testes: ICMP Echo, UDP-Echo (em porta configurável) e TCP-Connect (em porta configurável) e Jitter UDP para voz;
- 2.8.801. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
- 2.8.802. Deve implementar a configuração automática de Access Point wireless do mesmo fabricante quando conectado ao switch. Devem ser suportados os seguintes parâmetros para a configuração automática: VLAN, CoS, largura de banda máxima;
- 2.8.803. Deve suportar o encaminhamento de tráfego para controladora wireless do mesmo fabricante para inspeção e controle de acesso.

Licenciamento

- 2.8.804. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
- 2.8.805. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.

SWITCH DE ACESSO 24 PORTAS

Características Gerais

- 2.8.806. Deve possuir 24 (vinte e quatro) portas POE+ 10/100/1000Mbps do tipo RJ45;
- 2.8.807. Deve possuir 4 (quatro) portas 1/10Gbps SFP+;
- 2.8.807.1. Todas as portas óticas deverão conter *tranceivers* compatíveis (10G Base-SR) com as especificações das portas para distância mínima de 300 metros;
- 2.8.807.2. O fornecedor deverá entregar 4 *patch cords* óticos padrão OM4 compatíveis, sendo 2 unidades de 3 (três) metros e 2 unidades de 5 (cinco) metros;
- 2.8.808. Deve possuir capacidade de encaminhamento de, no mínimo, 40Mpps;
- 2.8.809. Deve possuir capacidade de comutação de, no mínimo, 56Gbps;
- 2.8.810. Deve implementar IEEE 802.3az para as portas 10/100/1000Mbps;
- 2.8.811. Deve possuir uma interface de console USB;
- 2.8.812. Deve suportar empilhamento de no mínimo 8 (oito) switches;
- 2.8.813. Deve suportar agregação de link através de LACP com no mínimo 20 grupos distribuídos através da pilha, com cada grupo permitindo até 8 portas;
- 2.8.814. Deve suportar a agregação de links entre diferentes membros da pilha;
- 2.8.815. Deve possuir no mínimo 15.000 endereços MAC;
- 2.8.816. Deve possuir latência máxima de 4µs, considerando pacotes de 64 bytes;
- 2.8.817. Deve possuir buffers de, no mínimo, 6 MB;
- 2.8.818. Deve implementar funcionalidade que permita a detecção de links unidirecionais;
- 2.8.819. Deve implementar funcionalidade que permita a detecção de falhas de uplink;
- 2.8.820. Deve implementar no mínimo 2000 VLANs simultaneamente;
- 2.8.821. Deve implementar MVRP (Multiple VLAN Registration Protocol);

- 2.8.822. Deve implementar LLDP (IEEE 802.1ab);
- 2.8.823. Deve implementar LLDP-MED;
- 2.8.824. Deve implementar PVST+, RPVST+ ou protocolo compatível;
- 2.8.825. Deve implementar MSTP (IEEE 802.1s);
- 2.8.826. Deve implementar túneis VxLAN (VTEP).

Roteamento

- 2.8.827. Deve possuir tabela de roteamento com no mínimo 2.000 rotas IPv4 e 1.000 rotas IPv6;
- 2.8.828. Deve implementar roteamento estático;
- 2.8.829. Deve implementar RIP v2, com suporte a autenticação MD5 (RIPv2);
- 2.8.830. Deve implementar RIPv6;
- 2.8.831. Deve implementar OSPF;
- 2.8.832. Deve implementar OSPFv3;
- 2.8.833. Deve implementar Policy-based Routing;
- 2.8.834. Deve implementar VRRP;
- 2.8.835. Deve implementar VRRPv3;
- 2.8.836. Deve implementar servidor DHCP;
- 2.8.837. Deve implementar DHCP snooping (IPv4 e IPv6);
- 2.8.838. Deve implementar DHCP relay (IPv4 e IPv6);
- 2.8.839. Deve implementar Gateway mDNS, com suporte a Apple Bonjour

Multicast

- 2.8.840. Deve implementar PIM-SM;
- 2.8.841. Deve implementar PIM-DM;
- 2.8.842. Deve implementar MLD snooping;
- 2.8.843. Deve implementar IGMP v3.

Software Defined Networking

- 2.8.844. Deve implementar OpenFlow 1.3 ou superior;
- 2.8.845. Deve implementar a separação lógica do tráfego sem suporte a OpenFlow do tráfego com suporte a OpenFlow através de instâncias. O tráfego OpenFlow não pode influenciar o tráfego não openflow no equipamento;
- 2.8.846. Deve permitir configurar cada instância como modo ativo (pacotes referentes a fluxos que o switch não conhece são enviados para a controladora) ou modo passivo (pacotes que não se referem a um fluxo na tabela do switch não são enviados para a controladora);
- 2.8.847. Deve implementar 16 instâncias de OpenFlow;
- 2.8.848. As instâncias de OpenFlow devem suportar a associação de múltiplas VLANs;

- 2.8.849. Cada instância OpenFlow configurada no equipamento deve suportar, pelo menos, a configuração de 3 controladores SDN;
- 2.8.850. Deve permitir utilizar intervalo de portas TCP/UDP e flags de TCP como parâmetros nas regras de OpenFlow;
- 2.8.851. Deve suportar no mínimo 16.000 regras openflow;
- 2.8.852. Deve possuir interface REST API;
- 2.8.853. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE;
- 2.8.854. Deve suportar a criação de VLANs e ACLs no equipamento através de REST.

QoS

- 2.8.855. Deve implementar controle de broadcast;
- 2.8.856. Deve implementar rate limiting para pacotes ICMP;
- 2.8.857. Deve implementar rate limiting para tráfego broadcast e multicast;
- 2.8.858. Deve implementar rate limiting baseado em tráfego classificado por uma ACL;
- 2.8.859. Deve suportar espelhamento de portas;
- 2.8.860. Deve suportar espelhamento de tráfego para um switch remoto.

Segurança

- 2.8.861. Deve implementar controle de acesso baseado em perfis (Role Based Access Control);
- 2.8.862. Deve implementar VLANs privadas, de forma que permita o isolamento de tráfego de uma porta de acesso das demais portas de acesso de uma mesma VLAN, permitindo acesso apenas para as portas de Uplink (porta promíscua);
- 2.8.863. Deve implementar 802.1x;
- 2.8.864. Deve implementar autenticação baseada em web;
- 2.8.865. Deve implementar autenticação baseada em endereço MAC;
- 2.8.866. Deve permitir a utilização simultânea de autenticação 802.1x e MAC em uma mesma porta;
- 2.8.867. Deve implementar TACACS+. Não serão aceitas soluções similares;
- 2.8.868. Deverá suportar o download de políticas ou ACLs a partir de um software de Controle de Acesso à Rede (NAC), sem necessidade de pré-configuração das regras no switch, permitindo a centralização das políticas;
- 2.8.869. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam à rede (device profiling) sem a necessidade de agentes instalados nos dispositivos;
- 2.8.870. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, Mac OS e Linux.

