TERMO DE REFERÊNCIA

SIGA Nº CTEC-TPS-2026/00007

1. OBJETO

1.1. DEFINIÇÕES DO OBJETO

O objeto desta contratação é o fornecimento de uma solução integrada e abrangente de Cibersegurança e Infraestrutura de Rede para o Município de Bento Gonçalves, visando a continuidade da proteção cibernética, a modernização da rede e a gestão proativa de eventos de segurança. A solução compreende os seguintes elementos e serviços:

- **Componentes de Hardware e Plataforma:**
  - **Firewall de Próxima Geração (NGFW)**: Fornecimento de 02 (duas) unidades em regime de comodato, incluindo um módulo de Gerenciamento Centralizado de Logs e Relatórios dedicado.
  - **Switches Core:** Aquisição de 02 (duas) unidades para o ambiente de rede do Município.
  - **Plataforma SIEM (Security Information and Event Management):** Implementação de uma plataforma em modalidade Software as a Service (SaaS).
- **Licenciamento:**
  - Fornecimento de licenças de software para os componentes da solução, com vigência de 36 (trinta e seis) meses.
- **Serviços Especializados:**
  - **Implantação:** Instalação e configuração completa dos equipamentos (NGFW e Switches Core) e da plataforma SIEM.
  - **Operação:** Centro de Operações de Segurança (SOC) em regime 24x7.
  - **Suporte Técnico:** Abrangente para todos os componentes da solução, incluindo capacidade comprovada de atendimento emergencial presencial em até 1 (uma) hora no Município de Bento Gonçalves, e com responsabilidade técnica formal de profissionais qualificados.
  - **Treinamento:** Capacitação da equipe técnica do Município sobre as funcionalidades da solução.

A presente contratação visa à seleção de uma solução que atenda integralmente às especificações técnicas detalhadas no Anexo I que é parte integrante e indissociável deste Termo de Referência.

A composição da solução para fins contratuais é apresentada nos itens abaixo:

ITEM	DESCRIÇÃO	UN.	QTD.
1	SERVIÇOS GERENCIADOS DE CIBERSEGURANÇA (incluindo 2 unidades de NGFW em Comodato, Licenças 36 meses, Plataforma SIEM SaaS, SOC 24x7, Suporte Técnico Especializado)	MÊS	36
2	AQUISIÇÃO DE 02 (DUAS) UNIDADES DE SWITCHES CORE (incluindo Licenças de Suporte do Fabricante para 36 meses e Suporte Técnico Especializado)	UN.	02
3	SERVIÇO DE IMPLANTAÇÃO DE FIREWALL, SWITCHES CORE E PLATAFORMA SIEM	UN.	01
4	SERVIÇO DE TREINAMENTO	UN.	01

1.2. NATUREZA DO OBJETO

Trata-se de bem comum a ser contratado mediante licitação, na modalidade pregão eletrônico.

1.3. QUANTITATIVOS

Os quantitativos seguem a descrição apresentada no item 1.1 deste Termo de Referência, pedido de compras e mapa de cotação em anexo.

1.4. REGISTRO DE PREÇO

Este processo não se enquadra no regime de registro de preços.

1.5. POSSIBILIDADE DE PRORROGAÇÃO

O Contrato terá vigência inicial de 36 (trinta e seis) meses, contados a partir da data de sua assinatura, conforme especificado na descrição do objeto, podendo ser renovado conforme art. 107 da Lei nº 14.133/2021, observando-se os limites legais de prorrogação contratual.

1.6. DESCRIÇÃO DA PRESTAÇÃO DO SERVIÇO

A solução proposta abrange o fornecimento, em regime de comodato, de equipamentos de Firewall de Próxima Geração (NGFW), o fornecimento de licenças de software de Cibersegurança com vigência de 36 (trinta e seis) meses, a aquisição de equipamentos Switches Core acompanhados de suas licenças de suporte do fabricante com vigência de

36 (trinta e seis) meses, a implementação de plataforma de Gerenciamento e Correlação de Eventos de Segurança da Informação (SIEM) em modalidade SaaS e a contratação de serviços especializados de suporte técnico, implantação, operação de Centro de Operações de Segurança (SOC) em regime 24x7, bem como treinamento para a equipe técnica do Município de Bento Gonçalves, e possui as seguintes condições de contratação:

1. Após a homologação, o adjudicatário será convocado para, no prazo de 03 (três) dias, assinar o contrato, preferencialmente na forma digital.

2. Para a assinatura do contrato, a adjudicatária deverá apenas comprovar a manutenção das condições de habilitação apresentadas na fase própria do certame, atualizando eventuais certidões vencidas e atendendo às exigências formais do edital e deste Termo de Referência. A apresentação dos documentos de habilitação dar-se-á na fase específica do procedimento licitatório, nos prazos e meios definidos no edital.

3. As certidões que tenham sido expedidas em meio eletrônico, serão tidas como originais após terem a autenticidade de seus dados e certificação digital conferidos pela Administração, dispensando nova apresentação, exceto se vencido o prazo de validade.

4. O prazo de que trata o item 1 poderá ser prorrogado uma vez e pelo mesmo período, desde que seja requerido de forma motivada e durante o transcurso do respectivo prazo.

5. O contrato para os Serviços Gerenciados de Cibersegurança (Item 1 da tabela do item 1.1) será celebrado por 36 (trinta e seis) meses, com possibilidade de renovação conforme legislação vigente. Os demais itens (aquisição de Switches Core, serviço de implantação e treinamento) são de contratação única e não possuem prorrogação de vigência.

6. A entrega dos equipamentos que compõem a solução de Firewall de Próxima Geração (NGFW) e os Switches Core deve se dar em até 30 dias a contar da data de assinatura do contrato.

7. Serviço de Implantação de Firewall de Próxima Geração (NGFW) e Switches Core (Item 3 da tabela do item 1.1) deverá ter início em no máximo 15 (quinze) dias após o recebimento dos equipamentos e das licenças.

8. O treinamento especializado para a equipe de TI da CONTRATANTE (Item 4 da tabela do item 1.1) deverá ser agendado de forma conjunta entre as partes após a assinatura do contrato.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. JUSTIFICATIVAS

A infraestrutura tecnológica do Município de Bento Gonçalves é protegida por soluções críticas de Cibersegurança, com destaque para o Firewall de Próxima Geração (NGFW). A constante evolução das ameaças cibernéticas e a necessidade de modernização da infraestrutura de rede exigem aprimoramento contínuo, agora com a inclusão de Switches

Core, que, de forma integrada, asseguram a integridade, a confidencialidade e a disponibilidade dos dados e sistemas governamentais.

Com a proximidade do término da vigência das funcionalidades do Firewall de Próxima Geração (NGFW) e a necessidade de modernizar a infraestrutura de rede com a aquisição de Switches Core, impõe-se a abertura de processo licitatório para contratação de solução que garanta a continuidade da proteção e a modernização da rede sem descontinuidade operacional, contemplando o fornecimento de equipamentos de NGFW em regime de comodato, a aquisição de Switches Core e o fornecimento de licenças de Cibersegurança.

A não adoção tempestiva de medidas para garantir a continuidade do Firewall de Próxima Geração (NGFW) e a modernização da rede com os Switches Core expõe a infraestrutura municipal a riscos relevantes: interrupção de funções essenciais de defesa (bloqueio de ataques de rede, prevenção e detecção de intrusões, filtragem de conteúdo, controle de acesso a sites, antispam do e-mail corporativo e controle de aplicações); ampliação da superfície de ataque por ausência de atualizações de assinatura e de mecanismos de inteligência contra ameaças emergentes; e risco de indisponibilidade de sistemas, comprometimento de dados e danos a ativos de TI, com impactos diretos sobre a continuidade de serviços públicos essenciais como saúde, educação e segurança pública. A complexidade e a criticidade dessas infraestruturas demandam, ainda, a atuação de profissionais com formação e responsabilidade técnica específicas, capazes de projetar, implementar e manter sistemas que integrem segurança e rede de forma coesa e resiliente.

Além da gestão de logs e relatórios específicos fornecidos pelos equipamentos de Firewall de Próxima Geração, complementarmente, propõe-se a implementação de plataforma de Gerenciamento e Correlação de Eventos de Segurança da Informação (SIEM) em modalidade SaaS, que elevará significativamente o nível de proteção cibernética do Município através de monitoramento centralizado de eventos de segurança em tempo real, detecção avançada de ameaças e comportamentos anômalos, correlação de eventos entre múltiplos ativos de rede, análise de causa raiz (RCA) de incidentes de segurança, resposta coordenada a ameaças e conformidade regulatória com requisitos de auditoria e rastreabilidade.

A contratação integrada de equipamentos em regime de comodato (NGFW), aquisição de Switches Core, licenças, plataforma SIEM em modalidade SaaS e serviços especializados de suporte técnico, implantação e treinamento garante economia de escala através de negociação única, responsabilidade única pela solução completa, integração técnica adequada entre os componentes (NGFW e Switches Core do mesmo fabricante), continuidade de serviços sem descontinuidade operacional e redução de custos comparado ao parcelamento da contratação.

