TERMO DE REFERÊNCIA

Município de Rio dos Índios/RS

Secretaria Municipal de Administração

Necessidade: Contratação de empresa especializada para prestação de Serviços Gerenciados de Cibersegurança destinados à proteção da infraestrutura tecnológica do Município de Rio dos Índios/RS.

1. DEFINIÇÃO DO OBJETO

1.1. Constitui objeto da presente contratação a prestação de Serviços Gerenciados de Cibersegurança, destinados à proteção da infraestrutura tecnológica do Município de Rio dos Índios/RS, compreendendo o fornecimento, em regime de comodato, de solução de Firewall de Próxima Geração (Next Generation Firewall – NGFW), acompanhado do respectivo licenciamento durante toda a vigência contratual, bem como o fornecimento de até 60 (sessenta) licenças de solução corporativa de proteção de endpoints, destinadas aos equipamentos localizados no Centro Administrativo, Secretarias Municipais, Unidade de Saúde, CRAS, Biblioteca Municipal, Museu Municipal e demais prédios, unidades ou setores integrantes da infraestrutura tecnológica municipal.

1.2. A contratação compreende, ainda, todos os serviços necessários para implantação, configuração, gerenciamento, monitoramento, atualização, manutenção e suporte técnico especializado da solução de segurança da informação, incluindo:

- fornecimento, em regime de comodato, de equipamento Firewall de Próxima Geração;
- instalação e configuração do firewall;
- fornecimento e manutenção do licenciamento do firewall durante toda a vigência contratual;
- instalação, configuração e ativação da solução corporativa de proteção de endpoints, contemplando recursos de prevenção, detecção e resposta a ameaças – NGAV/EDR, em até 60 computadores da Administração Municipal;
- definição e implementação das políticas de segurança da rede;
- migração das configurações existentes, quando necessária;
- gerenciamento integral da solução de segurança;
- monitoramento contínuo da infraestrutura tecnológica, durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

- detecção, análise e resposta a incidentes de segurança;
- atualização permanente das assinaturas de segurança, mecanismos de proteção e versões dos softwares utilizados;
- emissão de relatórios técnicos periódicos contendo informações sobre eventos de segurança, vulnerabilidades identificadas, incidentes registrados e ações corretivas executadas;
- suporte técnico especializado para atendimento das demandas relacionadas à solução contratada;
- manutenção preventiva, corretiva e evolutiva da solução durante toda a vigência contratual;
- monitoramento e proteção da infraestrutura tecnológica municipal abrangida pela solução, compreendendo os ativos, dispositivos, conexões e unidades integrantes ou interligadas à rede corporativa do Município.

1.3. Todos os equipamentos, licenças, softwares e demais recursos necessários ao perfeito funcionamento da solução deverão ser fornecidos pela contratada, permanecendo sob sua responsabilidade técnica durante toda a execução contratual.

1.4. O objeto será executado de acordo com os itens, etapas e quantitativos constantes da tabela abaixo, observadas as especificações técnicas mínimas estabelecidas no Anexo I deste Termo de Referência:

Item	Qtd.	Unid.	Especificação	Valor unitário Referência	Valor total Referência
1	**01**	Serviço	**Implantação da solução**, compreendendo: a) instalação e configuração da solução de Firewall de Próxima Geração – NGFW no Centro Administrativo; b) instalação, configuração e ativação da solução de proteção de endpoints em até 60 computadores da Administração Municipal; e c) instalação, configuração e habilitação da solução de gerenciamento unificado e de geração de relatórios em nuvem.	R$ 11.600,00	R$ 11.600,00

2	**12**	Mês	**Prestação continuada de Serviços Gerenciados de Cibersegurança**, compreendendo: a) disponibilização, em regime de comodato, de 01 equipamento de Firewall de Próxima Geração, com os respectivos licenciamentos; b) disponibilização de até 60 licenças da solução de proteção de endpoints; c) disponibilização da solução de gerenciamento unificado e relatórios em nuvem, com retenção mínima de dados pelo período de 01 ano; d) suporte técnico especializado; e) monitoramento contínuo 24 horas por dia, 7 dias por semana; f) detecção e resposta a incidentes de segurança; e g) análise e apresentação de relatórios para melhoria contínua da segurança.	R$ 4.000,00	R$ 48.000,00
Valor Global estimado, para o período inicial de 12 meses:					**R$ 59.600,00**

1.5. O valor total estimado do contrato para o período inicial de 12 (doze) meses será de R$ 59.600,00 (cinquenta e nove mil e seiscentos reais).

1.6. O valor relativo aos serviços de implantação, item 01 da tabela acima, não poderá ser superior a 20% (vinte por cento) do total do contrato inicial.

1.7. Os serviços relativos à implantação (item 01) serão executados e pagos uma única vez, após a sua conclusão, correção das inconsistências eventualmente identificadas e recebimento definitivo pela fiscalização.

1.8. Os serviços relativos ao item 02 serão executados de forma continuada, sendo pago mensalmente, durante o período inicial de 12 meses e nas eventuais prorrogações.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. A presente contratação se fundamenta na necessidade de fortalecimento da segurança da infraestrutura tecnológica utilizada pela Administração Pública Municipal, considerando que praticamente todas as atividades administrativas atualmente dependem de sistemas informatizados para execução dos serviços públicos.

2.2. O Município utiliza recursos tecnológicos para processamento de informações administrativas, financeiras, tributárias, patrimoniais, contábeis, recursos humanos, saúde, educação, assistência social e demais áreas essenciais ao funcionamento da Administração Pública. A indisponibilidade desses sistemas, bem como eventual comprometimento da integridade ou confidencialidade das informações, pode ocasionar prejuízos significativos à continuidade dos serviços públicos e ao atendimento da população.

2.3. A infraestrutura tecnológica municipal encontra-se distribuída entre o Centro Administrativo e diversas unidades públicas, incluindo Secretarias Municipais, Unidade de Saúde, CRAS, Biblioteca Municipal, Museu Municipal e demais prédios e setores integrantes da Administração, havendo necessidade de proteção coordenada dos ativos tecnológicos e das informações que transitam ou são processadas nesses ambientes.

2.4. Nos últimos anos é observado um crescimento significativo dos ataques cibernéticos direcionados aos órgãos públicos, incluindo tentativas de invasão, disseminação de programas maliciosos, sequestro de dados, vazamento de informações e demais incidentes capazes de comprometer a infraestrutura tecnológica das instituições públicas.

2.5. Além da necessidade de assegurar a continuidade dos serviços públicos, a contratação busca atender às boas práticas de governança em tecnologia da informação e fortalecer os mecanismos de proteção dos dados tratados pela Administração Municipal, em conformidade com a Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD).

2.6. A contratação de Serviços Gerenciados de Cibersegurança é considerada a alternativa mais vantajosa para o Município, tendo em vista a atuação coordenada de uma empresa especializada e com experiência na área e atuação objetiva, sendo esta responsável pela implantação, gerenciamento, monitoramento e manutenção da solução, dispensando investimentos elevados na aquisição de equipamentos próprios e reduzindo a necessidade de estrutura técnica interna altamente especializada.

2.7. A solução contempla não apenas o fornecimento do equipamento firewall e das licenças de antivírus, mas também o gerenciamento contínuo da segurança da infraestrutura tecnológica, monitoramento permanente, resposta a incidentes, atualização tecnológica e suporte especializado, garantindo maior disponibilidade dos serviços públicos, redução dos riscos operacionais e aumento da segurança das informações institucionais.

2.8. A contratação será realizada mediante Dispensa de Licitação, nos termos do art. 75, inciso II, da Lei Federal nº 14.133/2021, considerando que o valor estimado da contratação se enquadra no limite legal para contratação direta e que a solução pretendida possui ampla disponibilidade no mercado especializado.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

3.1. A solução consiste na contratação de empresa especializada para fornecimento de Serviços Gerenciados de Cibersegurança, compreendendo a disponibilização, em regime de comodato, de equipamento Firewall de Próxima Geração, acompanhado do respectivo licenciamento, bem como a disponibilização de até 60 (sessenta) licenças de solução de proteção de endpoints – NGAV/EDR, para proteção dos computadores da Administração Municipal.

3.2. A execução dos serviços compreenderá duas etapas distintas:

a) A primeira corresponde à implantação da solução, incluindo a instalação física e lógica do firewall, configuração das políticas de segurança da rede, instalação e configuração da solução de proteção de endpoints – NGAV/EDR, em até 60 computadores, realização dos testes necessários e homologação da solução.

b) A segunda corresponde à prestação continuada dos Serviços Gerenciados de Cibersegurança durante toda a vigência contratual, abrangendo o gerenciamento da solução, monitoramento contínuo da infraestrutura tecnológica, atualização dos mecanismos de proteção, identificação preventiva de vulnerabilidades, detecção de incidentes de segurança, resposta técnica aos eventos identificados, emissão de relatórios periódicos e suporte técnico especializado.