Gerenciamento

- 2.8.871. Deve implementar NTP com autenticação MD5;
- 2.8.872. Deve implementar Time Domain Reflectometry (TDR) para testes de cabos UTP, permitindo identificar falhas e verificar a distância do cabo;
- 2.8.873. Deve suportar duas imagens de software na flash;
- 2.8.874. Deve suportar múltiplos arquivos de configuração na flash;
- 2.8.875. Deve permitir o agendamento de tarefas, permitindo executar um comando em um dia e horário específicos;
- 2.8.876. Deve suportar a autoconfiguração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);
- 2.8.877. Deve suportar gerenciamento através de plataforma de nuvem do mesmo fabricante, com funcionalidades de gerenciamento de configuração, alertas e notificações e gerenciamento de firmware, sem necessidade de instalação de nenhum software ou dispositivo on-site;
- 2.8.878. Deve suportar IPSec para comunicação com o sistema de gerenciamento;
- 2.8.879. Deve implementar sFlow (IPv4 e IPv6) ou similar;
- 2.8.880. Deve possuir interface web para configuração;
- 2.8.881. Deve implementar TR-69 (CPE WAN Management Protocol) ou similar;
- 2.8.882. Deve suportar diagnóstico de transceivers ópticos;
- 2.8.883. Deve implementar Syslog sobre TLS ou similar;
- 2.8.884. Deve implementar Secure SFTP (SFTP);
- 2.8.885. Deve implementar SNMP v1/v2/v3;
- 2.8.886. Deve implementar funcionalidade que permita monitorar o SLA (Service Level Agreement) de conexões IP. Deve suportar os seguintes testes: ICMP Echo, UDP-Echo (em porta configurável) e TCP-Connect (em porta configurável) e Jitter UDP para voz;
- 2.8.887. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
- 2.8.888. Deve implementar a configuração automática de Access Point wireless do mesmo fabricante quando conectado ao switch. Devem ser suportados os seguintes parâmetros para a configuração automática: VLAN, CoS, largura de banda máxima;
- 2.8.889. Deve suportar o encaminhamento de tráfego para controladora wireless do mesmo fabricante para inspeção e controle de acesso.

Licenciamento

- 2.8.890. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
- 2.8.891. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.

Garantia e atualização de versão do fabricante da solução de redes (Comum aos equipamentos e sistemas do Grupo 2)

- 2.8.892. O serviço de garantia será do Fabricante, pelo período de 60 (sessenta) meses contados a partir do recebimento definitivo dos itens de gerenciamento da rede (com e sem fios), dos *switches* e dos *access points*, na modalidade 24x7, sem prejuízo de qualquer política de garantia adicional oferecido pelo fabricante;

- 2.8.893. Deverá fornecer direito de atualização contínua dos produtos licenciados - novas versões e *patches* de atualização.
- 2.8.894. O atendimento será em horário integral, telefônico e eletrônico, na modalidade 24x7x365;
- 2.8.895. Deverá ser disponibilizada pelo fabricante uma central de atendimento, 24 horas por dia, 7 dias por semana, todos os dias do ano;
- 2.8.896. A abertura de chamados na central de atendimento poderá ser feita através de telefone 0800, e-mail e portal web;
- 2.8.897. Deverá ser disponibilizado acesso a base de conhecimento do site do fabricante e fóruns de discussão.
- 2.8.898. Em caso de equipamento defeituoso, o envio de equipamento(s), componente(s), acessório(s) e dispositivo(s) novo(s), de primeiro uso e de modelo igual ou superior ao(s) danificado(s), desde que compatível com os equipamentos adquiridos, às expensas do fabricante, às dependências da CONTRATANTE;
- 2.8.899. O contrato de reposição de peças deverá ser na modalidade 8x5xNBD, com acionamento em horário comercial e devendo o equipamento substituto ser entregue na CONTRATADA até o próximo dia útil (Next Business Day - NBD) após a abertura do chamado;
- 2.8.900. Para determinação do horário de início de cada chamado referente a substituição de equipamento defeituoso devem ser levadas em consideração as seguintes condições:
- 2.8.900.1. caso a determinação de falha do hardware pela fabricante tenha ocorrido antes das 15h, horário local da Brasília-DF, de segunda a sexta-feira (excluindo os feriados), o equipamento deverá ser enviado no mesmo dia para chegar no próximo dia útil.
- 2.8.900.2. Para as solicitações feitas depois das 15h, o fabricante deverá entregar o equipamento substituto até o segundo dia útil após o a determinação da falha;
- 2.8.901. O equipamento substituto passará à propriedade da CONTRATANTE, devendo o mesmo ser imediatamente incluído no contrato de manutenção vigente em substituição ao equipamento danificado;
- 2.8.902. O equipamento substituído deverá ser devolvido ao fabricante às expensas do mesmo, em até 5 (cinco) dias úteis.
- 2.8.903. A CONTRATANTE deverá ter acesso direto ao centro de assistência técnica da fabricante dos equipamentos para abertura dos chamados, bem como para acompanhar e gerenciar os casos quando necessário. Esse acesso deverá ser provido 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de login/senha individual;
- 2.8.904. A CONTRATANTE deverá ter a opção de abrir os chamados junto a fabricante com o intermédio da CONTRATADA;
- 2.8.905. Não será aceita garantia para reposição de equipamentos da empresa revendedora;
- 2.8.906. Caso haja deslocamento do equipamento para outro *rack*, sala ou prédio da contratante, a contratada deverá realizar a movimentação e reinstalação dos equipamentos para o novo ambiente, a critério da contratante.

Implantação dos switches

- 2.8.907. Os *switches* serão implantados nas dependências da contratante, configurados com os padrões utilizados pelo ITI em sua rede atual, contendo (e não se limitando a):
- 2.8.907.1. Segmentação de redes;
- 2.8.907.2. Agregação de links;

- 2.8.907.3. Controle de acesso (a ser conectado ao padrão 802.1x do módulo de controle de acesso);
- 2.8.907.4. Alta disponibilidade de equipamentos;
- 2.8.907.5. QoS;
- 2.8.907.6. Roteamentos;
- 2.8.907.7. Defesas em níveis de enlace e rede;
- 2.8.907.8. Netflow/sFlow (ou similar);
- 2.8.907.9. SNMP;
- 2.8.907.10. NTP;
- 2.8.907.11. Syslog;
- 2.8.907.12. Conexões de gerenciamento dos ativos;
- 2.8.907.13. ACLs.

Treinamento para os switches

- 2.8.908. Oferecer treinamento para operacionalização dos *switches* (planejamento, instalação, configuração, operação, suporte e *troubleshooting*) com conteúdo teórico e atividades práticas, utilizando interfaces gráficas e linhas de comando (comand-line interface - CLI). A duração mínima de será de 40 (quarenta) horas e atenderá a 10 pessoas.
- 2.8.909. Os treinamentos deverão ser realizados em local situado na cidade de Brasília, nas dependências da CONTRATADA.
- 2.8.910. A CONTRATADA deverá fornecer o treinamento no período de vigência do contrato, no máximo até 30 (trinta) dias após pedido da CONTRATANTE.
- 2.8.911. A Contratada deverá fornecer material de treinamento e deverá ser ministrado por profissional certificado pelo fabricante do equipamento.