Para assegurar a operação contínua e a gestão proativa do ambiente, incluem-se serviços especializados em regime 24x7, com atuação de Centro de Operações de Segurança (SOC), observados os respectivos Acordos de Nível de Serviço (ANS).

A modalidade Pregão Eletrônico é a mais adequada para esta contratação, conforme art. 6º, XLI da Lei nº 14.133/2021, por permitir ampla participação de fornecedores, garantir transparência e competitividade, reduzir custos administrativos, acelerar o processo de contratação e facilitar a comparação de propostas.

3. DESCRIÇÃO DA SOLUÇÃO

3.1. SOLUÇÃO

1. FIREWALL DE PRÓXIMA GERAÇÃO (NGFW)

As especificações técnicas detalhadas dos equipamentos NGFW, incluindo seu módulo dedicado de Gerenciamento Centralizado de Logs e Relatórios, funcionalidades de software, capacidades de processamento, throughput, número de conexões simultâneas, módulos de segurança e demais características técnicas encontram-se descritas no Anexo I, que integra este Termo de Referência.

A solução proposta deve atender integralmente às especificações técnicas constantes do Anexo, não sendo permitidas substituições ou alterações sem prévia aprovação formal do Município.

2. PLATAFORMA SIEM

A plataforma de Gerenciamento e Correlação de Eventos de Segurança da Informação (SIEM) deve operar em Ambiente de Nuvem e possuir reconhecimento de mercado, conforme atestado por sua inclusão no Quadrante Mágico do Gartner para SIEM por, no mínimo, 2 (dois) anos consecutivos, e por seu posicionamento relevante em relatórios de avaliação de mercado da Forrester (Forrester Wave para SIEM).

O ambiente da plataforma SIEM deve possuir as certificações: FedRAMP Moderate Authorized, SOC 2 Type 2, HIPAA, PCI DSS e ISO 27001.

A comunicação entre o datacenter da CONTRATANTE e a plataforma SIEM deve ocorrer exclusivamente via TLS.

A solução deve permitir MFA (autenticação multifator), segregação de acessos e opções de armazenamento customizável.

A solução deve possuir registro de logs para fins de auditoria com retenção mínima de 90 (noventa) dias.

O correlacionamento de logs deve ser realizado pela própria plataforma SIEM fornecida pela CONTRATADA.

A solução deve integrar com o framework MITRE ATT&CK.

A solução deve possuir Machine Learning em suas regras.

A solução deve possuir integração nativa com ferramenta de SOAR do mesmo fabricante.

A solução deve coletar e processar, no mínimo, syslogs e flows de dispositivos como switches, NGFW, controladoras Wi?Fi, NAC e roteadores, considerando o ambiente com aproximadamente 1 GB/dia de logs brutos.

A plataforma SIEM deve operar de forma ininterrupta (24x7), garantindo monitoramento e resposta contínuos durante toda a vigência do contrato.

3. INTEGRAÇÃO COM INFRAESTRUTURA EXISTENTE E SWITCHES CORE

Os Switches Core adquiridos devem estar em conformidade com os requisitos de desempenho, funcionalidades e compatibilidade com a infraestrutura de rede existente, conforme especificado no Anexo I que integra este Termo de Referência.

A solução deve garantir compatibilidade e integração nativa entre o Firewall de Próxima Geração (NGFW) e os Switches Core, sendo os equipamentos de ambos do mesmo fabricante, para assegurar o funcionamento integrado da rede e a implementação de políticas de segurança unificadas.

A plataforma SIEM se integra com o NGFW e os Switches Core através de conectores e APIs, complementando a proteção com monitoramento centralizado e análise avançada de eventos de segurança.

A CONTRATADA é responsável por garantir a compatibilidade técnica entre todos os componentes da solução e a infraestrutura existente do Município, realizando testes de integração e validação antes da implantação em ambiente de produção.

4. REGIME DE COMODATO DO NGFW

As 02 (duas) unidades de equipamentos NGFW serão fornecidas em regime de comodato, permanecendo a CONTRATADA como proprietária dos equipamentos durante toda a vigência do contrato e responsável por sua manutenção, seguro e reposição, enquanto o Município terá direito de uso dos equipamentos durante o período contratual. A CONTRATADA assumirá integralmente:

a) Manutenção preventiva e corretiva dos equipamentos, sem custo adicional ao Município;

b) Reposição de equipamentos em caso de falhas, defeitos ou obsolescência, em prazo máximo de 48 (quarenta e oito) horas;

c) Garantia integral dos equipamentos durante toda a vigência do contrato;

d) Atualizações de software, patches de segurança e firmware, conforme disponibilizados pelo fabricante;

e) Substituição de componentes defeituosos sem custo adicional;

f) Devolução dos equipamentos ao final do contrato em perfeito estado de funcionamento.

4. REQUISITOS DA CONTRATAÇÃO

4.1. REQUISITOS PARA A EXECUÇÃO DO SERVIÇO

4.1.1. REQUISITOS GERAIS

A CONTRATADA deverá executar a instalação física e a configuração lógica da solução completa (Firewall de Próxima Geração, Switches Core e Plataforma SIEM), conforme especificado neste Termo de Referência.

Correrá por conta da CONTRATADA toda e qualquer despesa, independentemente da sua natureza, decorrente dos serviços de instalação e configuração aqui mencionados, incluindo deslocamento e demais despesas de seus profissionais para as unidades onde as soluções serão instaladas.

Caberá a CONTRATANTE subsidiar toda infraestrutura necessária para implantação dos equipamentos, exemplo: locais de instalação dos appliances de Firewalls e Switches Core (Racks, gavetas).

Os serviços de implantação deverão ser executados presencialmente nas instalações da CONTRATANTE por técnico(s) da CONTRATADA capacitado(s) para tal.

Após o recebimento dos equipamentos e das licenças, a CONTRATANTE deverá definir, juntamente com a CONTRATADA, o cronograma de instalação e configuração dos mesmos, enviando a CONTRATADA, documento contendo informações de Data, Hora, Local, e soluções a serem instaladas.

4.1.2. FASES DO SERVIÇO DE IMPLANTAÇÃO

As fases da implantação dos serviços devem contemplar:

Planejamento: nesta etapa a CONTRATADA deverá realizar o planejamento da solução a ser implementada, onde serão definidos os prazos por atividade, as pessoas, a estratégia de implantação do serviço, o plano de testes, bem como quaisquer outros itens que sejam necessários para a implantação da respectiva solução. Deve-se considerar as janelas de manutenção da CONTRATANTE, plano de rollback e o escopo definido. Os responsáveis técnicos da CONTRATANTE acompanharão e aprovarão o planejamento.

Implantação: após a aprovação do planejamento deverá ser iniciado o processo de implantação, levando-se em consideração a disponibilidade das equipes envolvidas, cumprimento dos prazos pactuados e o foco principal do projeto visando tornar o ambiente mais seguro e controlado, quanto à confidencialidade, integridade e disponibilidade do ambiente.

Etapa de Testes: todos os controles implantados para a ativação da solução deverão ser testados a cada etapa pré-definida no planejamento. Além disso, o plano de rollback deverá garantir o retorno exequível e ágil, caso ocorra alguma falha no processo de implantação dos controles necessários à prestação do serviço.

Homologação: Após a conclusão dos testes, a solução deverá ser formalmente homologada pela CONTRATANTE. A CONTRATANTE terá o prazo de 02 (dois) dias consecutivos, contados a partir da data de conclusão dos serviços de instalação e configuração dos serviços contratados, para emitir o relatório de homologação (aceite).

O serviço será aceito se, e somente se, houver comprovação de que todos os requisitos técnicos especificados neste Termo de Referência tenham sido atendidos. Essa comprovação será feita mediante observação direta das características dos equipamentos utilizados, consulta à documentação técnica fornecida e verificação dos serviços de instalação e configurações, comparadas aos itens deste Termo.

No cronograma de instalação poderão ser definidos períodos fora do horário comercial, assim como fins de semana e feriados.

O processo de instalação, implantação e configuração deverá ter início em no máximo 15 (quinze) dias após o recebimento dos equipamentos e das licenças.

4.1.3. ESCOPO DO SERVIÇO DE IMPLANTAÇÃO

4.1.3.1. Instalação física dos equipamentos de Firewall de Próxima Geração (NGFW) e Switches Core, conforme contratado.

4.1.3.2. Configuração lógica das Soluções de Firewall e Switches Core conforme segmentação de rede definida pela CONTRATANTE.

4.1.3.3. Atualização e aplicação de correções nas soluções de Firewall e Switches Core.

4.1.3.4. Implementação/migração de regras de Filtragem (para NGFW).

4.1.3.5. Implementação/migração de regras de NAT (para NGFW).

4.1.3.6. Implementação/migração de regras de QoS (para NGFW e Switches Core).

4.1.3.7. Implementação/migração de regras de Filtro de Conteúdo Web, IPS, Antimalware, Controle de Aplicativos, e Proteção Contra Ameaças Avançadas (para NGFW).