3.3. A solução deverá permanecer em pleno funcionamento durante toda a execução contratual, assegurando elevados níveis de disponibilidade, proteção da infraestrutura tecnológica, continuidade dos serviços públicos e redução dos riscos relacionados à segurança da informação.

3.4. A opção pela contratação integrada busca racionalizar a gestão contratual, concentrando em uma única empresa a responsabilidade pelo fornecimento dos equipamentos, licenciamento, implantação, monitoramento, gerenciamento e suporte técnico, reduzindo riscos operacionais e proporcionando maior eficiência administrativa.

3.5. Os acessos administrativos realizados pela equipe técnica da CONTRATADA deverão ser controlados e auditáveis, mediante utilização de solução de Gerenciamento de Acessos Privilegiados – PAM, ou mecanismo tecnicamente equivalente, conforme requisitos estabelecidos no Anexo I.

4. REQUISITOS DA CONTRATAÇÃO

4.1. O objeto contratual possui natureza de serviço comum, nos termos do art. 6º, inciso XIII, da Lei Federal nº 14.133/2021, uma vez que seus padrões de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais de mercado.

4.2. A contratação será realizada mediante Dispensa de Licitação, com fundamento no art. 75, inciso II, da Lei Federal nº 14.133/2021, considerando que o valor estimado se enquadra no limite legal para contratação direta.

4.3. A empresa contratada deverá fornecer todos os equipamentos, softwares, licenças, mão de obra especializada, ferramentas e demais recursos necessários para implantação, gerenciamento e manutenção da solução durante toda a vigência contratual.

4.4. **Da subcontratação:**

a) Não será permitida a subcontratação integral do objeto.

b) Excepcionalmente, poderá ser admitida a subcontratação parcial de atividades acessórias, desde que previamente autorizada pela Administração, permanecendo a contratada como única responsável pela perfeita execução contratual.

4.5. **Condições de execução:**

a) A execução dos serviços deverá observar integralmente as condições estabelecidas neste Termo de Referência, no Estudo Técnico Preliminar e demais documentos que integram o processo administrativo.

b) Os serviços deverão ser executados por profissionais qualificados, observando as boas práticas de Segurança da Informação, as recomendações dos fabricantes das soluções ofertadas e a legislação aplicável.

c) A contratada deverá manter, durante toda a vigência contratual, no mínimo, 02 (dois) profissionais certificados pelo fabricante da solução ofertada e aptos a realizar sua implantação, configuração, gerenciamento, monitoramento e suporte.

d) Os profissionais indicados para comprovação da qualificação técnica deverão participar efetivamente da execução dos serviços, admitida sua substituição por profissional que possua qualificação equivalente ou superior, mediante prévia comunicação e aprovação da Administração.

e) A substituição ou o afastamento de um dos profissionais não poderá ocasionar interrupção, redução da qualidade ou descumprimento dos níveis mínimos de atendimento.

f) A Administração poderá solicitar, mediante justificativa, a substituição de profissional cuja atuação não atenda às exigências técnicas, de segurança, confidencialidade ou desempenho estabelecidas no contrato.

g) A contratada será integralmente responsável pela implantação, configuração, gerenciamento, monitoramento, manutenção e suporte da solução, respondendo pela qualidade dos serviços executados.

h) A implantação compreenderá, no mínimo:

- instalação física e lógica do Firewall de Próxima Geração;
- configuração inicial do equipamento;
- definição das políticas de segurança;
- migração das regras existentes, quando aplicável;
- configuração de redes privadas virtuais (VPN), utilizadas pelo Município;
- instalação e configuração da solução de proteção de endpoints – NGAV/EDR, em até 60 computadores da Administração Municipal;
- realização de testes operacionais;
- homologação da solução juntamente com o fiscal do contrato.

i) Concluída a implantação, iniciar-se-á a fase de prestação continuada dos serviços.

j) A CONTRATADA deverá assegurar a continuidade operacional da solução durante toda a vigência contratual, adotando imediatamente medidas de contingência em caso de falha do equipamento Firewall ou de qualquer componente crítico da solução.

4.6. **Normativas legais que o serviço deve seguir:**

4.6.1. A solução deverá observar, sempre que aplicáveis:

- Lei Federal nº 14.133/2021;
- Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD);
- Marco Civil da Internet (Lei nº 12.965/2014);
- normas técnicas dos fabricantes das soluções fornecidas;
- boas práticas internacionais de Segurança da Informação;
- recomendações do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), quando aplicáveis.

4.7. **Proteção de dados, confidencialidade e segurança da informação**

4.7.1. A CONTRATADA deverá observar integralmente a Lei Federal nº 13.709/2018 – LGPD e demais normas aplicáveis à proteção de dados pessoais e à segurança da informação.

4.7.2. Os dados, informações, registros, credenciais e demais conteúdos acessados em razão da execução contratual somente poderão ser utilizados para as finalidades estritamente necessárias à prestação dos serviços.

4.7.3. A CONTRATADA deverá assegurar que seus profissionais mantenham absoluto sigilo sobre as informações acessadas durante a execução contratual, inclusive após o encerramento do contrato.

4.7.4. É vedada a utilização, reprodução, compartilhamento, transferência ou armazenamento de informações da Administração para finalidade diversa da execução contratual.

4.7.5. Qualquer incidente de segurança que envolva ou possa envolver dados, informações ou sistemas do Município deverá ser comunicado imediatamente à fiscalização contratual, acompanhado das informações disponíveis acerca da natureza do incidente, ativos afetados, medidas de contenção adotadas e providências recomendadas.

4.7.6. A CONTRATADA deverá cooperar com a Administração na apuração de incidentes, preservação de evidências, elaboração de relatórios e adoção das providências necessárias.

4.7.7. Os acessos administrativos realizados pela CONTRATADA deverão observar as exigências relativas ao Gerenciamento de Acessos Privilegiados – PAM previstas no Anexo I.

4.7.8. Encerrada a contratação, a CONTRATADA deverá promover, quando aplicável, a devolução, eliminação ou inutilização segura das credenciais, cópias e informações mantidas exclusivamente para execução do contrato, ressalvadas as hipóteses legais de conservação

4.8. **Local da execução:**

a) Os serviços serão executados no Centro Administrativo e nas demais unidades integrantes da infraestrutura tecnológica municipal, incluindo Secretarias Municipais, Unidade de Saúde, CRAS, Biblioteca Municipal, Museu Municipal e demais prédios, unidades ou setores pertencentes à Administração que estejam abrangidos pela rede ou pela solução contratada.
b) A instalação do firewall ocorrerá no rack de TI, localizado no Centro Administrativo, ou outro ambiente definido pela Administração Municipal.
c) As licenças da solução de proteção de endpoints – NGAV/EDR, serão instaladas em até 60 computadores pertencentes ao Município.
d) Durante a vigência do contrato, a Administração poderá solicitar a transferência das licenças entre equipamentos, conforme indicação da fiscalização contratual, desde que respeitado o quantitativo contratado.
e) A solução deverá considerar a arquitetura de conectividade existente entre as unidades municipais, cabendo à CONTRATADA realizar as configurações necessárias para proteção dos ativos e do tráfego efetivamente abrangidos pela solução.
f) As informações técnicas detalhadas da infraestrutura, inclusive aquelas cuja divulgação possa comprometer a segurança da rede, serão disponibilizadas à CONTRATADA apenas na medida necessária à implantação e execução dos serviços.

4.9. **Requisitos Mínimos da Solução:**

4.9.1. A solução deverá compreender, obrigatoriamente:

Firewall

A contratada deverá disponibilizar Firewall de Próxima Geração em regime de comodato, acompanhado do respectivo licenciamento durante toda a vigência contratual.

A solução deverá contemplar, no mínimo:

- inspeção inteligente do tráfego de rede;
- sistema de prevenção contra intrusões;
- controle de aplicações;
- filtro de navegação na internet;
- proteção contra programas maliciosos;
- atualização automática das assinaturas de segurança;
- criação da(s) rede(s) privada(s) virtual(is) (VPN) necessária(s);
- gerenciamento centralizado;
- registros de eventos de segurança;
- geração de relatórios;
- atualização permanente do firmware;
- substituição do equipamento em caso de falha ou defeito que impeça ou comprometa substancialmente seu funcionamento, devendo a CONTRATADA adotar imediatamente solução de contingência e providenciar o restabelecimento da operação dentro dos níveis de serviço estabelecidos neste Termo de Referência, sem custos adicionais ao Município.

Solução de proteção de endpoints – NGAV/EDR

A solução deverá disponibilizar até 60 licenças corporativas.