TREINAMENTO OFICIAL DO FABRICANTE DA SOLUÇÃO DE SWITCHES

- 2.8.912. O treinamento oficial do fabricante será de, no mínimo, 40 horas, em português.
- 2.8.913. O treinamento será realizado preferencialmente no modelo presencial, em instalações providas pela CONTRATADA.
 - 2.8.913.1. Os treinamentos só serão aceitos na modalidade à distância se:
 - 1. Por impossibilidade logística devido à pandemia de COVID-19;
 - 2. Por interesse e oportunidade da Administração.
- 2.8.914. Deve ser ministrado por profissional certificado pelo fabricante dos equipamentos como instrutor.
- 2.8.915. A ementa do curso deve abranger conteúdos que vão desde instalação, configuração, gerenciamento, operação a *troubleshooting* dos equipamentos de hardware e de softwares que compõem a solução de redes sem fios.
- 2.8.916. Os treinamentos deverão ser realizados no Brasil, em português, na modalidade presencial, em local fornecido pela CONTRATADA.
- 2.8.917. O local de treinamento deverá possuir todas as facilidades para um perfeito desempenho das atividades, incluindo os recursos áudio visuais e laboratórios necessários, sem ônus à contratante.

- 2.8.918. A empresa disponibilizará material em formato digital (PDF) aos participantes e quaisquer conteúdos e ferramentas adicionais que venham a ser necessárias para o treinamento.
- 2.8.919. Os cursos referentes a equipamentos e softwares que façam parte do objeto deverão usar o material oficial de treinamento do respectivo fabricante por meio de qualquer um dos seus respectivos centros autorizados de treinamento.
- 2.8.920. Caso não haja disponibilidade para realização em Brasília, a empresa custeará os gastos de passagens e estadia para o centro de treinamento mais próximo de Brasília.
- 2.8.921. Deverá ser fornecido certificado de conclusão oficial do fabricante da solução aos participantes.

SWITCHES FIBRE CHANNEL

Características físicas

- 2.8.922. Possuir altura máxima de 1 RU (Rack Units);
- 2.8.923. Suportar, no mínimo, 24 (vinte e quatro) portas de 8/16 Gigabit Fibre Channel, padrão SFP+ com conectores LC;
- 2.8.923.1. Todas as portas do equipamento entregue devem ser licenciadas para uso e acompanharem com os respectivos *transceivers*;
- 2.8.924. Deve possuir no mínimo 4 portas 10 GbE padrão SFP+ para uplink;
- 2.8.924.1. Serão aceitos equipamentos com padrões de velocidades maiores (ex.: QSFP+), desde que metade do quantitativo das portas acompanhe os respectivos cabos do tipo *breakout* para compatibilização com o padrão SFP+, e a outra metade acompanhe cabos DAC de 3 metros compatíveis com a porta de *uplink* do equipamento entregue;
- 2.8.925. Possuir fontes redundantes em configuração *grid* N+N, *hot-swappable*, operando entre 100-240V AC nominal ($\pm 10\%$ variação no intervalo) e 60Hz nominal, com cabeamento incluso;
- 2.8.926. Possuir ventiladores *hot-swappable* com gerenciamento integrado de temperatura e potência;
- 2.8.927. Possuir porta gerenciamento “out-of-band” 10/100/1000, permitindo um gerenciamento remoto;
- 2.8.928. Deverão ser fornecidos manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração.
- 2.8.929. O switch deverá estar em conformidade com a norma IEC 60950 (*Safety of Information Technology Equipment Including Electrical Business Equipment*), para segurança do usuário contra incidentes elétricos e combustão dos materiais elétricos.
- 2.8.930. O switch e seus acessórios deverão estar acondicionados em embalagens com caixa e calços de proteção especialmente desenvolvidos para suportar o empilhamento e as vibrações.
- 2.8.931. Garantia do equipamento e sistema operacional de 60 meses.

Características operacionais

- 2.8.932. Possuir capacidade de atualização não-disruptiva de software, *In-Service Software Upgrade* (ISSU);
- 2.8.933. Possuir capacidade de armazenamento de mais de uma versão de software no switch;
- 2.8.934. Possuir comutação e restabelecimento de processos de forma a manter o status e consistência das conexões (*stateful process restart/failover*);

- 2.8.935. Possuir capacidade de interligação entre chassis equivalentes através de canais de alta disponibilidade e desempenho;
- 2.8.936. Permitir a criação de ambientes independentes e isolados logicamente, dentro do switch.
- 2.8.936.1. Cada ambiente de SAN Virtualizado deve possuir as funcionalidades de zoneamento e os serviços nativos ao *Fabric* totalmente isolados, sendo independentes como uma SAN tradicional;
- 2.8.937. Suportar a criação de no mínimo 32 (trinta e dois) SANs Virtuais;
- 2.8.938. Possuir capacidade de configuração de *zones* em SAN Virtual, pelos seguintes critérios: N_Port World Wide Name (nWWN), N_Port FC-ID;
- 2.8.939. Possuir capacidade de configurar privilégios de leitura e escrita em um *zone* (*read-only zoning*);
- 2.8.940. Suportar modo NPIV ou Access Gateway;
- 2.8.941. Suportar os tipos de porta Fibre Channel básicos: E, F, FL;
- 2.8.942. Suportar os tipos de porta Fibre Channel avançados: TE, SD, ST;
- 2.8.943. Possuir a funcionalidade de espelhamento de tráfego em uma porta local (SPAN) ou em switch remoto (RSPAN), podendo ser configurada em qualquer porta FC, de qualquer módulo, permitindo que o tráfego de uma interface possa ser enviado para um analisador de protocolo externo;
- 2.8.944. Ter a capacidade de verificar o caminho de encaminhamento de um pacote na rede SAN (*FC trace route*);
- 2.8.945. Ter a capacidade de verificar o tempo de resposta de um dispositivo na rede SAN (*FC Ping*);
- 2.8.946. Suportar ao envio de informações ao um servidor externo, Syslog;
- 2.8.947. Possuir estatísticas por interface de utilização e erros;
- 2.8.948. Possuir roteamento de tráfego entre SANs Virtuais diferentes;

Desempenho e escalabilidade

- 2.8.949. O Chassi deve suportar tráfego máximo sustentado em todas as 24 portas à 16 Gbps Fibre Channel ou sem *oversubscription* nas portas;
- 2.8.950. Permitir a criação de até 24 *port-channels* por chassi;
- 2.8.951. Permitir a criação de até 24 Inter-Switch Link (ISL) por chassi;

Gerenciamento

- 2.8.952. Possuir ferramenta gráfica baseada em HTML5 para gerenciamento, provisionamento, configuração, monitoração, análise de eventos, verificação de conectividade, visualização de dispositivos e mapeamento dinâmico da topologia da SAN;
- 2.8.953. Permitir a visualização de representações gráficas dos equipamentos on-line, mostrando o estado operacional das portas, permitindo inclusive a configuração e monitoramento em tempo real.
- 2.8.954. A ferramenta deve exibir a topologia da rede. A descoberta dos equipamentos e suas interligações deve ser feita obrigatoriamente de forma automática, permitindo também sua customização manual.
- 2.8.955. Permitir a configuração de diferentes perfis de usuários do sistema, criando regras como administrador, operador e apenas leitura.
- 2.8.956. O software de gerência deve prover detecção de falhas em tempo real, além de oferecer relatórios e regras de tratamento de alarmes pré-configuradas para ações de intervenção.