4.1.3.8. Implementação de alta disponibilidade (para NGFW e Switches Core).

4.1.3.9. Implementação de monitoramento de links (para NGFW).

4.1.3.10. Integração com o Active Directory (para NGFW).

4.1.3.11. Tunning de configuração e regras de filtragem (para NGFW), removendo as regras inalcançáveis, adicionando uma descrição para cada regra implementada, remoção de elementos de rede não utilizados.

4.1.3.12. Testes gerais, validando o funcionamento das aplicações após a implementação das Soluções de Firewall, Switches Core e Plataforma SIEM.

4.1.3.13. Provisionamento e instalação do appliance virtual para a solução de Gerenciamento Centralizado de Logs e Relatórios.

4.1.3.14. Configuração inicial da solução de Gerenciamento Centralizado de Logs e Relatórios, incluindo parâmetros de rede, acesso administrativo e ajustes básicos.

4.1.3.15. Configuração do envio de logs dos Firewalls de Próxima Geração (NGFW) para a solução de Gerenciamento Centralizado de Logs e Relatórios.

4.1.3.16. Definição de políticas de armazenamento e retenção de logs na solução de Gerenciamento Centralizado de Logs e Relatórios.

4.1.3.17. Configuração de painéis (dashboards) e relatórios padrão na solução de Gerenciamento Centralizado de Logs e Relatórios.

4.1.3.18. Configuração de usuários e perfis de acesso na solução de Gerenciamento Centralizado de Logs e Relatórios.

4.1.3.19. Registro e associação dos dispositivos de firewall e Switches Core à plataforma SIEM.

4.1.3.20. Configuração de comunicação para permitir o tráfego de logs entre os equipamentos (NGFW e Switches Core) e a plataforma SIEM.

4.1.3.21. Importar configurações existentes (para NGFW e Switches Core), quando aplicável.

4.1.3.22. Configuração de alertas e notificações para eventos críticos de segurança na plataforma SIEM.

4.1.3.23. Definição de grupos de administração na plataforma SIEM.

4.1.3.24. Configuração de VLANs, roteamento e outras configurações de rede avançadas nos Switches Core.

4.1.3.25. Configuração da interconexão e integração entre o Firewall de Próxima Geração (NGFW) e os Switches Core, garantindo o fluxo de tráfego e a aplicação de políticas.

Não faz parte do Escopo dos Serviços de Implantação da Solução:

4.1.3.26. Passagens de cabo que não compreendam as necessárias para conectividade dos equipamentos (NGFW e Switches Core).

4.1.3.27. Instalação de demais soluções e equipamentos que não compreendam os mencionados neste serviço de implantação (NGFW, Switches Core, Plataforma SIEM).

4.1.3.28. Configuração de equipamentos de terceiros não relacionados diretamente à solução contratada.

4.1.4. DOCUMENTAÇÃO

Ao término da instalação, a CONTRATADA deverá entregar Caderno de Documentação do Projeto, no qual conste todos os detalhes da instalação, tais como:

a) Descrição dos serviços implantados;

b) Descrição de topologia lógica e de topologia física dos equipamentos (NGFW e Switches Core) após a ativação dos serviços;

c) Dados dos equipamentos e softwares (NGFW, Switches Core, Plataforma SIEM), incluindo configurações, números de série e versões;

d) Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos (NGFW e Switches Core) e softwares (NGFW e Plataforma SIEM);

e) Definição de responsabilidades;

f) Recursos de alta disponibilidade (para NGFW e Switches Core);

g) Procedimentos para abertura e atendimento a chamados;

h) Procedimentos de recuperação de equipamentos (NGFW e Switches Core);

i) Rotinas de backup e restore dos equipamentos (NGFW e Switches Core), softwares e configurações implantadas;

j) Documentação dos processos de trabalho associados ao item;

k) Desenho dos racks onde estão instalados os equipamentos (bayface);

l) Definição de padrões porventura existentes na solução (ex. padrão de nome de objetos).

4.1.5. SERVIÇOS DE CIBERSEGURANÇA

O propósito do gerenciamento executado pela CONTRATADA é manter a estabilidade, disponibilidade e integridade do ambiente computacional da CONTRATANTE, operando e sustentando todas as soluções de segurança contemplados nesse Termo de Referência (Firewall de Próxima Geração, Switches Core e Plataforma SIEM), além de responder às solicitações dos usuários, resolver incidentes e realizar atividades proativas para reforçar a segurança.

Durante os primeiros 30 dias de prestação do serviço, a CONTRATADA deverá conduzir uma avaliação abrangente do ambiente do CONTRATANTE, visando identificar lacunas ou oportunidades de aprimoramento (Gap Analysis) dos controles de segurança do CONTRATANTE.

A CONTRATADA deverá ter processos estabelecidos que assegurem a proteção das informações do CONTRATANTE, em conformidade com a norma ABNT NBR ISO/IEC 27001.

A CONTRATADA será responsável pela manutenção, ativação e gestão de licenciamento de todos os componentes da solução (NGFW e Switches Core), bem como a atualização da solução durante a vigência do contrato.

Principais atividades a serem executadas de forma contínua pela CONTRATADA:

4.1.5.1. Acompanhar a execução dos serviços para garantir a conformidade com os níveis de serviço estabelecidos.

4.1.5.2. Realizar monitoramento contínuo e avaliações periódicas dos produtos e serviços de segurança do CONTRATANTE.

4.1.5.3. Adotar medidas proativas para prevenir e identificar incidentes de segurança antes que impactem os serviços.

4.1.5.4. Responder prontamente aos eventos de Segurança da Informação que possam comprometer a disponibilidade, integridade ou confidencialidade das informações.

4.1.5.5. Agir imediatamente em caso de falha nos controles de segurança ou situações que possam ameaçar os sistemas e serviços de TI.

4.1.5.6. Em caso de necessidade definida pelo CONTRATANTE o atendimento à resposta de incidentes deverá ser executado presencialmente nas instalações da CONTRATANTE pela CONTRATADA.

4.1.5.7. Para a execução do atendimento presencial todos os custos atrelados como hospedagem, deslocamento e alimentação deverão ser arcados pela CONTRATADA sem ônus para a CONTRATANTE.

4.1.5.8. Fornecer relatórios técnicos e gerenciais para evidenciar a execução dos serviços.

4.1.5.9. Exercer supervisão sobre a equipe na realização dos serviços de segurança da informação.

4.1.5.10. Elaborar planos de execução e treinamento para os profissionais envolvidos, além de orientar a equipe técnica em situações críticas.

4.1.5.11. Prestar atendimento em primeiro nível de solicitações, requisições e incidentes relacionados aos serviços de segurança.

4.1.5.12. Oferecer recomendações e colaborar na elaboração e atualização contínua, com o respaldo e concordância do CONTRATANTE, de procedimentos estruturados e do repositório de conhecimento, abrangendo todas as soluções para questões resolvidas com respostas padronizadas.

4.1.5.13. Receber as solicitações dos serviços referentes à solução de Cibersegurança e infraestrutura de rede contempladas nesse Termo de Referência e coordenar a realização e distribuição de recursos de trabalho.

4.1.5.14. Desenvolver e apresentar relatórios de atividades mensais (mês calendário), referente aos serviços gerenciados de segurança, provendo informações gerenciais ao CONTRATANTE.

4.1.5.15. Propor novas tecnologias para atualizar o ambiente tecnológico, visando apoiar a equipe do CONTRATANTE na gestão da segurança da informação.

4.1.6. ACORDO DE NÍVEL DE SERVIÇO (ANS)

A prestação do serviço, objeto deste Termo de Referência, deverá estar disponível conforme os indicadores, níveis de prioridade e prazos detalhados abaixo:

NÍVEIS DE SERVIÇO

Tipo	Indicador	Nível de Serviço
Atendimento	Resolução de incidente dentro do prazo estipulado	95%
Atendimento	Atendimento de solicitação dentro do prazo estipulado	95%

NÍVEIS DE PRIORIDADE

Prioridade	Descrição
1. Emergencial	O serviço está inoperante ou há um impacto crítico nas operações para o negócio. ***O atendimento aos chamados com nível de prioridade Emergencial devem ser realizados obrigatoriamente de forma presencial (in loco) nas instalações físicas da CONTRATANTE***.
1. Alta	O serviço está comprometido ou aspectos significativos das operações foram negativamente afetados pelo desempenho insatisfatório
1. Média	O serviço está operacional, porém com problemas menores que não afetam diretamente as operações
1. Baixa	O desempenho operacional do serviço está comprometido, mas sem afetar sua funcionalidade ou operação
1. Planejada	Um incidente ou evento que não interrompe ou degrada os serviços ao cliente, mas requer ação planejada

PRAZOS DE ATENDIMENTO

Prioridade da solicitação	Nível de Serviço (SLA)
1. Emergencial	1 hora
1. Alta	2 horas
1. Média	8 horas
1. Baixa	16 horas
1. Planejada	24 horas

4.1.7. LOCAL DE EXECUÇÃO DO SERVIÇO

Os serviços acordados podem ser realizados à distância pela CONTRATADA, mas também podem ser executados in loco, mediante acordo entre as partes, nos casos em que o acesso remoto não seja viável ou quando a situação exija, cobrindo toda a infraestrutura de segurança e usuários da CONTRATANTE.