A solução deverá possuir, no mínimo:

- gerenciamento centralizado;
- proteção em tempo real;
- atualização automática;
- proteção contra vírus, trojans, worms, spyware, ransomware e demais códigos maliciosos;
- quarentena automática;
- bloqueio de arquivos suspeitos;
- varreduras programadas;
- geração de relatórios;
- painel de gerenciamento.

Monitoramento

A contratada deverá realizar monitoramento contínuo da infraestrutura protegida, compreendendo 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, visando identificar comportamentos anômalos, tentativas de invasão, indisponibilidade dos serviços e demais eventos relevantes de segurança.

O monitoramento deverá possibilitar a identificação precoce de incidentes, permitindo a adoção de medidas preventivas e corretivas para minimizar impactos ao ambiente tecnológico da Administração.

Detecção e resposta a incidentes

A contratada deverá manter estrutura técnica apta a detectar, analisar e responder a incidentes de segurança relacionados à solução contratada.

Sempre que identificado evento que represente risco à infraestrutura tecnológica, a contratada deverá adotar as medidas técnicas cabíveis para contenção, mitigação e restabelecimento da normalidade, comunicando formalmente a Administração quanto à ocorrência, às providências adotadas e às recomendações para evitar recorrências.

4.10. **Suporte técnico:**

a) A contratada deverá disponibilizar suporte técnico especializado durante toda a vigência contratual.
b) O atendimento deverá ocorrer, prioritariamente, durante o horário de expediente da Administração Municipal, sem prejuízo da atuação contínua do monitoramento da solução.
c) O suporte poderá ser realizado por acesso remoto ou presencialmente, sempre que necessário para solução da ocorrência.

4.11. **Níveis mínimos de atendimento:**

4.11.1. Os chamados deverão observar, no mínimo, os seguintes prazos:

Classificação	**Atendimento inicial**	**Contenção, restabelecimento**
Crítica (paralisação total dos serviços ou incidente grave de segurança)	até 30 minutos	até 4 horas
Alta	até 2 horas	até 8 horas
Média	até 4 horas	até 2 dias úteis
Baixa	até 1 dia útil	até 5 dias úteis

4.11.2. Caso a solução definitiva demande prazo superior, a contratada deverá apresentar solução alternativa que mantenha a continuidade dos serviços.

4.11.3. Nos incidentes críticos, quando a solução definitiva demandar prazo superior ao estabelecido, a CONTRATADA deverá implementar medida de contenção, contingência ou solução provisória capaz de restabelecer a continuidade dos serviços, sem prejuízo da adoção das providências necessárias à solução definitiva.

4.11.4. Os prazos de atendimento deverão ser registrados e demonstrados nos relatórios mensais, sendo eventuais descumprimentos injustificados considerados para fins de avaliação da execução contratual e aplicação das medidas previstas no contrato.

4.11.5. Em caso de falha do equipamento Firewall que impeça o funcionamento normal da rede protegida, a ocorrência será classificada como crítica.

4.12. **Atualizações:**

4.12.1. Durante toda a vigência contratual, caberá à contratada:

- manter atualizadas todas as assinaturas de segurança;
- manter atualizado o firmware do firewall;
- atualizar o sistema solução de proteção de endpoints sempre que houver novas versões do fabricante;
- corrigir vulnerabilidades identificadas na solução contratada;
- manter vigente todo o licenciamento da solução.

5. FORMA E CRITÉRIOS DE SELEÇÃO DO PRESTADOR DE SERVIÇO

A contratação será realizada mediante Dispensa de Licitação, observadas as disposições da Lei Federal nº 14.133/2021.

5.1. **Critério de Julgamento da Proposta apresentada**

A licitante deverá apresentar separadamente:

I – o valor da Implantação da Solução (item 01);

II – o valor mensal e o valor total para o período de 12 meses, correspondente ao Serviços Gerenciados de Cibersegurança (item 02);

III – o valor global.

O critério de julgamento será o de menor preço mensal, considerando-se, para fins de classificação das propostas, o valor mensal ofertado para o Serviços Gerenciados de Cibersegurança (item 02).

O valor da Implantação da Solução (item 01) não poderá ser superior 20% (vinte por cento) do valor global.

Caso o valor do item 01 ultrapasse o limite estabelecido, a licitante será convocada para adequar a proposta, sem majoração do valor mensal ofertado para o item 02. A ausência de adequação implicará a desclassificação da proposta.

A adoção do menor preço mensal é justificada pela predominância econômica e funcional do item 02, que corresponde à prestação continuada e poderá ser objeto de sucessivas prorrogações, enquanto o item 01 possui natureza acessória, inicial e não recorrente.

5.2. **Forma de Habilitação da empresa vencedora**

A empresa deverá apresentar documentação de habilitação jurídica, fiscal, trabalhista, econômico-financeira e técnica, nos termos da Lei Federal nº 14.133/2021.

5.2.1. **Habilitação jurídica**

5.2.1.1. Documento de constituição da empresa, podendo ser:

i. ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos deeleição de seus administradores; ou

ii. inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício; ou

iii. decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

5.2.2. **Habilitação Fiscal e trabalhista:**

i. Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ);

ii. Prova de inscrição no cadastro de contribuintes estadual ou municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

iii. Prova de regularidade para com a União, Fazenda Federal, Estadual e Municipal da sede do licitante, através de certidões expedidas pelos órgãos competentes, que estejam dentro do prazo de validade, expresso na própria certidão ou, na hipótese de não trazerem o prazo de validade, que sejam expedidas há, no máximo, 90 dias.

iv. Prova de situação regular perante o Fundo de Garantia por Tempo de Serviço (FGTS),

v. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa.

vi. Declaração de não empregar menor, salvo em condição de aprendiz

vii. Declaração de que não possui, direta ou indiretamente, sócio(s) ou empregado(s) que sejam servidores do Poder Executivo do Município.

5.2.3. **Habilitação econômico-financeira**

a) Certidão negativa de falência ou concordata expedida pelo distribuidor da sede da pessoa jurídica, em prazo não superior a noventa (90) dias da data da apresentação do documento.

Serão aceitas certidões positivas com efeitos de negativas, na forma da legislação pertinente.

As certidões deverão estar vigentes na data de sua apresentação. Quando o documento não estabelecer expressamente seu prazo de validade, serão aceitas certidões emitidas nos 90 dias anteriores à data de apresentação, salvo se houver prazo diverso previsto em lei ou regulamento específico.

Havendo restrição na comprovação da regularidade fiscal ou trabalhista de microempresa ou empresa de pequeno porte, será assegurado o prazo legal para regularização, na forma dos arts. 42 e 43 da Lei Complementar Federal nº 123/2006.

5.2.4. **Qualificação técnica**

A licitante deverá comprovar que possui qualificação técnica compatível com a execução do objeto mediante apresentação dos seguintes documentos:

a) um ou mais atestados de capacidade técnica, emitidos por pessoa jurídica de direito público ou privado, comprovando que a licitante executou satisfatoriamente serviços compatíveis com o objeto, especialmente serviços relacionados à implantação, configuração, gerenciamento ou monitoramento de firewall de próxima geração, proteção de endpoints, monitoramento de segurança ou resposta a incidentes cibernéticos;

b) comprovação da disponibilidade de, no mínimo, 02 (dois) profissionais que possuam certificação técnica válida emitida pelo fabricante da solução ofertada, aptos a realizar sua implantação, configuração, gerenciamento, monitoramento e suporte;

c) documentação comprobatória das certificações técnicas dos profissionais indicados;

d) comprovação do vínculo ou da disponibilidade dos profissionais indicados, mediante apresentação de um dos seguintes documentos:

i. Carteira de Trabalho e Previdência Social ou registro funcional, no caso de empregado;

ii. contrato de prestação de serviços;

iii. ato constitutivo da empresa, quando se tratar de sócio ou titular; ou

iv. Declaração de compromisso de vinculação profissional, acompanhada da anuência do respectivo profissional, ficando a formalização do vínculo condicionada à assinatura do contrato;

e) declaração de que dispõe de equipe técnica, equipamentos, ferramentas e estrutura operacional suficientes para a implantação e prestação continuada dos serviços;

f) catálogo, ficha técnica, manual ou documentação oficial do fabricante que demonstre o atendimento das especificações técnicas mínimas estabelecidas no Anexo I deste Termo de Referência; e

g) comprovação de que os equipamentos, sistemas e licenciamentos ofertados possuirão garantia, atualização e suporte técnico durante toda a vigência contratual.

A apresentação de mais de um atestado será admitida para comprovação conjunta da experiência exigida, desde que os documentos demonstrem a execução de serviços pertinentes e compatíveis com o objeto.