- 2.8.957. Suportar a implementação de alta disponibilidade através de sistema ativo-standby com banco de dados compartilhado;
- 2.8.958. Deve possuir integrações nativas com outras ferramentas de gerência com o VMware vCenter 6.x;
- 2.8.959. Deve permitir a criação de *Dashboards* customizados para visualização imediata das principais informações do Fabric SAN;

Segurança

- 2.8.960. Possuir autenticação, autorização e registro das operações dos administradores;
- 2.8.961. Suportar RADIUS e TACACS+;
- 2.8.962. Implementar controle de acesso baseado em regras configuráveis ("Role-Based Access Control" – RBAC);
- 2.8.963. Possuir gerenciamento via SNMPv3 com criptografia baseada no algoritmo AES;
- 2.8.964. Suportar SSHv2 (Secure Shell Protocol version 2);
- 2.8.965. Suportar SFTP (Security FTP) para proteção na transferência de arquivos;
- 2.8.966. Implementar listas de controle de Acesso (ACLs);
- 2.8.967. Possuir isolamento total entre os múltiplos *Fabrics* através de SANs Virtuais;
- 2.8.968. Possuir zoneamento baseado em hardware (Hardware-enforced zoning);
- 2.8.969. Possuir zonas independentes por SAN Virtual;
- 2.8.970. Possuir capacidade de fazer a associação fixa entre um determinado dispositivo identificável via World Wide Name e uma porta do Director (*Port Security*);
- 2.8.971. Possuir capacidade de garantir comunicação segura entre switches SAN, somente habilitando equipamentos previamente autorizada via configuração (*Fabric Binding*);

Treinamento para os switches fibre channel

- 2.8.972. Oferecer treinamento para operacionalização dos switches fibre channel (planejamento, instalação, configuração, operação, suporte e *troubleshooting*) com conteúdo teórico e atividades práticas, utilizando interfaces gráficas e linhas de comando (comand-line interface - CLI). A duração mínima de será de 40 (quarenta) horas e atenderá a 10 pessoas.
- 2.8.973. Os treinamentos deverão ser realizados em local situado na cidade de Brasília, nas dependências da CONTRATADA.
- 2.8.974. A CONTRATADA deverá fornecer o treinamento no período de vigência do contrato, no máximo até 30 (trinta) dias após pedido da CONTRATANTE.
- 2.8.975. A Contratada deverá fornecer material de treinamento e deverá ser ministrado por profissional certificado pelo fabricante do equipamento.

3. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

Grupo	ID	Bens/Serviços	CATMAT/CATSER	Medida	Estimativa
-------	----	---------------	---------------	--------	------------

1	1	Firewall perfil 1 com garantia do fabricante por 60 meses	150100	Unidade	6
	2	Firewall perfil 2 com garantia do fabricante por 60 meses	150100	Unidade	2
	3	Serviço de configuração da solução de <i>firewall</i> (por site)	26972	Unidade	2
	4	Treinamento oficial do fabricante da solução de <i>firewall</i>	03840	Pessoa	8
2	5	Sistema de gerenciamento e controle de acesso de redes sem fios e cabeada	150345	Unidade	1
	6	Sistema de controle de acesso a redes cabeadas	150345	Unidade	1
	7	Access Point	439759	Unidade	20
	8	Serviço de configuração do sistema de gerenciamento e controle de acesso de redes sem fios e cabeada	26972	Unidade	1
	9	Serviço de configuração do sistema de controle de acesso de redes cabeadas	26972	Unidade	1
	10	Treinamento oficial do fabricante da solução de controle de acesso	03840	Pessoa	8
	11	Switch core	393273	Par/Cluster	1
	12	Switch topo de rack 48 portas	393274	Unidade	10
	13	Switch de acesso 48 portas	266838	Unidade	18
	14	Switch de acesso 48 portas multigigabit	266838	Unidade	6
	15	Switch de acesso 24 portas	266838	Unidade	14
	16	Treinamento oficial do fabricante da solução de switches	03840	Pessoa	8
3	17	Switch fibre channel	393274	Unidade	16

- 3.1. A estimativa dos equipamentos e serviços é a seguinte:
- 3.2. Haverão 4 *clusters* de 2 firewalls para os ambientes do ITI, em 4 ambientes de *datacenter*, sendo 3 em Brasília e 1 em Florianópolis;
- 3.3. Serão 2 ambientes de gerência, um contendo 4 firewalls do perfil 1, e outro contendo 2 do perfil 1 e 2 do perfil 2;
- 3.3.1. Por conta das políticas distintas dos ambientes, serão consideradas 2 instalações;
- 3.4. Os equipamentos de firewall serão implantados utilizando a metodologia *Zero Touch*, que dispensará custos extras de configuração, uma vez já feita na ferramenta de gerência e controle de políticas dos equipamentos;
- 3.5. Os treinamentos serão realizados para até 8 servidores das áreas técnicas do ITI responsáveis pela operacionalização dos equipamentos que compõem a solução;
- 3.6. O ambiente de redes sem fios será implantada de modo que todo seja disponibilizado o serviço para todo o prédio sede da instituição, com qualidade de sinal ótimo;
- 3.7. A quantidade de *access points* adquiridos dependerá do modelo vencedor e disposição dos equipamentos no *site survey* realizado pela contratada após a contratação;
- 3.7.1. Esta medida visa manter o objetivo da contratação, resguardando os profissionais envolvidos de eventual risco de contaminação devido à pandemia de COVID-19;
- 3.8. A ferramenta de gerência será configurada de modo que propague para os access points as políticas do ITI em sua instalação;
- 3.9. Os access points serão instalados, inclusive quanto à fixação, e receberão as configurações pela ferramenta de gerência;

- 3.10. O treinamento será realizado para até 5 servidores das áreas técnicas do ITI responsáveis pela operacionalização dos equipamentos que compõem a solução;
- 3.11. Os sistemas de controle de acesso serão utilizados para gerenciamento de ativos cabeados e sem fios, a fim de garantir a gestão integrada da infraestrutura da COTIC em Brasília-DF;
- 3.11.1. O sistema de controle de acesso de redes cabeadas será utilizado para gerenciamento de ativos e controle de acessos para os ambientes da DINFRA em Brasília-DF e Florianópolis-SC;
- 3.12. Os *switches* LAN e SAN atenderão aos ambientes da COTIC e DINFRA;

4. ANÁLISE DE SOLUÇÕES

IDENTIFICAÇÃO DAS SOLUÇÕES	
Id	Descrição da solução (ou cenário)
1	Plataforma de firewall <i>software</i> em código aberto
2	Aquisição de soluções de perímetro de rede
3	Manutenção da infraestrutura atual
4	Aquisição de equipamentos unitários
5	Aquisição de solução integrada de redes

4.1. Plataforma de firewall *software* em código aberto

4.1.1. O ambiente atual do ITI pode ser mantido em caso de extrema restrição orçamentária. Entretanto, há uma latente limitação de funcionalidades, como: distribuição de assinaturas por listas pagas, necessidade de utilização de servidores de rede, interfaces de rede especializadas para tratamento e encaminhamento de pacotes e tratamento precário dos dados para geração de relatórios.

4.1.2. Essas limitações expõem o ITI a ataques diversos que qualquer infraestrutura de rede básica deveria conter, como controle de acesso aos perímetros de rede, monitoramento de tráfego, sistema de proteção de intrusões (*Intrusion Prevention System - IPS*), filtros de conteúdo, controle de aplicação, balanceamento de link e bloqueio de atividades maliciosas a partir de correio eletrônico (*antispam*).