As atividades de implantação, descritas no item 3 da tabela do item 1.1 deste Termo de Referência, devem ser realizadas presencialmente (in loco) nas instalações físicas da CONTRATANTE.

Os serviços de Cibersegurança, descritos no item 1 da tabela do item 1.1 deste Termo de Referência, podem ser oferecidos a partir das instalações da CONTRATADA ou de forma remota.

Chamados classificados como 'Emergencial' terão atendimento presencial obrigatório (in loco).

4.1.8. HORÁRIOS DE EXECUÇÃO DO SERVIÇO

Os Serviços de Cibersegurança para Firewall de Próxima Geração (NGFW), Switches Core, incluindo Plataforma SIEM, SOC, devem ser fornecidos remotamente em período integral, 24x7 (24 horas por 7 dias da semana), com a possibilidade de atendimento presencial nas instalações da CONTRATANTE em caso de incidentes graves de segurança que afetem a disponibilidade, integridade ou confidencialidade das informações.

4.1.9. SOC – OPERAÇÕES DE SEGURANÇA

4.1.9.1. Geral

4.1.9.1.1. O serviço de SOC deve ser prestado majoritariamente de forma remota.

4.1.9.1.2. O serviço deverá estar disponível 24x7 (24 horas por 7 dias da semana) durante toda a vigência do contrato.

4.1.9.1.3. Além do SOC, a CONTRATADA deverá utilizar ferramenta de monitoramento com console (podendo ser em nuvem), com acesso a partir do ambiente da CONTRATANTE e controle do monitoramento tanto no ambiente da CONTRATADA quanto da CONTRATANTE.

4.1.9.1.4. Requisitos mínimos:

a) Conectividade aos data centers dos sistemas de suporte, monitoramento, administração e gerenciamento via múltiplas conexões LAN/WAN, sem ponto único de falha;

b) Estrutura central para visualização simultânea de painéis por todos os profissionais.

4.1.9.2. SIEM (Requisitos Operacionais)

Os requisitos técnicos, certificações e reconhecimento de mercado da plataforma SIEM para suporte ao SOC são os estabelecidos na Seção 3.1 deste Termo de Referência. Adicionalmente, em termos operacionais, o SIEM deve:

4.1.9.2.1. Assegurar que a comunicação entre o datacenter da CONTRATANTE e o SIEM ocorra exclusivamente via TLS.

4.1.9.2.2. Exigir autenticação multifator (MFA) para acesso.

4.1.9.2.3. Possuir segregação de acessos compatível com os perfis operacionais do SOC.

4.1.9.2.4.Oferecer opções de armazenamento customizável para dados e logs.

4.1.9.2.5. Manter registro de logs para fins de auditoria com retenção mínima de 90 dias.

4.1.9.2.6. Integrar com o framework MITRE ATT&CK.

4.1.9.2.7. Empregar técnicas de Machine Learning para detecção e correlação de regras.

4.1.9.2.8. Possuir integração nativa com ferramenta de SOAR do mesmo fabricante.

4.1.9.2.9. Operar de forma ininterrupta, 24x7, garantindo monitoramento e resposta contínuos durante toda a vigência do contrato.

4.1.9.3. Incidentes

4.1.9.3.1. Monitoração

4.1.9.3.1.1. Monitoramento proativo e reativo (com anuência da CONTRATANTE) de aplicações web, servidores, virtualizadores, equipamentos de rede (NGFW, Switches Core) em Internet e Intranet.

4.1.9.3.1.2. Considera-se volume de 1 GB/dia de logs brutos de ativos (servidores, roteadores, switches etc.).

4.1.9.3.1.3. O SIEM deverá suportar retenção mínima de 90 dias.

4.1.9.3.1.4. Papéis da CONTRATADA:

a) Monitorar disponibilidade e desempenho dos equipamentos e de todo o escopo contratado quanto a incidentes de segurança;

b) Gerir incidentes (alertas, detecção, abertura de chamados);

c) Acompanhar incidentes de ponta a ponta;

d) Acionar por matriz de escalação hierárquica/funcional;

e) Correlacionar eventos e incidentes de forma automatizada entre ITSM e monitoramento;

f) Acompanhar por indicadores de desempenho.

4.1.9.3.2. Detecção e resposta

4.1.9.3.2.1. Elaborar Plano de Resposta aos Incidentes mais comuns, contendo:

4.1.9.3.2.2. Tipo de incidente;

4.1.9.3.2.3. Ações a serem realizadas;

4.1.9.3.2.4. Responsáveis (nome, telefone, e-mail).

4.1.9.3.2.5. Correlacionamento de logs por SIEM fornecido pela CONTRATADA, com reconhecimento de mercado, conforme atestado por sua inclusão no Quadrante Mágico do Gartner para SIEM por, no mínimo, 2 (dois) anos consecutivos e presença na listagem de SIEM da Forrester.

4.1.9.3.2.6. Detecção de atividades maliciosas via coleta de syslogs e flows de switches, NGFW, controladoras Wi?Fi, NAC e roteadores.

4.1.9.3.2.7. Reagir a eventos que afetem disponibilidade, integridade ou confidencialidade da informação.

4.1.9.3.2.8. Controlar ações, notificações e escalonamento, articulando-se com as equipes da CONTRATANTE para definir contenção, erradicação e recuperação.

4.1.9.3.2.9. Gerar alertas e estratégias de prevenção para todos os ambientes da CONTRATANTE em caso de ataque.

4.1.9.3.2.10. Criar, revisar e manter playbooks de segurança para agilizar a resposta a incidentes.

4.1.9.3.2.11. Transferir os playbooks para a CONTRATANTE (sem transferência de propriedade intelectual).

4.1.9.3.2.12. Ofertar treinamento mínimo de 4 horas à equipe de TI da CONTRATANTE, cobrindo operação do SIEM (relatórios e consultas).

4.1.9.3.3. Relatórios

4.1.9.3.3.1. Para cada incidente identificado, emitir relatório com, no mínimo:

4.1.9.3.3.2. Impactos observados;

4.1.9.3.3.3. Criticidade;

4.1.9.3.3.4. Componentes relacionados;

4.1.9.3.3.5. Vulnerabilidades exploradas;

4.1.9.3.3.6. Origem do ataque;

4.1.9.3.3.7. Destino do ataque;

4.1.9.3.3.8. Descrição do evento.

4.1.10. TREINAMENTO

O objetivo deste treinamento é capacitar os membros da equipe de TI da CONTRATANTE, permitindo que auxiliem efetivamente na gestão das tecnologias implementadas. A CONTRATADA, responsável pela gestão principal da solução, deverá fornecer este treinamento para assegurar que a equipe da CONTRATANTE compreenda os princípios fundamentais da solução de segurança de rede, realize operações básicas e intermediárias, identifique e reporte problemas com eficiência, interprete logs e relatórios e colabore na implementação de políticas de segurança, criando sinergia entre as equipes e melhor aproveitamento das tecnologias.

O treinamento deverá ser realizado na modalidade presencial

A carga horária total mínima será de 16 horas.

O treinamento deverá ser ministrado em 2 dias úteis consecutivos, com 8 horas diárias.

O treinamento deverá abordar os tópicos relevantes para a administração de segurança de rede, incluindo, mas não se limitando a:

Configuração inicial e setup dos equipamentos

Registro e gerenciamento de licenças

Criação de zonas e interfaces

Criação de objetos de endereço de host e objetos de serviço

Criação de regras e zonas de segurança

Configuração de regras de acesso

Configuração de Network Address Translation (NAT)

Configuração de roteamento

Configuração de balanceamento de carga e failover

Implementação de VPN e SSL VPN

Configuração de VPN Site-to-Site

Criação de VPN baseada em rota

Configuração de SSL-VPN com LDAP

Configuração de regras de aplicativos e controle de aplicações

Implementação de proteções básicas e avançadas (IPS, antivírus e anti-spyware; proteção básica; proteção avançada)

Configuração de filtro de conteúdo web

Integração com LDAP e autenticação de usuário com Single Sign-On (SSO)

Habilitação e configuração de inspeção HTTPS

Otimização de largura de banda de aplicativos

Configuração de WAN Failover

Configuração de SD-WAN

Configuração de alta disponibilidade básica (ativo/standby)

Ferramentas básicas de solução de problemas

O treinamento deverá ser oficial, ministrado por instrutores certificados pelo fabricante da solução, com comprovada experiência prática.

Ao final, a CONTRATADA deverá emitir certificado de participação para todos os participantes que atingirem a frequência mínima exigida, contendo, no mínimo: nome do participante, nome do curso, carga horária e período de realização.

A CONTRATADA deverá oferecer suporte pós-treinamento por 30 dias corridos, contados a partir da conclusão do treinamento.

O suporte pós-treinamento deverá incluir:

Esclarecimento de dúvidas relacionadas ao conteúdo ministrado durante o treinamento.

Auxílio na aplicação prática dos conhecimentos adquiridos.

O suporte deverá ser fornecido por meio de e-mail ou sistema de chamados, com prazo de resposta não superior a 2 dias úteis.