A exigência de disponibilidade de, no mínimo, 02 (dois) profissionais certificados pelo fabricante da solução justifica-se pela natureza contínua e crítica dos serviços de cibersegurança, que envolvem monitoramento, prevenção e resposta a incidentes capazes de comprometer a infraestrutura tecnológica e a continuidade dos serviços públicos municipais.

A manutenção de dois profissionais visa assegurar a continuidade do atendimento e evitar que a execução dos serviços fique comprometida em razão da indisponibilidade temporária de um único técnico, inclusive por motivo de férias, afastamento por saúde, folga, treinamento, atendimento simultâneo a outro cliente ou qualquer outra ocorrência que impeça sua atuação imediata.

5.2.5. **Prova de Conceito**

A Administração exigirá da licitante provisoriamente classificada em primeiro lugar a realização de Prova de Conceito da solução ofertada, destinada a verificar o atendimento às especificações técnicas mínimas previstas neste Termo de Referência, especialmente quanto às funcionalidades do Firewall de Próxima Geração (NGFW), da solução de proteção de endpoints – NGAV/EDR, do gerenciamento centralizado, do monitoramento e dos recursos de segurança exigidos.

A Prova de Conceito será realizada exclusivamente pelo licitante provisoriamente mais bem classificado, após a análise da documentação de habilitação e antes da adjudicação do objeto.

A convocação para realização da Prova de Conceito será efetuada pela Administração, devendo a solução ser disponibilizada no prazo máximo de 07 (sete) dias corridos, contados do recebimento da convocação, sem qualquer ônus para o Município.

A empresa deverá disponibilizar todos os equipamentos, softwares, licenças, ambiente de demonstração, acesso remoto, documentação técnica e demais recursos necessários à realização dos testes, bem como fornecer os respectivos manuais em língua portuguesa, excepcionalmente algum material poderá ser aceito em língua inglesa.

A Prova de Conceito será conduzida pela equipe técnica designada pela Administração, podendo ser acompanhada pelos demais licitantes interessados, desde que previamente identificados.

Durante a Prova de Conceito poderão ser verificados, entre outros aspectos:

- atendimento às especificações técnicas constantes do Anexo I;
- funcionamento das funcionalidades mínimas do firewall;
- gerenciamento centralizado;
- criação e gerenciamento de políticas de segurança;
- controle de aplicações;
- prevenção contra intrusões (IPS);
- geração de relatórios;
- funcionamento do sistema de proteção de endpoints – NGAV/EDR;
- monitoramento da solução;
- capacidade de administração e gerenciamento;
- demais funcionalidades previstas neste Termo de Referência.

Ao término da Prova de Conceito, a equipe técnica emitirá parecer conclusivo, classificando a solução como:

I – APROVADA: quando demonstrado o atendimento integral das especificações técnicas mínimas previstas neste Termo de Referência;

II – REPROVADA: quando constatado o não atendimento de qualquer requisito técnico considerado obrigatório.

A Prova de Conceito será realizada de acordo com roteiro previamente definido pela Administração, contendo os requisitos técnicos que serão objeto de demonstração, a forma de realização dos testes e os critérios objetivos de aprovação.

A ausência injustificada da licitante ou a não disponibilização da solução no prazo estabelecido será considerada desistência da proposta, ensejando sua desclassificação.

A reprovação na Prova de Conceito implicará a desclassificação da proposta, sem direito a qualquer indenização, sendo convocado o licitante remanescente, observada a ordem de classificação, para apresentação da documentação de habilitação e, se necessário, realização de nova Prova de Conceito.

6. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Estima-se para a contratação o valor global de R$ 59.600,00 (cinquenta e nove mil e seiscentos reais).

O valor estimado foi obtido mediante pesquisa de preços realizada junto a fornecedores especializados, observando-se as disposições do art. 23 da Lei Federal nº 14.133/2021 e do Decreto Municipal nº 014/2024.

7. ADEQUAÇÃO ORÇAMENTÁRIA

O dispêndio financeiro decorrente da contratação ora pretendida decorrerá da dotação orçamentária:

03.01	**SECRETARIA DE ADMINISTRAÇÃO**
2002	**MANUTENÇÃO SECRET. ADMINISTRAÇÃO**
33.90.40.00.00.000	**SERV TEC DA INFO E COMUNICAÇÃO - PJ**

8. VIGÊNCIA E PRORROGAÇÃO

8.1. O prazo de vigência da contratação será de 12 (doze) meses, contados da assinatura do contrato, podendo ser prorrogado sucessivamente, na forma dos arts. 106 e 107 da Lei Federal nº 14.133/2021, desde que demonstrada a vantajosidade para a Administração, mantidas as condições contratuais e observada a disponibilidade orçamentária.

8.2. Nas eventuais prorrogações contratuais, será prorrogado exclusivamente o item 02, correspondente aos Serviços Gerenciados de Cibersegurança, permanecendo o pagamento pelo valor mensal vigente, ressalvado o reajuste regularmente concedido.

8.3. O valor do item 01 não integrará o valor das prorrogações e não poderá ser novamente cobrado ou incorporado às mensalidades.

9. MODELO DE GESTÃO DO CONTRATO

9.1. A gestão e a fiscalização do objeto contratado serão realizadas conforme o disposto no Decreto Municipal nº 14/2024.

9.2. Fica designado como Gestor do presente contrato, o Sr. **Robson Coteskvisk**, Secretário Municipal de Administração e como Fiscal do contrato, **Idonez Roberto Piccoli**, cargo de Oficial Administrativo.

9.3. Dentre as responsabilidades do fiscal, está a necessidade de anotar, em registro próprio, todas as ocorrências relacionadas à execução do contrato, inclusive quando de seu fiel cumprimento, determinando o que for necessário para a regularização de eventuais faltas ou defeitos observados.

10. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

10.1. **Da implantação**

Os serviços de implantação serão considerados concluídos após:

- instalação física do firewall;
- configuração da solução;
- instalação das licenças do sistema da solução de proteção de endpoints nos equipamentos indicados pelo Município;
- realização dos testes operacionais;
- homologação pela fiscalização contratual.

Concluída a implantação e emitido o Termo de Recebimento correspondente, será autorizada a emissão da Nota Fiscal referente ao serviço de implantação.

10.2. **Dos serviços continuados**

A prestação mensal dos Serviços Gerenciados de Cibersegurança será considerada executada mediante a comprovação de que:

- o firewall permaneceu em funcionamento;
- o licenciamento permaneceu ativo;
- as licenças do sistema de proteção de endpoints permaneceram atualizadas;
- o monitoramento contínuo foi realizado;
- os incidentes registrados receberam tratamento;
- o suporte técnico foi disponibilizado;
- foram apresentados os relatórios mensais de acompanhamento.
- relatório de cumprimento dos níveis de serviço – SLA, contendo, quando houver ocorrências, número do chamado, data e horário, classificação da criticidade, horário de início do atendimento, medida de contenção adotada, restabelecimento do serviço e encerramento;
- informação sobre eventual descumprimento dos níveis mínimos de atendimento e respectiva justificativa;
- situação operacional do Firewall, licenciamento, proteção de endpoints e demais componentes integrantes da solução.

10.3. **Do pagamento**

O pagamento será realizado até o 10º (décimo) dia útil do mês subsequente ao da efetiva prestação dos serviços, mediante a emissão da Nota Fiscal, desde que atestada pelo Fiscal do Contrato.

A contratada deverá apresentar:

- Nota Fiscal;
- Certidões de regularidade fiscal e trabalhista, quando exigidas pela legislação;
- Relatório mensal dos serviços executados;
- Relatório de incidentes atendidos no período;
- Relatório contendo a situação operacional da solução.

Em caso de erro na Nota Fiscal ou de qualquer pendência que impeça sua liquidação, o prazo para pagamento ficará suspenso até a regularização.

Ocorrendo atraso de pagamento por responsabilidade da Administração, incidirá atualização monetária pelo IPCA, acrescida de juros legais.

O valor correspondente à implantação da solução (item 01), será pago uma única vez, após a conclusão integral da implantação, correção das inconsistências eventualmente identificadas e recebimento definitivo pela fiscalização.

Não será admitido pagamento antecipado nem pagamento parcial do item 01 antes da efetiva homologação da solução.

A prestação e a cobrança mensal, relativa ao item 02, terão início somente após a conclusão da implantação e a homologação da solução pela fiscalização contratual, mediante emissão do respectivo Termo de Recebimento.

10.4. **Do reajustamento**

O valor mensal da contratação poderá ser reajustado por ocasião de cada prorrogação contratual, desde que transcorrido o período mínimo de 12 (doze) meses da assinatura do contrato, mediante aplicação do Índice Nacional de Preços ao Consumidor Amplo – IPCA, ou outro índice oficial que venha a substituí-lo.