4.1.3. No que tange à rede sem fios do ITI, a estrutura é igualmente precária, composta de equipamentos antiquíssimos, sem suporte e garantia. A estrutura toda já foi descontinuada pelo fabricante. As equipes técnicas atuais do ITI não são contemporâneas à implantação da solução atual, não há documentação suficiente para manter a solução e há limitações temporais da ferramenta, por conta de novas tecnologias agora existentes para redes *wifi* corporativas atuais.

4.2. Aquisição de soluções de perímetro de rede

4.2.1. Existem diversas soluções de *firewall* e redes *wifi* corporativas, e ambas têm diversos fabricantes que podem atender ao ITI.

4.2.2. Dentre as possibilidades de *firewall*, há ferramentas baseadas em *software*, que utilizam recursos próprios da organização cliente, e em *hardware*. Ambos carregam riscos inerentes, sendo necessário balancear a solução mais adequada para o perfil de risco do ITI, mantendo sempre a economicidade, eficiência, eficácia e efetividade do processo licitatório.

4.2.3. Soluções de gerenciamento unificado de ameaças (*Unified Threat Management - UTM*) são *firewalls* com gerenciamento centralizado e apresenta funcionalidades de diversas soluções de segurança,

como: *firewall* de camada de transporte, filtro de conteúdo, antimalware de rede, controle de aplicações, antispam, IPS, balanceamento de *link* e de carga.

4.2.4. Dada a limitação orçamentária e de recursos humanos no ITI, é razoável a aquisição de uma solução centralizada, de forma que atenda às necessidades urgentes da Autarquia, possibilitando amadurecer o ambiente para uma eventual aquisição futura para solução especializada de segurança.

4.2.5. As soluções de rede *wifi* também apresentam suas peculiaridades, como adoção do padrão de transmissão do Wifi-6 (802.11ax), utilização de métodos de proteção especializados, estratégias de gerenciamento e funcionalidades de geração de relatórios. Há a necessidade de atualização desse serviço para a instituição e os principais fabricantes ofertam o mínimo de requisitos que atendem à realidade do ITI.

4.2.6. A Autarquia tem falhas nos equipamentos e há a necessidade de maior controle e monitoramento para o ambiente de redes sem fio, em especial pelo uso cada vez maior de dispositivos móveis e pessoais nos ambientes corporativos.

4.2.7. Com ambas as tecnologias de perímetro, há a necessidade de treinamento nas soluções ofertadas, a fim de dar expertise dos produtos para as equipes técnicas envolvidas no ITI.

4.3. **Manutenção da infraestrutura atual**

4.3.1. Os equipamentos funcionam, porém sem qualquer integração. Há limitação para implementação de padrões unificados de segurança, como a segregação de equipamentos corporativos com identificação por certificação digital.

4.3.2. O ambiente de rede sem fios tem dimensionamento insuficiente para qualidade dos sinais de rádio, e não há suporte para padrões de transmissão utilizados na atualidade, como o 802.11n, ac e ax. Inexiste a possibilidade de uso do padrão WPA3 para confidencialidade da rede, e não há qualquer meio viável de implementar políticas de conformidade para o acesso à rede.

4.3.3. As redes de armazenamento (*Fibre Channel/SAN*) estão saturadas pela quantidade de interfaces físicas, da capacidade do canal que é limitada a 8Gb, e as equipes de sustentação contam com a sorte para que os equipamentos não parem de funcionar.

4.3.4. A interface de acesso aos ativos de rede SAN estão instáveis, e o acesso é feito mediante improviso, com uma máquina virtual com sistema operacional e máquina virtual Java desatualizados, criada especificamente para os administradores do ambiente conseguirem acessar o ambiente.

4.3.5. Não existe uma arquitetura de rede definida a partir das boas práticas. A hierarquia de *switches* é feita a partir de um amontoado de equipamentos em descontinuidade, de 3 fabricantes diferentes, e a equipe de sustentação utilizou de camadas de abstração superiores, mediante virtualização, para prover um roteamento mínimo para a rede.

4.3.6. Todos os *switches* do parque são de acesso, independente da posição na rede, sendo uma fragilidade enorme para o ITI. Este modelo de equipamento não foi dimensionado para o roteamento e outras funcionalidades de gerência de redes realizada por um roteador, *switch* central (*core* em uma arquitetura de três camadas) ou *switch spine* (em uma rede *spine-leaf*, de duas camadas).

4.3.7. Há total precariedade nos equipamentos de conexão de rede, e o ITI pode ficar totalmente sem rede a qualquer instante.

4.4. **Aquisição de equipamentos unitários**

4.4.1. Há a possibilidade de aquisição de equipamentos separadamente, conforme o planejamento inicial de instrução dos processos 00100.001257/2020-11 e 00100.000273/2020-88. Entretanto, foi observado que haveria o risco de o ITI precisar adquirir duas vezes a ferramenta de NAC para administrar as redes sem fios e cabeada, caso fabricantes diferentes dos processos viessem a lograr êxito nos certames.

4.4.2. Além disso, os equipamentos poderiam ter funcionalidades incompatíveis, impossibilitando o trânsito de ativos entre as redes por conta das eventuais soluções distintas de NAC.

4.4.3. Caso fossem segregados em itens unitários como um todo haveria risco ainda maior de incompatibilidade, como *firewalls* sem funcionamento unificado, *switches* com incompatibilidades tecnológicas - como é visto hoje na Autarquia - e redes sem fios com falhas de implementação pela implementação inadequada.

4.5. **Aquisição de solução integrada de redes**

4.5.1. A partir do consenso sobre a unificação dos processos (SEI 0437939 e 0437938), foram definidos 3 grupos de soluções interdependentes para a estruturação da rede de computadores do ITI: *firewalls*, *switches* (e *wifi*), e *switches Fibre Channel*.

4.5.2. A aquisição com esses três grupos viabilizará a mudança de protocolos de comunicação, velocidades de transmissão e padrões de portas de conexão. As demandas do ITI por soluções com alocação dinâmica e entregas rápidas de recurso demandam cada vez mais de soluções com gerenciamento centralizado, a fim de entregar recursos computacionais em prazos escassos.

4.5.3. Em 2019 foram testadas iniciativas para a até então futura e improvável implementação de teletrabalho, algo que se concretizou a partir da pandemia de SARS-Cov-2, o novo coronavírus. O provisionamento de um simples acesso remoto hoje custa em torno de 4 horas e um recurso humano da equipe de sustentação de infraestrutura da COTIC.

4.5.4. Caso houvessem ferramentas minimamente adequadas para essa funcionalidade, a demanda poderia ser resolvida em poucos cliques e/ou comandos, sendo entregue em poucos minutos.

4.5.5. Se tratando do gerenciamento de redes em geral, a rede sem fios possibilitará o uso de dispositivos próprios pelos servidores, caso queiram, com enquadramento automatizado de acessos a partir de boas práticas de segurança da informação.

4.5.6. Os equipamentos de *datacenter* especificados nesse processo foram dimensionados para provisionar adequadamente o ambiente virtualizado recém adquirido por esse Instituto - processos 00100.007211/2019-63, 00100.006601/2019-16 e 00100.003109/2019-99 - e receber necessidades ainda pendentes, como implementação de nova infraestrutura de telefonia, serviço de videoconferência e unificação dos parques *on premise* para montagem de um ambiente híbrido com provedor de computação em nuvem.

4.5.7. Cada um dos grupos que compõem a aquisição desse processo depende da outra, o que foi identificado como risco caso fossem instruídos separadamente. Como há mudança dos padrões de portas de comunicação e seus respectivos protocolos, a aquisição apartada resultaria no efeito "elefante branco" até que todas pudessem ser adquiridas.