4.2. QUALIFICAÇÕES TÉCNICAS

1. Visita Técnica: A empresa deve apresentar na habilitação uma declaração assinada de que realizou visitação e que tem pleno conhecimento da totalidade dos serviços a serem contratados. Esta visita deverá ser agendada previamente junto à CONTRATANTE e comprovada na fase de habilitação por meio de declaração assinada pelo responsável técnico da CONTRATANTE. O agendamento deverá ser realizado através do telefone (54) 3055 7248 com Ariel Petroli, Munir Hassen Ismael ou Rodrigo Golin Fernandes. A exigência de realização de visita técnica pelas licitantes justifica-se pela necessidade de que os participantes do certame conheçam as condições reais do local de execução do objeto da licitação, possibilitando o correto dimensionamento de recursos, equipe, equipamentos e cronograma de execução. Entretanto, nos termos dos §§ 2º e 3º do art. 63 da Lei Federal nº 14.133/2021, será admitida a substituição da visita técnica por autodeclaração da licitante, na qual esta ateste possuir conhecimento pleno das condições e peculiaridades necessárias à execução do objeto contratado.
2. Declaração do Fabricante: Declaração emitida pelo fabricante da solução ofertada, atestando que a licitante está autorizada a comercializar, implementar e prestar suporte técnico para os produtos e serviços propostos neste certame.
3. Apresentar certificação válida do fabricante da solução ofertada, garantindo a competência técnica necessária para a execução dos serviços especificados neste contrato de no mínimo 1 funcionário. Em caso de substituição de funcionário, deverá ser apresentada a documentação do novo colaborador.
4. Para assinatura do Contrato a empresa deverá comprar vínculo dos profissionais que possuem certificação válida do fabricante da solução ofertada com a empresa por meio de: CTPS (empregados), contrato de prestação de serviços (terceirizados) ou ato constitutivo (sócios/titulares).

4.2.1. ATESTADOS DE CAPACIDADE TÉCNICO–PROFISSIONAL

A CONTRATADA deverá disponibilizar, durante a execução do contrato, equipe técnica composta, no mínimo, por um (01) profissional que possua certificação válida do fabricante da solução ofertada, garantindo a competência técnica necessária para a execução dos serviços especificados neste contrato.

O profissional designado deverá comprovar sua certificação mediante apresentação de documentação oficial.

4.2.2. ATESTADOS DE CAPACIDADE TÉCNICO-OPERACIONAL

A CONTRATADA deverá apresentar, no mínimo, 01 (um) Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, que comprove a execução satisfatória de serviços de Cibersegurança com características semelhantes e complexidade tecnológica e operacional equivalente ou superior ao objeto desta licitação.

4.2.3. PESSOAL TÉCNICO DISPONÍVEL

4.2.3.2. CONDIÇÃO PARA ASSINATURA DO CONTRATO

Comprovação do vínculo dos profissionais que possuem certificação válida do fabricante da solução ofertada com a empresa por meio de: CTPS (empregados), contrato de prestação de serviços (terceirizados) ou ato constitutivo (sócios/titulares).

Participação efetiva, nos serviços contratados, dos profissionais indicados para fins de comprovação técnico profissional; admite-se substituição por profissionais de experiência equivalente ou superior, mediante aprovação prévia da CONTRATANTE.

A CONTRATANTE poderá solicitar, a qualquer tempo, a substituição de profissional cujo desempenho seja considerado insatisfatório ou que não atenda às exigências contratuais.

4.3. SUB-CONTRATAÇÃO PARCIAL DO OBJETO

Será permitida a subcontratação do SOC (Centro de Operações de Segurança) e SIEM (Gerenciamento e Correlação de Eventos de Segurança), desde que:

a) Seja previamente aprovada por escrito pelo Município;

b) O subcontratado atenda aos mesmos requisitos de qualificação técnica e segurança;

c) A CONTRATADA permaneça responsável integralmente pelos serviços subcontratados;

d) O Município possa exigir substituição do subcontratado que não atendam aos requisitos;

e) Seja mantida a qualidade e continuidade dos serviços conforme ANSs estabelecidos.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1. INÍCIO DA EXECUÇÃO DO SERVIÇO

A execução do objeto deste Termo de Referência seguirá o seguinte cronograma:

a) Entrega dos equipamentos de Firewall de Próxima Geração (NGFW) e Switches Core: até 30 dias após a assinatura do contrato.

b) Início da instalação e implantação da solução de Firewall de Próxima Geração (NGFW), Switches Core e Plataforma SIEM: em no máximo 15 (quinze) dias após o recebimento dos equipamentos e das licenças.

c) Início dos Serviços de Cibersegurança para Firewall de Próxima Geração (NGFW), Plataforma SIEM, SOC (item 1 da tabela do item 1.1): imediatamente após a conclusão do Serviço de Implantação da solução completa e a ativação das suas respectivas licenças.

d) O treinamento especializado para a equipe de TI da CONTRATANTE deverá ser agendado de forma conjunta entre as partes após a assinatura do contrato.

e) Vigência das licenças de Firewall de Próxima Geração (NGFW): 36 (trinta e seis) meses a partir da data de ativação, podendo ser prorrogado conforme legislação vigente e interesse da Administração.

f) Vigência do contrato para os serviços contínuos (item 1 da tabela do item 1.1): 36 (trinta e seis) meses, podendo ser prorrogado conforme legislação vigente e interesse da Administração.

g) O faturamento do item 1 (serviços gerenciados de Cibersegurança, infraestrutura de rede, SIEM, SOC, com comodato e licenças) terá início exclusivamente após a emissão do Termo de Aceite da Implantação pela CONTRATANTE e a ativação das licenças correspondentes.

A CONTRATADA deverá observar rigorosamente os prazos de início da execução dos serviços, bem como os demais prazos estipulados neste Termo de Referência, sob pena de aplicação das sanções previstas no contrato.

5.2. LOCAL DE EXECUÇÃO DO SERVIÇO

Coordenadoria de Tecnologia de Informação e Comunicação - CTEC.

Rua 10 de Novembro, 190. Bairro Cidade Alta, Bento Gonçalves/RS

CEP: 95700-382

5.3. UNIDADE RESPONSÁVEL

Coordenadoria de Tecnologia de Informação e Comunicação - CTEC.

6. GESTÃO DO CONTRATO

6.1. MODELO DE GESTÃO DO CONTRATO

O não cumprimento dos requisitos estabelecidos neste Termo de Referência poderá resultar na aplicação de penalidades previstas em contrato, incluindo multas e rescisão contratual, conforme a gravidade da infração.

6.2. MODELO DE GESTÃO DO CONTRATO

a) Nos termos da Lei nº 14133, de 2021, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário a regularização de falhas ou defeitos observados.

b) A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer Irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com a Lei nº 14133, de 2021.

c) O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

6.2. FISCAL DO CONTRATO OU SERVIDOR RESPONSÁVEL

Ariel Petroli e Munir Hassen Ismael

7. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

7.1. FORMA DE PAGAMENTO

O pagamento será efetuado de acordo com o seguinte cronograma:

a) Para o item 1 (serviços gerenciados de Cibersegurança, infraestrutura de rede, Plataforma SIEM, SOC, incluindo o comodato de NGFW e licenças): pagamentos mensais, com início exclusivamente após a emissão do Termo de Aceite da Implantação pela CONTRATANTE e a ativação das licenças correspondentes.

b) Para o item 2 (Serviço de Implantação de Firewall de Próxima Geração (NGFW), Switches Core e Plataforma SIEM): O valor total deste será pago após a conclusão e aceite formal do serviço pela CONTRATANTE.

c) Para o item 3 (Serviço de Treinamento): O valor total deste será pago após a conclusão e aceite formal do serviço pela CONTRATANTE.

A Nota Fiscal da prestação de serviço mensal deverá ser emitida até o dia 25 do mês e o pagamento será efetuado até o 10º (décimo) dia do mês subsequente ao fornecimento e serviços prestados, mediante aceite dos servidores responsáveis.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

8.1. FORMA DE JULGAMENTO

O fornecedor será selecionado por meio da realização de procedimento licitatório, com adoção do critério de julgamento pelo MENOR PREÇO GLOBAL.

8.2. ADJUDICAÇÕES DO OBJETO

A adjudicação do objeto será realizada pelo critério de menor valor global, considerando todos os itens listados na descrição do objeto deste Termo de Referência. Esta decisão se justifica pelos seguintes motivos:

Integração Técnica e Operacional da Solução: A solução proposta é um ecossistema integrado que abrange o Firewall de Próxima Geração (NGFW), os Switches Core e a Plataforma de Gerenciamento e Correlação de Eventos de Segurança da Informação (SIEM). É crucial que o NGFW e os Switches Core sejam do mesmo fabricante, para assegurar uma sinergia técnica profunda, compatibilidade e otimização de funcionalidades de segurança e rede. Já a Plataforma SIEM, que pode ser de um fabricante distinto, será integrada aos demais componentes e à infraestrutura existente por meio de conectores e APIs, garantindo o monitoramento centralizado e a correlação de eventos de toda a solução.