Os reajustes subsequentes observarão o interregno mínimo de 12 meses, contado da data de início dos efeitos financeiros do último reajuste concedido.

O(s) reajuste(s) incidirá(ão) exclusivamente sobre o item 02, considerando que o item 01 será executado e pago uma única vez, não sendo objeto de renovação.

Permanece assegurado o direito ao reequilíbrio econômico-financeiro nas hipóteses previstas nos arts. 124 a 136 da Lei Federal nº 14.133/2021.

Rio dos Índios/RS, 11 de setembro de 2026.

Robson Coteskvisk
Secretaria Municipal de Administração

ANEXO I

REQUISITOS TÉCNICAS MÍNIMOS DA SOLUÇÃO DE CIBERSEGURANÇA

As especificações estabelecidas neste Anexo constituem requisitos técnicos mínimos e obrigatórios da solução. Será admitida a oferta de solução com características superiores, desde que integralmente compatível com o ambiente tecnológico do Município e sem custos adicionais.

1. DISPOSIÇÕES GERAIS

As três soluções que compõem o objeto, Firewall de Próxima Geração (NGFW), Gerenciamento Unificado e Relatórios e Proteção de Endpoints (Antivírus), deverão ser fornecidas pelo mesmo fabricante, integradas nativamente entre si, operadas por meio de uma única plataforma/console de gerenciamento centralizado, de modo a atuar de forma harmônica e sincronizada na proteção do ambiente. Não serão aceitas soluções de fabricantes distintos ou que exijam consoles de gerenciamento separadas, ainda que integradas por meio de APIs ou ferramentas de terceiros.

A exigência de integração nativa e de fornecimento das principais soluções pelo mesmo fabricante decorre da necessidade de administração centralizada, correlação automática de eventos, interoperabilidade dos mecanismos de proteção, padronização da operação e resposta coordenada aos incidentes de segurança, conforme fundamentação constante do Estudo Técnico Preliminar.

2. REQUISITOS TÉCNICOS MÍNIMOS DO FIREWALL DE PRÓXIMA GERAÇÃO

Para prestação de serviço a CONTRATADA deve fornecer a solução de NGFW que atenda aos requisitos técnicos abaixo detalhados durante todo o período de vigência do contrato.

2.1. REQUISITOS DE DESEMPENHO DO APPLIANCE

2.1.1. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 1 Gbps ou superior.

2.1.2. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 500 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante que atendam as especificações mínimas apresentadas a seguir:

a) Desempenho mínimo de 1.5 Gbps de IPS;

b) Suporte mínimo de 900.000 conexões simultâneas/concorrentes;

c) Suporte mínimo de 9.000 novas conexões por segundo;

d) Permitir expansão de armazenamento de até 256Gb;

e) Fonte de alimentação com chaveamento automático de 100-240 VAC;

f) Possuir 8 interfaces GbE padrão RJ-45;

g) Possuir 1 interface do tipo console ou similar;

h) Possuir 1 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.

2.1.3. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 5 usuários simultâneos.

2.1.4. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos.

2.1.5. Suportar 100 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.

2.1.6. Suportar 1.3 Gbps de desempenho de VPN IPSEC.

2.1.7. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitado. Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame.

2.1.8. O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.

2.1.9. O Equipamento deverá ser homologado pela ANATEL.

2.1.10. A solução deve realizar a inspeção de arquivos, no uso da tecnologia 'gateway antimalware', sem limite de tamanho, tendo em vista que, se houver limitação, poderia haver a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

2.2. CARACTERÍSTICAS GERAIS DO FIREWALL

2.2.1. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.

2.2.2. Para proteção do ambiente contra ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.

2.2.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada.

2.2.4. Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço. Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade.

2.2.5. Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes.

2.2.6. O firewall deverá ser entregue com licenciamento válido, incluindo garantia e suporte.

2.2.7. Deve ser capaz de atualizar de forma automática o Firmware, patches e atualizações de segurança.

2.2.8. A solução deve permitir o uso de armazenamento externo para System Logs, Threat Logs, AppFlow reporting data e Packet Captures, garantindo persistência de dados após reinicializações do firewall.

2.2.9. O painel deve exibir detalhes sobre o último contato do Firewall com o gerenciador de licenciamento, mostrando o status de atualização de licenças e atualizações de assinaturas.

2.2.10. Deve fornece APIs para que os fornecedores externos de NAC possam transmitir o contexto de segurança ao firewall e que esta funcionalidade seja compatível com a utilização simultânea de fornecedores externos distintos.

2.3. CARACTERÍSTICAS DIVERSAS

2.3.1. Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.

2.3.2. Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do tunel IPSec.

2.3.3. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

2.3.4. Deve possuir proteção anti-spoofing.

2.3.5. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP.

2.3.6. Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF.

2.3.7. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação.

2.3.8. A solução deverá possuir a tecnologia SD-WAN (Software Defined WAN), e que a mesma seja nativa da solução, sem a necessidade de qualquer tipo de licenciamento complementar, para evitar indisponibilidade no ambiente mesmo em caso de expiração do licenciamento vigente.

2.3.9. Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

a) Latência;

b) Jitter;

c) Perda de pacotes.

2.3.10. O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal logico.

2.3.11. A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.

2.3.12. A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.

2.3.13. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

2.3.14. Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

2.3.15. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

2.3.16. Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN.

2.3.17. Deve suportar DHCP relay.

2.3.18. Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.

2.3.19. Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, interface (física e virtual) ou zona de segurança.

2.3.20. Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer), para usuários da rede, individualmente ou em grupo.

2.3.21. Deve ter suporte à proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.

2.3.22. Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados.

2.3.23. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

2.3.24. Detectar e bloquear a origem de portscans.

2.3.25. Deve permitir o bloqueio de ataques.

2.3.26. Deve permitir o bloqueio de exploits conhecidos.

2.3.27. O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP e SMTP.

2.3.28. Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser decriptografado de forma transparente à aplicação.

2.3.29. Implementar DSCP (Differentiated Services Code Points).

2.3.30. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.

2.3.31. Implementar controle e gerenciamento de banda para a tecnologia VoIP (Voice over IP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.

2.3.32. Implementar mecanismo de sincronismo de horário através do protocolo NTP.

2.3.33. Possuir suporte ao protocolo SNMP versões 2 e 3.

2.3.34. Possuir suporte a log via Syslog.

2.3.35. Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.

2.3.36. O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para firewall, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período de tempo, e baseado em normas nacionais e internacionais de segurança da informação.

2.3.37. Visando estabelecer efetividade de segurança do firewall de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante ou a solução deverá possuir certificação, avaliação ou teste independente de eficácia em segurança, emitido por entidade reconhecida, tais como NetSecOPEN, ICSA, Common Criteria ou a comprovação por outros organismos independentes de reconhecida credibilidade.

2.3.38. Reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.

2.3.39. Para tráfego criptografado SSL/TLS, deve descriptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.

2.3.40. Controle, inspeção e descriptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3.

2.3.41. Deve permitir a funcionalidade de ARP bridging.

2.3.42. Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm".

2.3.43. A solução deve permitir a visualização gráfica das regras de segurança e acesso.

2.4. CARACTERÍSTICAS DE VPN

2.4.1. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

2.4.2. Suportar algoritmos de criptografia 3DES, AES128, AES256 e AESGCM16-256.

2.4.3. Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.

2.4.4. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits.

2.4.5. Deverá suportar algoritmo Internet Key Exchange (IKE) v1 e v2.

2.4.6. Autenticação via de túneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site.

2.4.7. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.

2.4.8. Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico.

2.4.9. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

2.4.10. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos.

2.4.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário.

2.4.12. Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.

2.4.13. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

2.4.14. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication.

2.4.15. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário.

2.4.16. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

2.5. CONTROLE DE AMEAÇAS

2.5.1. Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança.

2.5.2. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança do appliance através de assinaturas.

2.5.3. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

2.5.4. Implementar funcionalidade de detecção e bloqueio de “call-backs”.

2.5.5. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede.

2.5.6. A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP.

2.5.7. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

2.5.8. Implementar interface CLI segura através do protocolo SSH.

2.5.9. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.

2.5.10. A solução deve permitir criar regras de exceção de acordo com a proteção.

2.5.11. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots.

2.5.12. Permitir o bloqueio de malwares (vírus, worms, spyware e etc).

2.5.13. A solução deve ser capaz de proteger contra ataques a DNS.

2.5.14. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.

2.5.15. A solução deve ser capaz de prevenir acesso a websites maliciosos.

2.5.16. A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.

2.5.17. A solução deverá receber atualizações de um serviço baseado em cloud.

2.5.18. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

2.5.19. A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.

2.5.20. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade.

2.5.21. A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente ameaças exploradas por vulnerabilidades do tipo meltdown.