4.5.8. A quantidade de equipamentos dos fabricantes possíveis inviabiliza o dimensionamento quantitativo dos itens, assim como outras variações, como a duração e eficácia da MP 983, que pode alterar a demanda dos equipamentos.

4.5.9. Não é possível também apartar os itens de sistemas de controle de acesso, visto que o ITI não tem os equipamentos a serem controlados. Seria inviável adquirir a ferramenta sem informar aos eventuais licitantes quais equipamentos de rede seriam gerenciados. Caso fosse contratado em separado, haveria o risco de não haver o uso correto e necessário das funcionalidades do NAC para controle e gerenciamento dos *switches* e *access points*, acarretando assim em aquisição de bens já inúteis a seu propósito.

4.5.10. Diante desse risco, foi considerado colocar as ferramentas no mesmo grupo, mitigando a possibilidade de incompatibilidade entre ferramentas, uma vez que é pressuposto que um fabricante faça com que tal compatibilidade aconteça.

4.5.11. Sendo assim, foi identificado que, pela precariedade do ambiente, não haveria a possibilidade de fazer a atualização por etapas. O ITI sequer tem requisitos mínimos para tal estratégia.

5. ANÁLISE COMPARATIVA DE SOLUÇÕES

5.1. Após análise das necessidades institucionais e a busca de uma solução que supra as necessidades de TIC levantadas, constatou-se projetos de sucesso com as soluções de *firewall* das fabricantes: Cisco, Palo Alto, Watchguard, Checkpoint, Forcepoint e Fortinet, bem como de redes sem fios: Aruba, Cisco, Fortinet, Watchguard em outros órgãos e entidades da Administração Pública.

5.2. Essas empresas são líderes do mercado, conforme abaixo:



Líderes de vendas no mercado de *firewall* (Gartner Magic Quadrant 2019)

Figure 1. Magic Quadrant for the Wired and Wireless LAN Access Infrastructure



Líderes de vendas no mercado de wifi (Gartner Magic Quadrant 2019)

5.3. Tomando como referência de que são os líderes de cada mercado, sem excluir eventuais fabricantes não incluídos nos quadrantes do Gartner que venham a atender plenamente as especificações contidas nesse estudo técnico, espera-se que haja produtos que atendam à demanda do ITI.

5.4. Especificamente sobre a solução de firewall, conforme explicitado ao longo desse estudo técnico preliminar e do mapa de riscos da contratação (SEI 0432015), há a necessidade de um equipamento de alto nível de segurança, pois o equipamento será ativo crítico de segurança para as infraestruturas da Coordenação de Tecnologia da Informação e Comunicações (COTIC) e Diretoria de Infraestrutura de Chaves Públicas (DINFRA).

5.5. Dada essa criticidade, foi adotado como critério de efetividade das soluções de segurança a metodologia de avaliação de soluções da NSS Labs (disponível em <https://www.nsslabs.com/tested-technologies/next-generation-firewall-ngfw/>), tendo como critério de aceitação que a fabricante esteja em ao menos uma das 3 últimas avaliações com 95% de efetividade.

5.6. Como referência, o relatório mais recente foi anexado ao processo (SEI 0435917), com os fabricantes com melhor capacidade de proteção de redes de acordo com a metodologia da instituição supracitada.

5.7. Todas, de forma exemplificativa, aparentam ter soluções aderentes às especificações propostas por este estudo. Contudo, é requisito legal que os licitantes vencedores comprovem a plena adequação ao instrumento licitatório e seus anexos.

5.8. Os equipamentos de conectividade - tanto *switches LAN, SAN e access points* - devem possibilitar a comunicação das redes de computadores do ITI, com o uso de protocolos e técnicas de otimização e segurança de tráfego, com o auxílio dos sistemas de gerenciamento e controle de acesso. Assim, será possível entregar conceitos de vanguarda para assegurar uma rede resiliente e com tempo de vida útil prolongado.

5.9. De acordo com o guia de teletrabalho e BYOD do NIST (*SP 800-114 - User's Guide to Telework and Bring Your Own Device (BYOD) Security*, disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf>), os computadores devem ter:

5.9.1. Limitação para funcionalidades de rede desnecessárias;

5.9.2. Uso limitado de utilitários de acesso remoto;

5.9.3. Antimalware atualizado;

5.9.4. Evitar técnicas de *rooting/jailbreaking* de dispositivos;

5.9.5. Atualização do sistema operacional em dia.

5.10. Esses recursos podem ser monitorados no ambiente corporativos mediante solução de NAC.

5.11. O ITI pretende utilizar conceitos da arquitetura de confiança zero para fortificar sua infraestrutura de rede. Nesse modelo, descrito pelo NIST na SP 800-207 (2nd draft) - Zero Trust Architecture (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf>), todo e qualquer perímetro de rede - inclusive o local - deve ser considerado como não confiável.

5.12. Para tal, há diversas implementações a serem feitas. Dentre elas, todos os acessos devem ser registrados, autenticados e devidamente autorizados. Essa ação só pode ser feita a partir do uso do padrão 802.1x nas portas de acesso à rede, além de haver(em) gateway(s) de acesso, provendo a capacidade da organização provisionar credenciais a partir de papéis organizacionais (*role based access control*).

5.13. Já a NBR/ISO 27002:2013 cita controles sobre os perímetros de rede, descrevendo controles que convém serem implementados a fim de dar maior gerência à equipe responsável, bem como o incentivo a práticas do uso de privilégios mínimos em rede:

13.1.1 Controle de redes

Controle

Convém que as redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações.

Diretrizes para implementação

Convém que controles sejam implementados para garantir a segurança da informação nestas redes, e a proteção dos serviços a elas conectadas, de acesso não autorizado. Em particular, convém que os seguintes itens sejam considerados:

[...]

b) convém que a responsabilidade operacional pelas redes seja separada da operação dos recursos computacionais, onde apropriado (ver 6.1.1);

- c) convém que controles especiais sejam estabelecidos para proteção da confidencialidade e integridade dos dados que trafegam sobre redes públicas ou sobre as redes sem fio (wireless) e proteger os sistemas e aplicações a elas conectadas (ver 10 e 13.2); controles especiais podem também ser requeridos para manter a disponibilidade dos serviços e computadores conectados;
- d) convém que sejam aplicados mecanismos apropriados de registro e monitoração para habilitar a gravação e detecção de ações que possam afetar, ou ser relevante para a segurança da informação;
- e) convém que atividades de gerenciamento sejam coordenadas para otimizar os serviços para a organização e assegurar que os controles estão aplicados de forma consistente sobre toda a infraestrutura de processamento da informação;
- f) convém que sistemas sobre as redes sejam autenticados;
- g) convém que a conexão de sistemas à rede seja restrita.

[...]

13.1.3 Segregação de redes

Controle

Convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes.

Diretrizes para implementação

Um método de controlar a segurança da informação em grandes redes é dividir em diferentes domínios de redes. Os domínios podem ser escolhidos baseado no nível de confiança (por exemplo, domínio de acesso público, domínio de estação de trabalho, domínio de servidor), em todas as áreas da organização (por exemplo, RH, financeiro, marketing). A segregação pode ser feita, tanto usando diferentes redes físicas ou usando diferentes redes lógicas (por exemplo, VPN).

Convém que o perímetro de cada domínio seja bem definido. O acesso entre os domínios de rede é permitido, porém é recomendado que seja controlado no perímetro por meio do uso de um gateway (por exemplo, firewall, roteador de filtro). Convém que o critério para segregação de redes em domínios e o acesso permitido através dos gateways seja baseado em uma avaliação dos requisitos de segurança da informação de cada domínio.

Convém que a avaliação seja feita de acordo com a política de controle de acesso (ver 9.1.1), os requisitos de acesso, o valor e a classificação da informação processada, e que leve em conta o impacto no desempenho e no custo da incorporação da tecnologia gateway, adequada.

Redes wireless requerem tratamento especial devido ao perímetro de rede definido ser fraco. Convém que, para ambientes sensíveis, consideração seja dada para tratar todos os acessos wireless como conexão externa (ver 9.4.2) e segregar esse acesso das redes internas, até que o acesso tenha passado por um gateway, baseado na política de controle de redes (ver 13.1.1), antes de conceder o acesso aos sistemas internos.

Autenticação, encriptação e as normas modernas de tecnologia de níveis de controle de acesso do usuário a rede, baseadas nas redes wireless podem ser suficientes para controlar a conexão com a rede interna da organização, quando implementado adequadamente.

5.14. Já a Norma Complementar nº 7 da IN/1 GSI/PR, diz:

6.3. Quanto aos ativos de informação:

6.3.1. Conter ferramentas de proteção contra acesso não autorizado aos ativos de informação, que favoreça, preferencialmente, a administração de forma centralizada.

6.3.2. Respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação;

5.15. Ou seja, o ITI está implementando um conjunto razoável de boas práticas para ter um ambiente gerenciável e seguro de redes de comunicação.

5.16. Por fim, segue abaixo a análise de conformidade a padrões governamentais exigida pela Instrução Normativa SGD nº1/2019:

Requisito	Solução	Sim	Não	Não se Aplica	Justificativa
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X			Todas as soluções são encontradas em outros órgãos e entidades da Administração Pública
	Solução 2	X			
	Solução 3	X			
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X	Não se aplica pois não se tratam de soluções de software.
	Solução 2			X	
	Solução 3			X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X	
	Solução 2			X	
	Solução 3			X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X	
	Solução 2			X	
	Solução 3			X	
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X	Todas são capazes de receber chaves criptográficas no padrão ICP-Brasil, bem como outros modelos de padrões criptográficos. Entretanto, nenhuma das soluções precisa necessariamente estar aderente às regulamentações da ICP-Brasil para seu pleno funcionamento
	Solução 2			X	
	Solução 3			X	
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X	Não se aplica pois não se tratam de soluções de software.
	Solução 2			X	
	Solução 3			X	

6. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

6.1. Manter o ambiente em código aberto se mostrou ineficaz pelas circunstâncias atuais. O ITI tem sofrido ameaças cada vez mais sofisticadas que sobrecarrega a sustentação de infraestrutura, com pouca efetividade no controle de perímetro. Considerando a rede sem fios, a infraestrutura atual não atende a Autarquia, pois os equipamentos já saíram de produção, contam com tecnologias legadas e os equipamentos começaram a apresentar instabilidades e falhas.

7. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

7.1. Cálculo dos custos totais de propriedade

7.1.1. Visto que a solução 5, considerada viável, é dividida em 2 partes, a análise abaixo também será, tendo a primeira como o que compete à proteção para rede cabeada e a segunda é relativa à proteção de redes com e sem fios.

Solução Viável 5 - Solução de <i>firewall</i> de rede
Descrição
Esta parte da solução abrange um novo perímetro de redes cabeada a partir da aquisição de novos <i>firewalls</i> , com funcionalidades também de prevenção de intrusões, filtro de conteúdo, SD-WAN, antispam, antimalware, geração de relatórios e outras funcionalidades.
Abrange também um novo perímetro de rede sem fios a partir da aquisição de uma nova rede sem fios (<i>wifi</i>), com funcionalidades de segurança por criptografia, métodos fortes de autenticação, prevenção de intrusões e outras funcionalidades, bem como ferramenta de controle e gerenciamento de acessos e novos <i>switches</i> de rede (LAN) e armazenamento (SAN).
Custo Total de Propriedade – Memória de Cálculo
A memória de cálculo dessa solução inclui: aquisição de equipamentos, aquisição e/ou subscrição de licenças, instalação, suporte e garantia do fabricante por 60 meses. Os valores foram estimados conforme Pesquisa de preços (SEI 0453446).

7.2. Mapa comparativo dos cálculos totais de propriedade (TCO)

<Sugere-se a elaboração de um mapa comparativo, consolidando os resultados apresentados. Esta tabela pode variar conforme a complexidade de cada projeto>.

Descrição da solução	Estimativa de TCO ao longo dos anos					Total
	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5	
Solução Viável 5 (firewalls)	R\$ 2.891.994,41	R\$ 0	R\$ 0	R\$ 0	R\$ 0	R\$ 2.891.994,41
Solução Viável 5	R\$ 4.900.333,20	R\$ 0	R\$ 0	R\$ 0	R\$ 0	R\$ 4.900.333,20

(dividido em LAN e SAN)	R\$ 1.387.624,91	R\$ 0	R\$ 0	R\$ 0	R\$ 0	R\$ 1.387.624,91
Total						R\$ 9.179.952,51

8. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

8.1. CENÁRIO: Aquisição de solução integrada de redes

Descrição

Dada a janela de oportunidade de aprimoramento dos controles de perímetro de rede do ITI, é adequado buscar ferramentas que tenha a maior efetividade possível de defesas do ambiente da Autarquia.

Soluções de *firewall* unificadas são capazes de realizar diferentes funções de defesa. O meio ideal de modelagem de defesa é o de segregação total de ativos de proteção, mas há o contexto que o Instituto é uma organização de pequeno a médio porte, com orçamento demasiadamente limitado para adquirir tantas ferramentas.

Portanto, é pertinente que a Administração Pública busque ferramentas de alta taxa de bloqueio, a fim de garantir com o mínimo possível de aquisições aumentar a capacidade de proteção do seu perímetro de rede.

Com a mesma visão, a solução de rede sem fios deve abranger funcionalidades de defesa que suportem as tecnologias atuais, dando capacidade de longo prazo para que o ITI disponibilize conectividade para dispositivos móveis a seus usuários e visitantes, de forma segura.

A compatibilidade dos equipamentos de rede sem fios com os padrões mais atuais de transmissão (802.11x) e segurança (WPA3) possibilitarão que a vida útil dos equipamentos seja prolongada, dado que os equipamentos da rede atual têm mais de 5 anos de uso. A especificação com visão de longo prazo é, também, uma medida de prevenção de riscos de descontinuidade tecnológica dos equipamentos no final do contrato de suporte, caso haja qualquer tipo de restrição orçamentária que impeça o ITI de adquirir nova solução.

Os *switches* serão componentes vitais para o controle de acesso da rede cabeada. Serão montados com base na arquitetura de 3 camadas, entretanto, sem a camada de distribuição. A montagem dos equipamentos possibilitará o ITI a se manter e, se necessário, crescer em quantidade de pontos de acesso, seja pelo crescimento de usuários, seja por novos ativos conectados, a exemplo de telefones de voz sobre IP (VoIP) e dispositivos de internet das coisas (IoT). Aproveita-se também para preparar o ambiente para um futuro uso de redes definidas por *software* (SDN), a partir da compatibilidade dos *switches* para tal arquitetura.

Os *access points* comporão a infraestrutura de redes sem fios, com a adoção de protocolos atuais de transmissão (802.11ax) e segurança (WPA3). Com isso, o ITI mitigará o risco de descontinuidade da solução em eventual encerramento do contrato de garantia com o fabricante em um cenário de restrição orçamentária.

Essa é a realidade encontrada na Autarquia, além de ter ferramentas legadas, estão sem contrato de garantia podendo parar a qualquer momento visto que não houve renovação do parque, em especial pela restrição orçamentária dos últimos anos.

A solução terá também como componente sistemas de controle de acesso. Um será utilizado pela COTIC para administrar o ambiente interno do Instituto (redes sem fios e cabeada) adotando várias técnicas de controle de acesso, a exemplo do registro de dispositivos corporativos por meio de certificado digital. A segunda ferramenta, administrado pela CGISI, será responsável pelo controle de acesso no ambiente que hospeda serviços da ICP-Brasil, fundamental para suprir demandas de toda a infraestrutura de chaves públicas do país.

Por fim, haverá a aquisição de *switches* para redes de armazenamento. Eles serão utilizados para sustentar a comunicação entre servidores e *storages* dos parques computacionais do ITI, viabilizando a disponibilidade dos sistemas hospedados pela Autarquia.

8.1.1. **Relação entre a demanda e a quantidade a ser adquirida**

8.1.2. Durante o estudo realizado, foram observados os seguintes aspectos para o ambiente tecnológico existente no ITI (produção):

- Quantidade de sites (*datacenters*) administrados pela COTIC;
- Necessidade de redundância entre equipamentos;
- Quantidade de usuários e dispositivos conectados;
- Quantidade de largura de banda mensurada pelas ferramentas atuais de monitoramento;
- Quantidade de pontos de acesso (*access points*) da rede sem fios atual;
- Protocolos de rede utilizados no ambiente, inclusive para interligação entre *datacenters*;
- Número de portas de comunicação nos ambientes LAN e SAN;
- Número de fibras óticas dos *backbones* e links dos provedores de *internet*; e
- Perfil de ataques já identificado pelas equipes técnicas da COTIC.

8.1.3. O ITI identificou a necessidade de adquirir 2 perfis de firewall: o primeiro, de maior capacidade, terá a incumbência de atuar também como equipamento principal para proteção da rede local, serviços internos e publicados. O segundo, poderá ser utilizado para a LAN, mas será priorizado para defesa dos serviços publicados, além de ser utilizado nos cenários de contingência e recuperação de desastre.

8.1.4. Os switches serão utilizados para o acesso dos usuários e dispositivos conectados (câmeras, impressoras, etc). Os switches multigigabit serão utilizados nas pilhas de acesso para disponibilizar velocidade compatível com os *access points* da rede sem fios. Os chamados *switches* topo de rack serão utilizados para conectar os nós de virtualização dos ambientes de *datacenter*. Não foram chamados "*switch de datacenter*" pois esta é uma categoria muito mais complexa, robusta e cara para este mesmo fim. Os *switches core* conectarão todos os *switches* da LAN, *firewall*, *links* dos provedores e demais elementos de rede. Todos serão gerenciados por políticas de segurança seguindo boas práticas internacionais, a partir de um sistema de controle de acesso a redes cabeadas e sem fios.

8.1.5. O ambiente de redes sem fios foi elaborado com a finalidade de prover o ITI de capacidade de trabalho com *BYOD*, apoiado por definições de perfis baseados em papéis organizacionais (*Role Based Access Control* - RBAC), além de microsegmentação dos ambientes, utilizando de premissas de redes de confiança zero (*Zero Trust Networks*).

8.1.6. Os equipamentos de redes de armazenamento (*switches fibre channel*) serão utilizados para dar continuidade nos serviços armazenados nas *storages* do ITI, uma vez que foi detectado que os equipamentos atuais podem falhar a qualquer momento, o que causaria a completa indisponibilidade dos sistemas da Autarquia.

8.1.7. Equipamentos adicionais serão utilizados para montar um ambiente compatível com as demandas da DINFRA resultantes das atribuições institucionais elencadas na MP 983/2020.

9. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

9.1. O custo total da contratação foi estimado em R\$ 9.179.952,51.

10. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

10.1. Os resultados esperados da presente contratação são:

10.1.1. Utilização de tecnologias adequadas de controle de acesso da instituição responsável pela infraestrutura de chaves públicas do Brasil;

10.1.2. Ter visibilidade de ataques ocorridos contra o perímetro de rede, possibilitando respostas adequadas para cada caso;

10.1.3. Prover o balanceamento entre os links de telecomunicações contratados pelo ITI para seu site principal e seu site de contingência;

10.1.4. Aperfeiçoar a segurança da informação nos critérios de segurança de rede;

10.1.5. Conter ataques hoje não vistos pela equipe de sustentação de infraestrutura do ITI;

10.1.6. Gerenciar o uso de recursos de rede e mapear os padrões de ataques a fim de compreender, remediar e aprimorar estratégias de defesa de rede; e

10.1.7. Prover segurança para viabilizar o fornecimento e uso de assinaturas eletrônicas avançadas.

10.2. A presente aquisição visa aumentar a efetividade de segurança dos serviços sustentados pelo ITI, bem como estruturar os projetos de inovação presentes em atribuições recentes, como as elencadas na Medida Provisória nº 983, cumprindo requisitos de eficácia, eficiência, efetividade e economicidade para o cumprimento das políticas públicas sob a égide desse Instituto.

10.3. O presente planejamento foi elaborado em harmonia com a Instrução Normativa nº 1/2019 – Secretaria de Governo Digital do Ministério da Economia, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da aquisição. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a aquisição proposta.

10.4. Considerando as informações do presente estudo, entende-se que a presente contratação configura-se técnica e economicamente **VIÁVEL**.

11. APROVAÇÃO E ASSINATURA

A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 36, de 07 de maio de 2020 (SEI 0428205).

Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

Integrante Requisitante	Integrante Técnico
-------------------------	--------------------

ROBERTO WAGNER DE CARVALHO ARAÚJO

Analista de Tecnologia da Informação

Matrícula/SIAPE: 1686826

GIORDANNO AZEVEDO COSTA MARTINS

Analista de Tecnologia da Informação

Matrícula/SIAPE: 1820024

Autoridade Máxima da Área de TIC (ou autoridade superior, se aplicável)

FELIPE BIMBATO RODRIGUES

Coordenador de Tecnologia da Informação e Comunicações

Matrícula/SIAPE: 1820968



Documento assinado eletronicamente por **Giordanno Azevedo Costa Martins, Integrante Técnico**, em 29/10/2020, às 17:02, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).
Nº de Série do Certificado: 48033346914305620050757767996



Documento assinado eletronicamente por **Roberto Wagner de Carvalho Araújo, Integrante Requisitante**, em 29/10/2020, às 17:07, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).
Nº de Série do Certificado: 1287494053113912491



Documento assinado eletronicamente por **Felipe Bimbato Rodrigues, Coordenador**, em 04/11/2020, às 11:57, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).
Nº de Série do Certificado: 22850



A autenticidade deste documento pode ser conferida no site https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0453395** e o código CRC **317C0D0A**.