A contratação de uma única empresa (CONTRATADA) responsável por fornecer, implementar e gerenciar todos esses componentes, bem como seus serviços especializados, é fundamental para garantir a integração técnica e operacional fluida, a eliminação de pontos de falha na responsabilidade e a maximização da eficácia de toda a infraestrutura de segurança e rede**.**

Continuidade e consistência dos serviços: A empresa que fornecerá os serviços gerenciados de Cibersegurança (incluindo o comodato de NGFW, licenças e Plataforma SIEM - Item 1 da tabela do item 1.1) será também responsável pelos serviços de implantação (NGFW, Switches Core e Plataforma SIEM - Item 2), e pelos serviços de Treinamento (Item 3). Isso assegura uma abordagem coesa e consistente em todas as fases, desde a implementação até a manutenção e operação das soluções.

Otimização de recursos: A contratação global permite uma negociação de condições mais vantajosas e preços competitivos, aproveitando a economia de escala que um fornecedor único pode oferecer, resultando em uma otimização significativa dos recursos públicos.

Simplificação da gestão contratual: A existência de um único contrato para todos os itens da solução (equipamentos, licenças, plataforma e serviços especializados) simplifica drasticamente os processos de gestão, fiscalização e acompanhamento por parte da Administração, reduzindo a carga administrativa.

Garantia de compatibilidade: A adjudicação global assegura que todos os componentes da solução sejam plenamente compatíveis entre si, especialmente considerando que os equipamentos de Firewall e Switches Core serão do mesmo fabricante, e que a Plataforma SIEM se integrará com a infraestrutura via interfaces padronizadas. Isso minimiza riscos de incompatibilidades, falhas de comunicação ou conflitos técnicos que poderiam surgir com múltiplos fornecedores e integradores.

Responsabilidade unificada: Um único fornecedor será o ponto de contato e responsável por todos os aspectos da solução, desde a entrega e instalação dos equipamentos até a prestação dos serviços contínuos de monitoramento, suporte e resposta a incidentes. Esta responsabilidade unificada facilita a resolução rápida de problemas e garante o cumprimento dos Acordos de Nível de Serviço (ANS) estabelecidos.

Esta abordagem de adjudicação global está alinhada com os objetivos estratégicos de modernização e padronização da infraestrutura tecnológica, fortalecimento da postura de segurança, manutenção da alta disponibilidade dos serviços de TI e garantia da continuidade dos serviços públicos essenciais ao cidadão, conforme estabelecido nos objetivos deste Termo de Referência.

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1. MODELO UTILIZADO PARA DESCRIÇÃO DOS PREÇOS

Conforme mapa de cotação e orçamentos em anexo. Para composição do preço de mercado em acordo com o Art. 23 da lei 14133/2021, realizou-se consulta com fornecedores que já atenderam ao município de forma satisfatório. A definição do preço de mercado foi realizada com base na média aritmética dos valores obtidos nas referidas fontes, conforme planilha detalhada em anexo, assegurando a razoabilidade dos custos estimados para o objeto licitado.

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1. DOTAÇÃO ORÇAMENTÁRIA

Órgão: 02 - Gabinete do Prefeito
Unidade: 05 - [Coordenadoria de Tecnologia de Informação e Comunicação]
Referência de Dotação: 153
MANUTENCAO DAS ATIVIDADES DAS SECRETARIAS E ORGAOS - Serviços de tecnologia da informação e comunicação - PJ

Órgão: 02 - Gabinete do Prefeito
Unidade: 05 - [Coordenadoria de Tecnologia de Informação e Comunicação]
Referência de Dotação: 130
MANUTENCAO DAS ATIVIDADES DAS SECRETARIAS E ORGAOS - Material Permanente

11. ESPECIFICAÇÃO DA GARANTIA

11.1. GARANTIA DO OBJETO

a) Licenças:

As licenças de Firewall de Próxima Geração (NGFW) terão validade de 36 (trinta e seis) meses, conforme especificado nos itens de licenças da descrição do objeto.

b) Equipamentos em Comodato (NGFW):

Os equipamentos de Firewall de Próxima Geração (NGFW) fornecidos em regime de comodato (item 1 da tabela do item 1.1) devem possuir garantia integral durante toda a vigência do contrato, ou seja, 36 (trinta e seis) meses, contados a partir da data de sua ativação. A garantia deve cobrir defeitos de fabricação, mal funcionamento e substituição de peças defeituosas. A CONTRATADA é responsável pela manutenção preventiva e corretiva, reposição em caso de falhas e garantia integral dos equipamentos durante toda a vigência do contrato.

c) Switches Core Adquiridos: Os Switches Core adquiridos deverão incluir uma licença de suporte técnico do fabricante, com vigência de 36 (trinta e seis) meses. Adicionalmente, a CONTRATADA será responsável por fornecer suporte técnico para estes equipamentos

durante toda a vigência do contrato de serviços, conforme detalhado no Anexo Técnico do Termo de Referência.

d) Serviços de Cibersegurança:

Os serviços de Cibersegurança para Firewall de Próxima Geração (NGFW), Plataforma SIEM, SOC (item 1 da tabela do item 1.1) devem ser prestados de forma contínua, 24x7 (24 horas por 7 dias da semana), durante toda a vigência do contrato de 36 (trinta e seis) meses, garantindo o cumprimento dos níveis de serviço estabelecidos.

e) Atualizações:

Durante o período de vigência das licenças de 36 (trinta e seis) meses, o FABRICANTE da solução deve fornecer todas as atualizações de software, patches de segurança e novas versões sem custo adicional para a CONTRATANTE, para NGFW, Switches Core e Plataforma SIEM (conforme aplicável e contratado).

f) Substituição:

Em caso de defeito nos equipamentos (NGFW em comodato ou Switches Core adquiridos) que não possa ser solucionado no prazo estabelecido para atendimento, a CONTRATADA deve acompanhar e auxiliar a CONTRATANTE no processo de RMA (Return Merchandise Authorization) junto ao fabricante.

12. GESTÃO

12.1. SECRETARIA / ÓRGÃO / RESPONSÁVEL

Coordenadoria de Tecnologia da Informação e Comunicação - CTEC. Rodrigo Golin Fernandes.

Bento Gonçalves, 16 de janeiro de 2026.

- assinado eletronicamente -
Rodrigo Golin Fernandes
Diretor

ANEXO I
Especificações Técnicas Obrigatórias

Este Anexo detalha as Especificações Técnicas Obrigatórias para os componentes que integram a solução de infraestrutura de rede e segurança a ser contratada pelo Município de Bento Gonçalves.

As diretrizes técnicas apresentadas neste documento aplicam-se aos seguintes elementos, os quais deverão ser fornecidos em regime de comodato ou implementados de acordo com o Termo de Referência:

- **Firewall de Próxima Geração (NGFW):** Abrangendo suas funcionalidades essenciais de segurança de rede, controle de aplicações, prevenção de ameaças, filtragem de conteúdo e conectividade avançada.
- **Gerenciamento Centralizado de Logs e Relatoria:** A solução dedicada à coleta, armazenamento, análise e geração de relatórios de eventos de segurança e rede.
- **Switches Core:** Os equipamentos de comutação de rede, incluindo suas capacidades de conectividade de alto desempenho, roteamento e segurança nas camadas 2 e 3.

Todos os equipamentos e soluções aqui especificados deverão atender integralmente aos requisitos mínimos de desempenho, funcionalidades, certificações e compatibilidade. A aderência a estas especificações é mandatório, e quaisquer substituições, alterações ou desvios não serão aceitos sem prévia e formal aprovação do Município de Bento Gonçalves.

1. FIREWALL DE PRÓXIMA GERAÇÃO (NGFW)

As diretrizes técnicas a seguir detalham os requisitos para o Firewall de Próxima Geração (NGFW), um componente central da solução a ser contratada em regime de comodato. Conforme o Termo de Referência e o Estudo Técnico Preliminar, este equipamento é fundamental para assegurar a proteção cibernética, a modernização da rede e a gestão proativa de eventos de segurança, abrangendo funcionalidades essenciais de controle de aplicações, prevenção de ameaças, filtragem de conteúdo e conectividade avançada. Para atender a esses objetivos, são exigidos os seguintes requisitos técnicos:

1.1. CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW)

1.1.1. Deve suportar, no mínimo, 37 (trinta e sete) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4;
1.1.2. Deve suportar, no mínimo, 10,5 (dez vírgula cinco) milhões de conexões simultâneas;
1.1.3. Deve suportar, no mínimo, 350.000 (trezentos e cinquenta mil) novas conexões por segundo;
1.1.4. Deve Suportar, no mínimo, 33 (trinta e três) Gbps de throughput VPN IPSec;
1.1.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 1.900 (mil e novecentos) túneis de VPN IPSEC Site-to-Site simultâneos;
1.1.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 14.000 (quatorze mil) túneis de clientes VPN IPSEC simultâneos;
1.1.7. Deve suportar, no mínimo, 2,7 (dois vírgula sete) Gbps de throughput de VPN SSL;