2.5.22. A solução de Gateway AntiVirus deverá ter a tecnologia complementar de Anti Virus-Cloud, para que os mecanismos existentes de verificação sejam ampliados.

2.5.23. A solução deve ser capaz de bloquear proativamente o acesso a domínios maliciosos conhecidos por meio de filtragem DNS, reduzindo assim o risco de infecções por malware e outros ataques cibernéticos.

2.6. PROTEÇÃO CONTRA ATAQUES AVANÇADOS

2.6.1. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.

2.6.2. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.

2.6.3. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.

2.6.4. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

2.6.5. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.

2.6.6. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb.

2.6.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.

2.6.8. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware.

2.6.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

2.6.10. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas.

2.6.11. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados.

2.6.12. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego.

2.6.13. Conter ameaças avançadas de dia zero.

2.6.14. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador.

2.6.15. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

2.6.16. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.

2.6.17. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado.

2.6.18. Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado.

2.6.19. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP , IMAP e CIFS.

2.6.20. Mitigar ameaças de dia zero de forma transparente para o usuário final.

2.6.21. Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro.

2.6.22. Implementar mecanismo de pesquisa por diferentes intervalos de tempo.

2.6.23. Mitigar ameaças de dia zero via tráfego de internet.

2.6.24. Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança.

2.6.25. Mitigar ameaças de dia zero que possam burlar o sistema operacional emulado.

2.6.26. A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo.

2.6.27. Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso.

2.6.28. Conter e mitigar exploits avançados.

2.6.29. A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Anti-Vírus e Anti-Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede).

2.6.30. Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.

2.6.31. ,31 As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real.

2.6.32. A Solução de segurança do firewall deverá ter um sistema de inspeção baseado em fluxo que execute análises simultâneas de tráfego de entrada e saída em alta velocidade, sem proxying ou buffering.

2.6.33. A Solução deve unificar diversas funções de segurança em um único conjunto integrado, inspecionando os arquivos de usuários locais, remotos e móveis.

2.6.34. A Solução deve unificar diversas funções de segurança em um único conjunto integrado inspecionando os arquivos de usuários locais, remotos e móveis.

2.6.35. A Solução deve descriptografar e inspecionar o tráfego criptografado, como HTTPS, SMTPS, NNTPS, etc., sem afetar o desempenho.

2.6.36. A solução de segurança do firewall deverá fornecer tecnologias avançadas de proteção contra ameaças , com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

a) Inspeção profunda de memória em tempo real;

b) Inspeção profunda de pacotes livre de remontagem;

c) Descriptografia e inspeção TLS/SSL;

d) Inteligência e controle de aplicativos;

e) Recursos SD-WAN seguros.

2.6.37. É imprescindível que a solução não possua um limite de tamanho de inspeção de arquivos no uso da tecnologia 'gateway antimalware', já que tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

2.7. CARACTERÍSTICAS DE FILTRO DE CONTEÚDO WEB

2.7.1. Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 89 (oitenta e nove) categorias distintas, com mecanismo de atualização e consulta automáticas.

2.7.2. 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.

2.7.3. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico.

2.7.4. Permitir a customização de página de bloqueio.

2.7.5. Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante.

2.7.6. Deve permitir submissão de novos sites para categorização.

2.7.7. Permitir a classificação dinâmica de sites web, URLs e domínios.

2.7.8. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.

2.7.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web.

2.7.10. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.

2.8. CARACTERÍSTICAS DE AUTENTICAÇÃO

2.8.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea.

2.8.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API.

2.8.3. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento.

2.8.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW.

2.8.5. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.

2.8.6. 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 NGFW.

2.8.7. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.

2.8.8. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.

2.8.9. Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

2.8.10. A solução deve possibilitar SSO via API.

2.8.11. A solução deve prover o bloqueio de URL baseado em reputação, identificando e bloqueando proativamente entidades suspeitas.

2.9. CARACTERÍSTICAS DE ADMINISTRAÇÃO

2.9.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração.

2.9.2. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW.

2.9.3. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional.

2.9.4. Possuir mecanismo para agendamento realização das cópias de segurança(backups) de configuração.

2.9.5. Possuir mecanismo para exportar as configurações através de FTP, HTTPS ou SFTP.

2.9.6. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante.

2.9.7. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões.

2.9.8. Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real.

2.9.9. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados.

2.9.10. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de “ICMP Unreachable” para máquina de origem do tráfego, “TCP-Reset” para o cliente, “TCP-Reset” para o servidor ou para os dois lados da conexão.

2.9.11. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

2.9.12. Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento.

2.9.13. Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF.

2.9.14. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP IPV4 e IPV6.

2.9.15. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização.

2.9.16. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web).

2.9.17. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto.

2.9.18. Ser capaz de implementar a funcionalidade de “Zero-Touch”, permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada.

2.9.19. A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android.

2.9.20. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB.

2.9.21. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW.

2.9.22. O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW.

2.9.23. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW.

2.9.24. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS.

2.9.25. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.

2.9.26. A solução deve possibilitar ao administrador habilitar ou desabilitar as capacidades de auto provisionamento da plataforma através de ponto central de gerenciamento.

2.9.27. Deve ser capaz de emitir relatório, mostrando a saúde do ambiente, agendado ou sob demanda, que liste informações de aplicações, risco, atividade WEB, análise de botnets, análise de malware, ameaças, países por tráfego, Arquivos compartilhados por aplicações, sessões e recomendações.

2.9.28. A solução deve suportar API como alternativa à interface de linha de comando (CLI), para configurar funções diversas.

2.9.29. Deve permitir que os administradores criem/recuperem/excluam listas de URLs ou endereços IP a serem bloqueados por meio de chamadas de API RESTful.

3. GERENCIAMENTO UNIFICADO E RELATÓRIOS

A CONTRATADA deve fornecer uma Solução de Gerenciamento Unificado e Relatórios que atenda aos requisitos técnicos detalhados abaixo, durante todo o período de vigência do contrato.

3.1. Deve possuir solução de gerenciamento centralizado em nuvem do mesmo fabricante, para gerenciamento de toda solução.

3.2. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções dos usuários da console que determinem usuários.

a) Firewall permitido;

b) Funcionalidades permitidas para o firewall, de acordo com o perfil de uso designado;

c) Perfil de nível de acesso (escrita, leitura, administração, relatórios).

3.3. Deve suportar organizar os dispositivos administrados em grupos. Estes grupos devem permitir isolamento tanto de acesso para os administradores como de configuração massiva ou individual.

3.4. O gerenciamento deve permitir/possuir:

a) Criação e administração de políticas de firewall e controle de aplicação;

b) Monitoração de logs;

c) Investigação de eventos de segurança e falhas (debugging);

d) Acesso concorrente de administradores, conforme políticas e perfis previamente definidos.

3.5. Deve permitir o provisionamento e configuração sem intervenção de operadores (Zero-Touch). O firewall deve se conectar automaticamente à plataforma de gerenciamento, e a partir desta conexão receber as configurações previamente determinadas pelos operadores da plataforma.

3.6. A solução de gerenciamento deve ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL.

3.7. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança, possibilitando geração de relatórios analíticos e de forma centralizada de todos os dispositivos gerenciados.

3.8. A solução deve possuir tela situacional com todo o inventário de firewall gerenciado centralizadamente, informando no mínimo para o administrador:

a) nome do firewall;

b) número de série;

c) modelo;

d) versão do firmware e estado da conectividade do equipamento com a gerência em online ou offline.

3.9. Deverá permitir atualizar o sistema operacional de múltiplos equipamentos gerenciados de uma única vez.

3.10. A solução deve possuir Dashboard com sumário de alertas e informação de status de licença.

3.11. A solução deverá permitir seu gerenciamento por Web GUI utilizando protocolo HTTPS sem a necessidade de uso de cliente ou console do tipo aplicativo.

3.12. Deve manter um canal de comunicação segura, com encriptação baseada HTTPS, entre todos os componentes que fazem parte da solução de firewall, gerência.

3.13. A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão no console de gerência local do firewall sem a necessidade de o administrador utilizar endereço IP do dispositivo, URL ou FQDN.

3.14. A solução deve permitir a criação de modelos de configuração (templates) para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação no firewall.

3.15. A solução deve possibilitar gerar, editar, salvar e aplicar templates de configuração no firewall, pelo administrador da plataforma.

3.16. Os modelos de configuração (templates) devem suportar configurações de interfaces físicas ou virtuais.

3.17. A solução deve permitir a criação de grupos lógicos, para o agrupamento de dispositivos, com isso permitindo a aplicação de modelos de configuração a diversos equipamentos de uma única vez.