1.1.8. Deve suportar, no mínimo, 475 (quatrocentos e setenta e cinco) clientes de VPN SSL simultâneos;
1.1.9. Deve suportar, no mínimo, 8,5 (oito vírgula cinco) Gbps de throughput de IPS;
1.1.10. Deve suportar, no mínimo, 6,5 (seis vírgula cinco) Gbps de throughput de Inspeção SSL;
1.1.11. Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
1.1.12. Deve possuir, pelo menos, 4 (quatro) interfaces Gigabit Ethernet com conectores SFP;
1.1.13. Deve possuir, pelo menos, 8 (oito) interfaces 10 Gigabit Ethernet com conectores SFP+;
1.1.14. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;
1.1.15. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para Alta-Disponibilidade;
1.1.16. Deve possuir fonte de alimentação AC redundante;

1.2. CARACTERÍSTICAS GERAIS PARA OS EQUIPAMENTOS NGFW

1.2.1. O fabricante dos equipamentos de Firewall de Próxima Geração (NGFW) ofertados deverá estar posicionado no Quadrante Mágico do Gartner para 'Network Firewalls', conforme a edição mais recente publicada do ano 2025;
1.2.2. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source (produto montado);
1.2.3. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
1.2.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
1.2.5. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
1.2.6. Os dispositivos de proteção de rede devem possuir suporte a Vlans;
1.2.7. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
1.2.8. Deve suportar BGP, OSPF, RIP e roteamento estático;
1.2.9. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
1.2.10. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
1.2.11. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
1.2.12. Deve suportar ao menos 30 tabelas independentes de roteamento, por contexto de firewall;
1.2.13. Deve suportar NAT dinâmico (Many-to-Many);
1.2.14. Deve suportar NAT estático (1-to-1);
1.2.15. Deve suportar NAT estático bidirecional 1-to-1;
1.2.16. Deve suportar Tradução de porta (PAT);
1.2.17. Deve suportar NAT de Origem;
1.2.18. Deve suportar NAT de Destino;
1.2.19. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
1.2.20. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
1.2.21. Deve suportar NAT64;

1.2.22. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
1.2.23. Enviar log para sistemas de monitoração externos;
1.2.24. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
1.2.25. Proteção anti-spoofing;
1.2.26. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
1.2.27. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
1.2.28. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;
1.2.29. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
1.2.30. Controle, inspeção e decriptografia de SSL para tráfego de Saída (Outbound);
1.2.31. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;
1.2.32. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
1.2.33. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
1.2.34. A solução de firewall deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;
1.2.35. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
1.2.36. Deve possuir integração com soluções de NAC, para autenticação SSO no firewall de elementos registrados no NAC e execução de políticas de compliance na VPN;

1.3. POLÍTICAS

1.3.1. Deverá suportar controles por zonas de segurança;
1.3.2. Deverá suportar controles de políticas por porta e protocolo;
1.3.3. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
1.3.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
1.3.5. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
1.3.6. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
1.3.7. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
1.3.8. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
1.3.9. Suporte a objetos e regras IPV6;

1.3.10. Suporte a objetos e regras multicast;
1.3.11. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.4. CONTROLE DE APLICAÇÕES

1.4.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
1.4.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
1.4.3. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
1.4.4. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
1.4.5. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
1.4.6. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
1.4.7. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;
1.4.8. Identificar o uso de táticas evasivas via comunicações criptografadas;
1.4.9. Atualizar a base de assinaturas de aplicações automaticamente;
1.4.10. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
1.4.11. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
1.4.12. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
1.4.13. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
1.4.14. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
1.4.15. Deve alertar o usuário quando uma aplicação for bloqueada;
1.4.16. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

1.4.17. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
1.4.18. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, vendor e popularidade;
1.4.19. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
1.4.20. Deve permitir forçar o uso de portas específicas para determinadas aplicações;
1.4.21. Deve permitir o filtro de vídeos que podem ser visualizados no YouTube;

1.5. PREVENÇÃO DE AMEAÇAS

1.5.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

1.5.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
1.5.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
1.5.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;
1.5.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
1.5.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
1.5.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
1.5.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
1.5.9. Deve permitir o bloqueio de vulnerabilidades;
1.5.10. Deve permitir o bloqueio de exploits conhecidos;
1.5.11. Deve incluir proteção contra-ataques de negação de serviços;
1.5.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
1.5.13. Detectar e bloquear a origem de portscans;
1.5.14. Bloquear ataques efetuados por worms conhecidos;
1.5.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
1.5.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;
1.5.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
1.5.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

1.5.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
1.5.20. Identificar e bloquear comunicação com botnets;
1.5.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
1.5.22. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
1.5.23. Os eventos devem identificar o país de onde partiu a ameaça;
1.5.24. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
1.5.25. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
1.5.26. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
1.5.27. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;
1.5.28. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;
1.5.29. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;

1.6. FILTRO DE URLs

1.6.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.6.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
1.6.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
1.6.4. A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;
1.6.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
1.6.6. Possuir categorias de URLs previamente definidas pelo fabricante e atualizáveis a qualquer tempo;
1.6.7. Possuir pelo menos 60 categorias de URLs;
1.6.8. Deve possuir a função de exclusão de URLs do bloqueio;
1.6.9. Permitir a customização de página de bloqueio;

1.6.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

1.6.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

1.6.12. Os requisitos de filtro de URL descritos acima aplicam-se apenas ao firewall das pontas remotas

1.7. IDENTIFICAÇÃO DE USUÁRIOS

1.7.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

1.7.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

1.7.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

1.7.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

1.7.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

1.7.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

1.7.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

1.7.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

1.7.9. Deve suportar o envio e recebimento de credenciais via RADIUS;

1.8. FILTRO DE DADOS

1.8.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

1.8.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.8.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.8.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

1.9. GEOLOCALIZAÇÃO

1.9.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

1.9.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.10. VPN CLIENT TO SITE

1.10.1. Suportar IPSec VPN;

1.10.2. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

1.10.3. Atribuição de DNS nos clientes remotos de VPN, inclusive com DNS split tunnel;

1.10.4. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL;

1.10.5. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

1.10.6. Suportar leitura e verificação de CRL (certificate revocation list);

1.10.7. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

1.11. RECURSOS GERAIS DE SD-WAN

1.11.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

1.11.2. Deve ser possível criar políticas que definam os seguintes critérios para match:

1.11.2.1. Endereços de origem;

1.11.2.2. Grupos de usuários;

1.11.3. Endereços de destino;

1.11.4. DSCP;

1.11.5. Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox e etc);

1.11.6. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp;

1.11.7. O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente;

1.11.8. O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo (sessão) entre múltiplos links simultaneamente;

1.11.9. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

1.11.10.A solução de SD-WAN deve possibilitar o uso de túneis VPN dinâmicos, entre pontas remotas, para aplicações sensíveis. Uma vez que as pontas se trocam informações entre si, é feito by-pass do hub;

1.11.11.Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;

1.11.12.A solução deve permitir a definição do roteamento para cada aplicação;

1.11.13.Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;

1.11.14.Deve possibilitar a definição do link de saída para uma aplicação específica;

1.11.15.Deve implementar balanceamento de link por hash do IP de origem;

1.11.16.Deve implementar balanceamento de link por hash do IP de origem e destino;

1.11.17.Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

1.11.18.Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

1.11.19.A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;

1.11.20.Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF);

1.11.21.Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;

1.11.22.Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;

1.11.23.A solução de SD-WAN deve suportar nativamente conectores com clouds públicas. Pelo menos: Azure, AWS e GCP;

1.11.24.Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:1.11.21.1. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações e porta;

1.11.25.O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

1.11.26.O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc;

1.11.27.Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;

1.11.28.O QoS deve possibilitar a definição de fila de prioridade;

1.11.29.Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;

1.11.30. A capacidade de agendar intervalos de tempo em que as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;
1.11.31. Deve possibilitar a definição de bandas distintas para download e upload;
1.11.32. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);
1.11.33. A solução de SD-WAN deve suportar IPv6;
1.11.34. Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;
1.11.35. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
1.11.36. O SD-WAN deverá possuir serviço de Firewall Stateful;
1.11.37. A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;
1.11.38. A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site;
1.11.39. Deve ser capaz de bloquear acesso às aplicações;
1.11.40. Deve suportar NAT dinâmico bem como NAT de saída;
1.11.41. Deve suportar balanceamento de tráfego por sessão e pacote;
1.11.42. Suportar VPN IPSec Site-to-Site;
1.11.43. A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);
1.11.44. A VPN IPSEc deve suportar Autenticação MD5, SHA1. SHA256, SHA384 e SHA512;
1.11.45. A VPN IPSEc deve suportar Diffie-Hellman Group 1. Group 2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 32;
1.11.46. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
1.11.47. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;
1.11.48. Deve suportar o uso de DDNS, para casos onde uma ou ambas as pontas possuam IPs dinâmicos;
1.11.49. Deve suportar VPN dial up, no caso da ponta remota não possui IP estático na WAN;
1.11.50. Deve possuir suporte e estar licenciamento para uso de VRFs;
1.11.51. A solução de SD-WAN pode ser fornecida em composição com o firewall, desde que atenda aos mesmos requisitos de performance;

1.12. GERENCIAMENTO DE LOGS E RELATORIA CENTRALIZADO

Esta seção especifica os requisitos para a solução dedicada à coleta, armazenamento, análise e geração de relatórios de eventos de segurança e rede. Sua implementação visa elevar o nível de proteção cibernética do Município através de monitoramento centralizado de eventos em tempo real, detecção avançada de ameaças e conformidade regulatória. Para atender a esses objetivos, são exigidos os seguintes requisitos técnicos:

1.12.1. Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;
1.12.2. A solução deve suportar receber, no mínimo, 25 (cinco) GB de logs diários;
1.12.3. A solução de gerenciamento centralizado poderá ser ofertada em formato de appliance físico ou appliance virtual, e caso ofertado em formato virtual, será responsabilidade da

contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;

1.12.4. Caso a solução seja entregue em appliance virtual, deverá ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2012 / 2016/ 2019 e KVM no Redhat 7.1;
1.12.5. Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;
1.12.6. Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;
1.12.7. Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;
1.12.8. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;
1.12.9. A solução deverá ser capaz de armazenar logs por no mínimo 12 (doze) meses;
1.12.10. Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;
1.12.11. Possuir suporte para SNMP versão 2 e 3;
1.12.12. Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;
1.12.13. Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;
1.12.14. Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;
1.12.15. Suporte a autenticação de usuários de acesso à plataforma via LDAP, Radius ou TACACS+;
1.12.16. Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;
1.12.17. Deve permitir gerar alertas de eventos a partir de logs recebidos;
1.12.18. A solução deve ter relatórios predefinidos;
1.12.19. Permitir importação e exportação de relatórios;
1.12.20. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
1.12.21. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
1.12.22. Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
1.12.23. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
1.12.24. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;
1.12.25. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
1.12.26. Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;
1.12.27. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;
1.12.28. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

1.12.29.Deve possuir mecanismos de remoção automática para logs antigos;
1.12.30.Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;
1.12.31.Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
1.12.32.Permitir o envio por e-mail relatórios automaticamente;
1.12.33.Permitir que o relatório seja enviado por Email para o destinatário específico;
1.12.34.Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
1.12.35.Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
1.12.36.Deve permitir o uso de filtros nos relatórios;
1.12.37.Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
1.12.38.Permitir especificar o idioma dos relatórios criados;
1.12.39.Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
1.12.40.Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
1.12.41.Deve permitir o envio automático dos logs para um servidor FTP externo a solução;
1.12.42.Deve permitir exportar os logs no formato CSV;
1.12.43.Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
1.12.44.Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
1.12.45.Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;
1.12.46.Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
1.12.47.Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;
1.12.48.Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
1.12.49.Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
1.12.50.Deve permitir visualizar em tempo real os logs recebidos;
1.12.51.Deve permitir o encaminhamento de log no formato syslog e CEF (Common Event Format);
1.12.52.Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;
1.12.53.Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;
1.12.54.Deve possuir um painel de operações que monitore as principais ameaças à segurança da sua rede;

1.12.55. Deve possuir um painel de operações que monitora o envolvimento do usuário e o uso suspeito da web em sua rede;
1.12.56. Deve possuir um painel de operações que monitora o tráfego da rede, aplicativos e sites web;
1.12.57. Deve possuir um painel de operações que monitoram a atividade da VPN em sua rede;
1.12.58. Deve possuir um painel de operações que monitoram o desempenho dos recursos locais da solução (CPU, Memória);
1.12.59. Deve permitir a criação de painéis personalizados para monitorar operações de segurança e rede;
1.12.60. Deve possuir relatório de uso de aplicações e mídias sociais;
1.12.61. Deve possuir relatório de prevenção de perda de dados (DLP);
1.12.62. Deve possuir relatório de VPN, Prevenção de Intrusão (IPS), análise de ameaças cibernéticas;
1.12.63. Deve possuir relatório diário resumido de eventos e incidentes de segurança;
1.12.64. Deve possuir um relatório de tráfego DNS e e-mail;
1.12.65. Deve possuir relatório das 10 principais aplicações utilizadas na rede;
1.12.66. Deve possuir relatório dos 10 principais sites web utilizados na rede;
1.12.67. Deve possibilitar a visibilidade da utilização do balanceamento inteligente de links (SD-WAN), mostrando informações de utilização das regras por aplicação, largura de banda e níveis de serviços dos links (latência, Jitter e descarte de pacotes);
1.12.68. Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados, o monitoramento de computadores que estão potencialmente comprometidas ou usuários com uso de rede suspeito;
1.12.69. Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados pelos computadores, atribuição de pontuações de risco que definem os vereditos dos níveis de comprometimento como baixo, médio ou alto;
1.12.70. Deve suportar a análise detalhada dos computadores comprometidos e exibir os detalhes das ameaças detectadas;
1.12.71. Deve suportar recursos de automação (playbooks) que, por meio de integrações com soluções de firewall, endpoint, Email, ITSM e eventos pré-determinados, possa tomar ações automáticas visando mitigar riscos;
1.12.72. Deve permitir a correlação de eventos, provendo painéis diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança;

2. SWITCHES CORE

Esta seção detalha as especificações dos equipamentos de comutação de rede, os Switches Core, que serão adquiridos para modernizar a infraestrutura. Eles devem garantir conectividade de alto desempenho, roteamento e segurança nas camadas 2 e 3, integrando-se plenamente com o Firewall de Próxima Geração para otimizar o funcionamento da rede e aplicar políticas de segurança unificadas. Para atender a esses objetivos, são exigidos os seguintes requisitos técnicos:

2.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

2.2. Deve possuir 48 (quarenta e oito) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE;
2.3. Adicionalmente, deve possuir 4 (quatro) slots QSFP28 para conexão de fibras ópticas operando com velocidades de 40 e 100 Gigabit Ethernet;
2.4. Deve permitir a configuração das interfaces QSFP28 para que operem com conexões do tipo "breakout" ou "split", modo em que uma determinada porta 40GbE pode operar com 4 conexões em 10GbE. Deve permitir ainda que as portas 100GbE sejam divididas em 4 conexões de 25GbE;
2.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
2.6. Deve possuir interface dedicada para gerenciamento local do tipo "out-of-band". Esta interface de gerenciamento deverá possuir porta 1000Base-T com conector RJ-45;
2.7. Deve possuir 1 (uma) interface USB;
2.8. Deve possuir capacidade de comutação de pelo menos 1.76 Tbps (terabits por segundo) e ser capaz de encaminhar até 1.5 Bpps (bilhões de pacotes por segundo);
2.9. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
2.10. Deve suportar Q-in-Q, recurso também conhecido como Stacked VLAN ou VLAN sobre VLAN em que é possível configurar duas TAGs de VLAN no mesmo frame;
2.11. Deve possuir tabela MAC com suporte a 144.000 endereços;
2.12. Deve operar com latência igual ou inferior à 1us (microsegundo);
2.13. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
2.14. Em conjunto com o Flow Control (IEEE 802.3x) o switch deverá, ao invés de enviar pause frames, definir um limite de banda que poderá ser recebida na interface quando o buffer estiver cheio. O switch deverá medir o volume de utilização do buffer para que o recebimento seja restaurado à capacidade máxima automaticamente;
2.15. Deve suportar o padrão IEEE 802.1Qbb (Priority-based Flow Control);
2.16. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);
2.17. Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica;
2.18. Deve suportar a comutação de Jumbo Frames;
2.19. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
2.20. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
2.21. Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIP, BGP, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação dos protocolos;
2.22. Deve possuir hardware capaz de suportar roteamento multicast através do protocolo PIM-SSM (Protocol Independent Multicast - Source-Specific Multicast). É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação dos protocolos;

2.23. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação do protocolo;

2.24. Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação do protocolo;

2.25. Deve ser capaz de criar múltiplas tabelas de roteamento através de VRF (Virtual Routing and Forwarding). É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação deste recurso;

2.26. Deve implementar serviço de DHCP Server e DHCP Relay;

2.27. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos;

2.28. Deve suportar MLD (Multicast Listener Discovery) Snooping para otimizar a transmissão de tráfego multicast em IPv6;

2.29. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN);

2.30. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN;

2.31. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 30 (trinta) instâncias de Multiple Spanning Tree;

2.32. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status “Forwarding” do Spanning Tree após sua conexão física;

2.33. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

2.34. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

2.35. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

2.36. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

2.37. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

2.38. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

2.39. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

2.40. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

2.41. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;

2.42. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ);

2.43. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

2.44. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;

2.45. Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement;

2.46. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

2.47. Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

2.48. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

2.49. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

2.50. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

2.51. Deve suportar MAC Authentication Bypass (MAB);

2.52. Deve implementar RADIUS CoA (Change of Authorization);

2.53. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

2.54. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

2.55. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

2.56. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

2.57. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

2.58. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

2.59. Deve suportar o protocolo PTP (Precision Time Protocol);

2.60. Deve implementar Netflow, sFlow ou similar;

2.61. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

2.62. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1. v2c e v3;

2.63. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

2.64. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
2.65. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
2.66. Deve permitir ser gerenciado através de IPv6;
2.67. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
2.68. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
2.69. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
2.70. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
2.71. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
2.72. Deverá suportar ser configurado e monitorado através de REST API;
2.73. Deve possuir ferramenta para captura de pacotes que auxiliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark;
2.74. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash;
2.75. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
2.76. Deve suportar temperatura de operação de até 40º Celsius;
2.77. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
2.78. Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V;
2.79. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;