3.18. Deverá permitir visualizar a diferença nas mudanças antes que a configurações sejam implantadas.

3.19. De forma centralizada deve permitir gerenciar, mas não limitado há, políticas de firewall, NAT, rotas, PBR (Policy Based Routing), configuração de endereçamento IP das interfaces dos equipamentos, criação e administração de políticas de IPS, configuração de políticas de antivírus e antimalware, configuração e criação de políticas de controle de URL, criação e configuração de políticas de controle de aplicações, criação e configuração de política de SANDBOX, criação e configuração de políticas de controle de banda, criação e configuração de objetos necessários para configuração das políticas especificadas acima, usando uma única interface de gerenciamento.

3.20. Deve incluir console de configuração e monitoramento SD-WAN, possibilitar a criação de políticas SD-WAN em todos os elementos gerenciados, baseando-se em parâmetros de latência, perda de pacote e jitter, para a tomada de decisão de encaminhamento de tráfego no firewall.

3.21. Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria.

3.22. Durante a alterações de políticas de segurança do firewall, deverá ser possível o agendamento para determinar o horário que as mudanças entrarão em vigor, proporcionando ao administrador aplicar políticas de segurança em horários com menor impacto para o ambiente.

3.23. Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, este processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente.

3.24. A funcionalidade de Workflow deve permitir configurar, em dias, a validade dos pedidos de aprovação, caso o pedido de aprovação não seja aprovado no período configurado, essa mudança deve ser expirada e não efetivada.

3.25. A solução deve oferecer monitor de auditoria de configurações aplicadas ao firewall gerenciado pela plataforma, permitindo comparativo diferencial entre registros para rápida identificação de configurações e alterações aplicadas.

3.26. A solução deve oferecer módulo centralizado que possibilite realização e armazenamento de backup de configurações do firewall gerenciado.

3.27. A solução deve oferecer possibilidade de auditoria de configurações.

3.28. A solução deve possibilitar o monitoramento em tempo real do firewall gerenciado, informando minimamente:

a) Utilização de CPU/Processamento;

b) Aplicações em uso e seu consumo de banda;

c) Interfaces em uso e utilização de banda;

d) Conexões concorrentes em uso.

3.29. A solução deverá permitir visualizar sumário com as informações referentes as principais ameaças identificadas ou bloqueadas pelo firewall.

3.30. Deverá suportar logs do tipo Netflow, IPFIX ou Syslog, para a geração de relatórios e monitoramento em tempo real.

3.31. A solução deverá prover relatórios com no mínimo histórico de 365 dias.

3.32. A solução deverá prover relatórios referente as atividades dos usuários.

3.33. A solução deverá prover relatórios referente ao uso de aplicações web, com no mínimo as seguintes informações:

a) nome da aplicação;

b) quantidade de conexões;

c) percentual que a aplicação representa do tráfego da rede e quantidade de Megabytes trafegados.

3.34. A solução deverá prover relatórios referente ao consumo de rede dos usuários, com no mínimo as seguintes informações:

a) nome do usuário;

b) quantidade de conexões;

c) percentual que tráfego do usuário representa na rede;

d) quantidade de Megabytes trafegados.

3.35. A solução deverá prover relatórios referente ao consumo de rede por endereço IP, com no mínimo as seguintes informações:

a) endereço IP;

b) quantidade de conexões;

c) percentual que tráfego que o IP representa na rede;

d) quantidade de Megabytes trafegados.

3.36. A solução deverá prover relatórios referente aos acessos web com no mínimo informações referentes às categorias acessadas, quantidade de conexões e percentual que cada categoria web representou no tráfego de rede.

3.37. A solução deverá arquivar relatórios gerados automaticamente, permitindo o administrador fazer o download em formato PDF.

3.38. A solução deverá permitir geração e envio agendado de relatórios.

3.39. A solução deve permitir a customização de alertas e notificações, possibilitando o envio de e-Mail com as informações relativas a este evento.

3.40. A solução deve possibilitar configuração e monitoramento centralizados das VPNs estabelecidas pelo firewall.

3.41. A solução deve apresentar consoles de indicação com os principais eventos, riscos e ameaças contendo:

a) Aplicações de maior risco, e volume de dados consumido por estas

b) Aplicações de maior utilização, por volume de dados transferidos e conexões consumidas

c) Aplicações de maior utilização, por categoria

3.42. A solução deve apresentar consoles de indicação dos principais usuários contendo:

a) Usuários utilizando mais conexões;

b) Usuários consumindo mais dados.

3.43. A solução deve apresentar console de indicação de:

a) Virus/Spyware bloqueados;

b) Intrusões bloqueadas;

c) Botnets bloqueados;

d) Origens e destinos mais utilizados.

3.44. A solução deve apresentar console de indicação de Aplicações indicando:

a) Aplicações identificadas;

b) Categorização e uso das aplicações;

c) Risco das aplicações.

3.45. A solução deve permitir visualização de eventos correlacionados que possam ser investigados por:

a) Lista de eventos correlacionados com opção de navegação "drilldown"; ou

b) Modo gráfico; ou

c) Lista de logs.

3.46. A solução deve apresentar console de monitoramento de produtividade dos usuários, indicando suas características de navegação de acordo com políticas previamente estabelecidas e categorizadas como:

a) Produtivas;

b) Não produtivas;

c) Aceitáveis para a política de uso corporativa;

d) Inaceitáveis para a política de uso corporativa;

e) Customizadas.

3.47. A solução deve permitir visualização de topologia do firewall e elementos a ele conectados (dispositivos de rede complementares, dispositivos de usuários, Access Points).

3.48. O Fabricante deverá comprovar que possui tecnologia holística capaz de integrar suas principais soluções em uma base centralizada gráfica com informações e alertas, comprovando integração de pelo menos 2 de suas plataformas de segurança.

3.49. Controle de Acessos Privilegiados – PAM

3.49.1. A CONTRATADA deverá disponibilizar e utilizar solução de Gerenciamento de Acessos Privilegiados – PAM, ou mecanismo tecnicamente equivalente, para controle, proteção, conformidade e auditoria dos acessos administrativos realizados por sua equipe técnica nos dispositivos, sistemas e ferramentas que compõem a solução contratada.

3.49.2. A solução deverá permitir, no mínimo:

a) a individualização e identificação dos profissionais responsáveis pelos acessos;

b) o controle das permissões administrativas conforme o perfil e a necessidade de cada usuário;

c) a proteção e o armazenamento seguro das credenciais privilegiadas;

d) a realização dos acessos administrativos sem exposição das senhas reais dos dispositivos aos profissionais;

e) o registro automático das datas, horários, duração e atividades realizadas em cada acesso;

f) a gravação ou manutenção de registro auditável das sessões administrativas, de forma nativa e automática;

g) a consulta e disponibilização dos registros e das evidências de acesso à fiscalização contratual, sempre que solicitado; e

h) a adoção de mecanismos que impeçam a alteração ou exclusão dos registros pelos usuários responsáveis pelo acesso.

3.49.3. A solução PAM ou mecanismo equivalente deverá estar disponível a partir da conclusão da implantação e permanecer ativa durante toda a vigência contratual, inclusive nas eventuais prorrogações, sem custos adicionais para o Município.

3.49.4. A CONTRATADA deverá demonstrar o funcionamento do mecanismo de controle de acessos privilegiados durante a implantação da solução ou, quando solicitado pela Administração, por ocasião da Prova de Conceito.

3.49.5. Os registros das sessões administrativas deverão ser mantidos pelo prazo mínimo de 12 meses, assegurada sua integridade, confidencialidade e disponibilidade para fins de auditoria.

4. REQUISITOS TÉCNICOS MÍNIMOS DA PROTEÇÃO DE ENDPOINTS

A CONTRATADA deve fornecer uma Solução de Proteção De Endpoints (Antivírus) que atenda aos requisitos técnicos detalhados abaixo, durante todo o período de vigência do contrato.

A solução de proteção de Endpoints deve possuir de módulos de software integrados gerenciados por um único fabricante de forma a atender ao conjunto de requisitos técnicos exigidos nessa especificação.

Devido ao progresso de ataques a dispositivos e regulamentações nacionais e internacionais, far-se-á necessária o fornecimento de módulo de detecção e resposta de endpoints, coletando, inspecionando e centralizando as informações importantes que acontecem em tempo real, para que, a qualquer momento, mesmo após a ocorrência de um incidente de segurança, a equipe técnica do contratante possa investigar a causa raiz e responder/mitigar o impacto com o máximo de informações possíveis remediando os endpoints da rede corporativa por ventura comprometidos com maior rapidez.

Deve permitir a integração de forma nativa com gerência centralizada da solução de segurança, para trabalhar de forma harmônica e sincronizada com os demais componentes de segurança da solução do fabricante.

Deve ser entregue com o gerenciamento do sistema ofertado baseado em modelo de nuvem computacional.

Deverá implementar mecanismo de descoberta de ameaças cibernéticas baseado em análise de inteligência artificial permitindo a coleta de dados dos endpoints e seu armazenamento centralizado em console de gerência em ambiente de nuvem (SaaS).

A solução não poderá depender exclusivamente de assinaturas tradicionais para identificação de ameaças, devendo empregar mecanismos adicionais de detecção e prevenção, tais como análise comportamental, inteligência artificial, machine learning, heurística ou tecnologias equivalentes.

Todos os módulos de software do sistema ofertado deverão atender às especificações técnicas descritas neste documento em sua integralidade.

O licenciamento deve ser realizado de acordo com o quantitativo do órgão, sendo necessário a proteção para até 60 endpoints simultaneamente protegidos.

Suporte total para os seguintes sistemas operacionais:

a) Windows 10;

b) Windows 11;

c) Windows Server 2022.

A console de gerência deverá ser centralizada com interface gráfica web.

A solução deverá prover permitir a instalação inicial de agentes de segurança nos endpoints pelos administradores de forma silenciosa.

A gerência centralizada deverá permitir a distribuição de atualizações nos módulos de Next Generation antivírus em execução nos agentes de segurança.

Deve prover detecção e prevenção de ameaças em real-time.

O funcionamento da solução deve operar analisando a pré-execução e pós-execução da ameaça em potencial, em nível de sistema operacional (O/S), memória e prevenindo a entrada de códigos maliciosos.

Capacidade de análise automática do código do arquivo, identificando suas características antes da sua capacidade de execução.

A solução deve aplicar análise baseada em código algoritmo, para identificar programas maliciosos antes da sua execução.

Caso seja encontrado um programa malicioso a sua execução não deve ser permitida.

A solução deve identificar e bloquear a execução de códigos executáveis, scripts ou comandos.

A solução de endpoint deve prevenir e detectar qualquer alteração oriunda de código malicioso em programas que sejam executados em memória.

Deve utilizar a tecnologia de “Machine Learning” para identificar qualquer ameaça nos arquivos potencialmente perigosos.

Caso necessário a solução deve ter a capacidade de encaminhar arquivos identificados como ameaças para uma solução de “Sandbox On-premisses ou On-Cloud”, com o objetivo de fazer uma segunda análise em diferentes sistemas operacionais.

Identificar ameaças avançadas, chamadas de “Zero-day”, sem a necessidade de base de assinaturas (DATs) e suas atualizações, detecção por heurística, detecção por comportamento ou sandboxing.

Seu engine deve ter passado satisfatoriamente, sob documentação a ser avaliada , nos 3 testes de ameaças mais recentes do MITRE@ATTACK.

Permitir o uso de Filtro de Conteúdo Categorizado.

Permitir recurso de Restaurar uma máquina no caso de uma contaminação por ransomware.

4.1. GERENCIAMENTO E ADMINISTRAÇÃO CENTRALIZADA PARA ESTAÇÕES DE TRABALHO

4.1.1. A console de monitoração e configuração deve ser feita através de uma central para o grupo de antimalware, baseada em web e em nuvem, que deve conter toda a ferramentas para a monitoração e controle da proteção dos dispositivos.

4.1.2. A console deve apresentar painel com o resumo dos status de proteção dos computadores, bem como indicar os alertas de eventos de criticidades alta, média e informacional.

4.1.3. A console deve permitir a divisão dos computadores, dentro da estrutura de gerenciamento em grupos.

4.1.4. Permitir sincronização com LDAP ou Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção.

4.1.5. Aplicar regras diferenciadas baseado em grupos ou usuários.

4.1.6. A instalação do agente poderá ser realizada através de soluções de distribuição de softwares ou através de GPO.

4.1.7. A console deve permitir criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários ou endpoint, não importando em que equipamentos eles estejam acessando.

4.1.8. Fornecer atualizações do agente instalado através da console de gerenciamento; aceita-se documentação.

4.1.9. Permitir exclusões de escaneamento para os seguintes tipos tanto a nível geral quanto específico em uma determinada política:

a) Caminho (Path);

b) Hash;

c) Permitir a exportação dos relatórios gerenciais.

4.2. FUNCIONALIDADES COMPLEMENTARES

4.2.1. Serviço nativo de nuvem para proteção, no modelo Software como Serviço.

4.2.2. As quantidades para proteção devem ser do mesmo fabricante a fim de trabalharem conjuntamente na proteção do ambiente; A correlação e relatório dos eventos poderão ser realizados com agregação de outras soluções de forma transparente ao usuário final.

4.2.3. Deve buscar algum sinal de malware ativo e detectar malwares desconhecidos.

4.2.4. O agente deve ter a capacidade de submeter o arquivo desconhecido ou seus metadados à nuvem de inteligência do fabricante para detectar a presença de ameaças.

4.2.5. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência.

4.2.6. A solução deve proteger a estação de trabalho independente da estação estar conectada à internet.

4.2.7. Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot.

4.2.8. Suportar equipamentos com arquitetura 32-bit e 64-bit que o cliente deve ter instalado nas estações de trabalho e deve ser compatível com os sistemas operacionais: Mac OS Sonoma e superiores, Microsoft Windows 10 e 11.

4.2.9. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção.

4.2.10. Permitir a utilização de senha de proteção para permitir a reconfiguração local no cliente ou desinstalação dos componentes de proteção.

4.2.11. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo.

4.2.12. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas ou possuir modulo capaz de prevenir a exploração de vulnerabilidades conhecidas ou desconhecidas.

4.2.13. Deve possuir técnicas de proteção, que inclui:

a) técnica para detectar malware criptografado mais complexo;
b) Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;
c) Possuir capacidade para a detecção de vírus polimórficos, ou vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham.

4.2.14. Verificação de ameaças web avançadas: bloqueia tentativas de exploração do tipo fileless, quando o usuário abrir um site e o mesmo conter códigos malicioso, a solução deverá ser capaz de prevenir.

4.2.15. Ser capaz de segregar as contas de usuários de forma hierárquica com no mínimo os perfis “usuário” e “administrador”, não limitando o número de acesso de usuários simultâneos.

4.2.16. A solução deverá possuir módulo de investigação e detecção integrados.

4.3. ANTIVÍRUS E ANTISPYWARE

4.3.1. Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

4.3.2. Proteção antimalware nativa da solução ou incorporada sem a utilização de agentes adicionais, desde que distribuídos pelo fabricante.

4.3.3. As configurações do Anti-Spyware deverão ser realizadas através da mesma console do antivírus.

4.3.4. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware.

4.3.5. Permitir a inclusão de arquivos em listas de exclusão (whitelist) para que não sejam verificados pelo produto.

4.3.6. Permitir a varredura das ameaças da maneira manual e em tempo real na máquina do usuário.

4.3.7. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos, através do antivírus.

4.3.8. Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção.

4.3.9. A solução deverá possuir a capacidade de isolar o host, após a infecção, permitindo apenas a comunicação com a console de gerenciamento.

4.3.10. Permitir o bloqueio (ou desativação na política de Antivírus) da verificação de vírus em recursos mapeados da rede.

4.4. DETECÇÃO PROATIVA E RECONHECIMENTO DE NOVAS AMEAÇAS

4.4.1. Deve possuir funcionalidade de detecção de ameaças via técnicas de deep machine learning.

4.4.2. Funcionalidade de detecção de ameaças desconhecidas que estão em memória.

4.4.3. Deve possuir capacidade de detecção, e bloqueio proativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória.

4.4.4. Deve possuir capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória; aceita-se documentação.

4.4.5. Deve possuir capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada. aceita-se documentação.

4.4.6. Funcionalidade de proteção contra ransomwares.

4.4.7. Deve dispor de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas; aceita-se documentação.

4.4.8. Dispor de remediação da ação de criptografia maliciosa dos ransomwares com função de Rollback no console em caso de contaminação.

4.4.9. A solução deve prevenir ameaças e interromper que eles sejam executados em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas.

4.4.10. Possuir uma tecnologia anti-exploit baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de malware, protegendo os endpoints de ameaças desconhecidas e vulnerabilidades zero-day.

4.4.11. A solução deve trabalhar silenciosamente na máquina do usuário e deve detectar a criptografia maliciosa de dados (ransomware), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deve realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve fazer a limpeza e remoção completa do ransomware na máquina do usuário sem a necessidade intervenção humana.

4.4.12. Deve fornecer também uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real, indicando todas as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

4.4.13. A console de monitoração e a de configuração deve ser feita através de central, baseada em web e em nuvem ou appliance (físico ou virtual), que deve conter todas a ferramentas para a monitoração e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware.

4.4.14. A console deve apresentar painel com o resumo detalhado de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional.