# ESTUDO TÉCNICO PRELIMINAR

## 1. NECESSIDADE DA CONTRATAÇÃO

### 1.1. IDENTIFICAÇÃO DA NECESSIDADE DA CONTRATAÇÃO

1.1.1. A Equipe de Planejamento da Contratação elaborou o Estudo Técnico Preliminar com o objetivo de pesquisar uma Solução de Tecnologia da Informação e Comunicação (TIC) que proporcione o fornecimento de serviços de segurança da informação envolvendo solução de hardware, software, assinaturas de atualização, instalação, treinamento, customização e suporte técnico qualificado em proteção e inspeção de tráfego em redes corporativas, conforme especificações técnicas, incluindo os appliances necessários e suficientes para a prestação destes serviços, com o objetivo de garantir a proteção eficaz da rede de computadores, assim como a segurança das estações de trabalho, servidores de arquivos e dispositivos móveis, por meio de soluções antimalware endpoint com detecção e resposta de última geração, para análise da sua viabilidade e levantamento dos elementos essenciais que servirão para compor o Termo de Referência, de forma que melhor atenda às necessidades da Secretaria de Estado de Saúde de Mato Grosso do Sul, em conformidade com o disposto no art. 8° do Decreto Estadual n. 15.606 de 12 de fevereiro de 2021.

1.1.2. A referida contratação, após a devida autorização, deverá possuir adequação orçamentária e financeira com a Lei Orçamentária Anual – LOA e compatibilidade com o Plano Plurianual - PPA e Lei de Diretrizes Orçamentárias – LDO.

### 1.2. JUSTIFICATIVA DA NECESSIDADE:

1.2.1. A Secretaria de Estado de Saúde de Mato Grosso do Sul, por meio da Coordenadoria de Tecnologia de Informática e Informação (CTEC/SES/MS), está em constante processo de atualização tecnológica de seus sistemas de informação, programas e softwares legados. Esses sistemas estão gradualmente sendo substituídos por soluções computacionais baseadas em plataforma Web, proporcionando maior escalabilidade e portabilidade aos serviços públicos digitais, acessados por diversas plataformas e dispositivos conectados via Intranet e/ou Internet. Isso visa aprimorar o atendimento às necessidades dos usuários internos e aumentar a capilaridade dos serviços públicos disponíveis à sociedade.

1.2.2. Considerando a abrangência das ações da Secretaria de Estado de Saúde, as soluções de TIC desenvolvidas pela CTEC/SES/MS são utilizadas diariamente por todos os cidadãos sul-mato-grossenses, bem como por pessoas, empresas e instituições de outras localidades,

municípios, estados e até países que necessitam se relacionar com os serviços públicos prestados pela Secretaria de Estado de Saúde de Mato Grosso do Sul (SES/MS).

1.2.3. Como em qualquer sistema de informação, os dados produzidos e manipulados são armazenados e processados em bancos de dados gerenciais. No âmbito da SES/MS, esses dados são centralizados em seu Data Center, localizado nas dependências da CTEC, com parte da infraestrutura tecnológica também abrigada no Data Center da Secretaria-Executiva de Transformação Digital (SETDIG).

1.2.4. Dentre as várias atribuições da Coordenadoria de Tecnologia de Informática e Informação (CTEC), destacam-se as seguintes:

> *"II - coordenar as atividades de gestão e de execução da área de* ***gerência de redes de computadores, suporte técnico e operação do ambiente operacional****, manutenção corretiva e preventiva de equipamentos de informática e desenvolvimento e suporte em sistemas de informação;*
> *III - atuar nas áreas de projeto e* ***gerência de redes de computadores, suporte técnico e operação do ambiente operacional****, manutenção corretiva e preventiva de equipamentos de informática e desenvolvimento e suporte em sistemas de informação;*
> *IV - participar na formulação e avaliação de diretrizes,* ***estruturas e níveis de segurança da informação****, aplicadas à arquitetura de sistemas eletrônicos corporativos;*
> *V -* ***avaliar os recursos de sistemas de informação existentes no âmbito da SES****, visando otimização de sua eficácia, produtividade,* ***conectividade****, integração e a concepção de sistemas de apoio à decisão;"*

1.2.5. Nesse contexto, a CTEC tem adotado diversas iniciativas para cumprir suas atribuições com eficiência, disponibilizando soluções que assegurem níveis adequados de segurança aos dispositivos de tecnologia da informação, conforme padronizações determinadas pela SETDIG.

1.2.6. Para atingir esses objetivos, bem como os demais apresentados neste Estudo Técnico Preliminar, a SES/MS tem buscado, de forma racional e persistente, o melhor emprego de seus recursos, visando garantir a eficácia e eficiência de suas ações.

1.2.7. A estrutura tecnológica da SES/MS está em constante crescimento e expansão, impulsionada principalmente pelo aumento contínuo no volume de dados e pela ampliação significativa do número de aplicações e recursos ofertados. Isso torna essencial a manutenção dessa estrutura de forma estável.

1.2.8. É importante destacar que todas as informações recebidas, enviadas, tratadas e/ou armazenadas são de natureza sensível e/ou crítica. Isso reforça a necessidade de prover um nível elevado de segurança, condizente com o porte da estrutura tecnológica da SES/MS, uma vez que camadas avançadas de proteção mantêm a confiança, robustez e seguridade da rede corporativa do Governo do Estado de Mato Grosso do Sul como um todo.

1.2.9. Deve-se salientar que, sendo este um serviço que agrega modernização ao ambiente atual e à infraestrutura tecnológica da SES/MS, todo o investimento anteriormente realizado em outras iniciativas será integralmente aproveitado. Não haverá prejuízos à infraestrutura existente; pelo contrário, a proposta visa a integração nativa aos sistemas em uso, sem a necessidade de alterações em linhas de código ou configurações do ambiente atual.

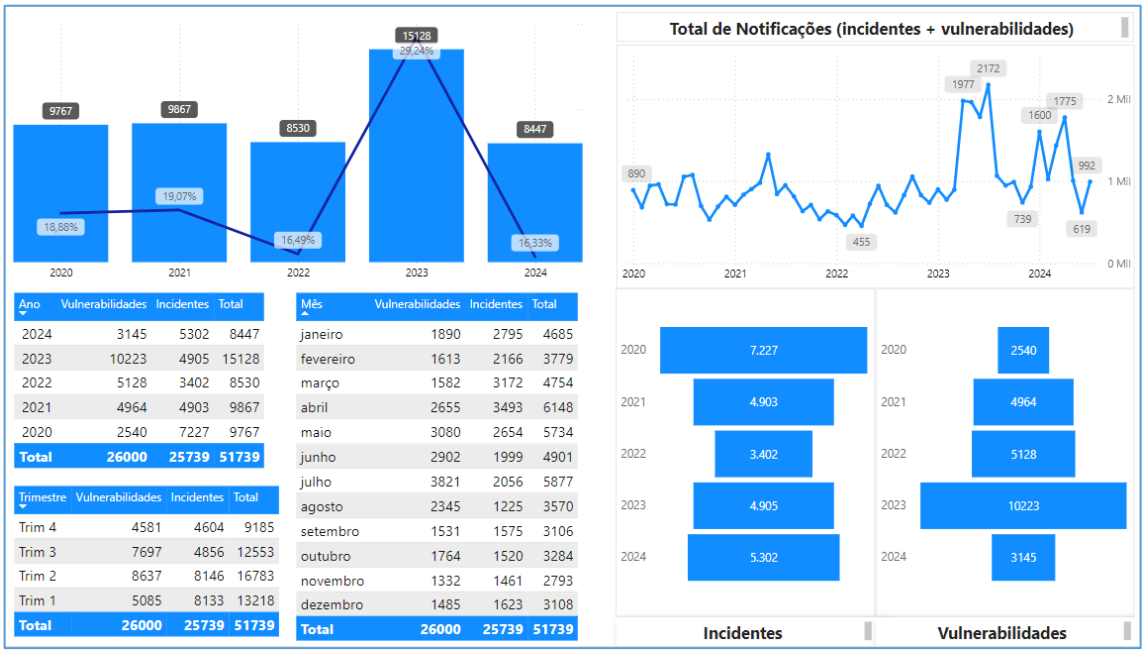
1.2.10. Considerando ainda a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que regulamenta o tratamento de dados pessoais, inclusive nos meios digitais, a LGPD está redefinindo o funcionamento e a operação das organizações ao estabelecer regras claras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo um padrão mais elevado de proteção e penalidades significativas em casos de não cumprimento.

1.2.11. A LGPD define "dados pessoais" como qualquer informação relacionada à pessoa natural identificada ou identificável, e "tratamento de dados" como toda operação realizada com dados pessoais, como coleta, classificação, utilização, acesso, reprodução, processamento, armazenamento, eliminação, controle da informação, entre outros.

1.2.12. Os órgãos da Administração Pública, especialmente a SES/MS, lidam com uma vasta quantidade e volume de dados e informações do público, desde dados simples, como nomes, até informações de caráter específico, sensível e/ou sigiloso, como dados fiscais, de saúde, cíveis e criminais. Portanto, é essencial garantir a proteção e segurança no tratamento dessas informações, adequando-se às regras e exigências da LGPD.

1.2.13. Em termos de proteção contra acessos não autorizados à rede governamental, vale ressaltar que, nos últimos anos, temos enfrentado novas e volumosas ameaças, especialmente aquelas alertadas pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), que emite diariamente diversos alertas relacionados a essas ameaças.

1.2.14. O CTIR Gov é um "*Computer Security Incident Response Team (CSIRT)*", ou Grupo de Resposta a Incidentes de Segurança. Um dos serviços providos pelo CTIR Gov é a disponibilização de estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos.




| Ano | Vulnerabilidades | Incidentes | Total |
|---|---|---|---|
| 2024 | 3145 | 5302 | 8447 |
| 2023 | 10223 | 4905 | 15128 |
| 2022 | 5128 | 3402 | 8530 |
| 2021 | 4964 | 4903 | 9867 |
| 2020 | 2540 | 7227 | 9767 |
| **Total** | **26000** | **25739** | **51739** |

| Trimestre | Vulnerabilidades | Incidentes | Total |
|---|---|---|---|
| Trim 4 | 4581 | 4604 | 9185 |
| Trim 3 | 7697 | 4856 | 12553 |
| Trim 2 | 8637 | 8146 | 16783 |
| Trim 1 | 5085 | 8133 | 13218 |
| **Total** | **26000** | **25739** | **51739** |

| Mês | Vulnerabilidades | Incidentes | Total |
|---|---|---|---|
| janeiro | 1890 | 2795 | 4685 |
| fevereiro | 1613 | 2166 | 3779 |
| março | 1582 | 3172 | 4754 |
| abril | 2655 | 3493 | 6148 |
| maio | 3080 | 2654 | 5734 |
| junho | 2902 | 1999 | 4901 |
| julho | 3821 | 2056 | 5877 |
| agosto | 2345 | 1225 | 3570 |
| setembro | 1531 | 1575 | 3106 |
| outubro | 1764 | 1520 | 3284 |
| novembro | 1332 | 1461 | 2793 |
| dezembro | 1485 | 1623 | 3108 |
| **Total** | **26000** | **25739** | **51739** |

Figura 1 - Notificações Reportadas pelo CTIR Gov - 2020 a 2024

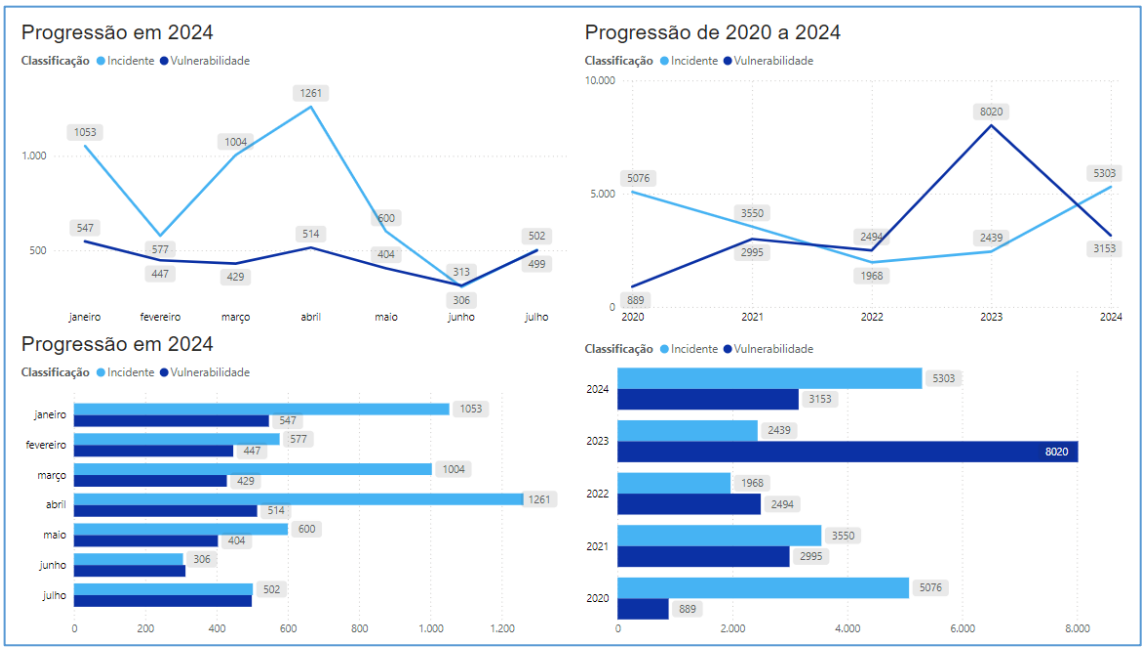



Figura 2 - Estatísticas dos Incidentes e Vulnerabilidades - Progressão

1.2.15. Diante dos desafios apresentados no tema de segurança da informação, surge a necessidade de encontrar medidas que possam garantir a segurança da informação do ambiente de TIC mantido pela Coordenadoria de Tecnologia de Informática e Informação, da Secretaria de Estado de Saúde de Mato Grosso do Sul.

1.2.16. Nesse sentido, para a continuidade e modernização das soluções de segurança existentes, são relacionadas as seguintes necessidades de negócio a serem atendidas:

1.2.16.1. Permitir a manutenção dos níveis adequados de segurança da informação, no que tange as ameaças provenientes de ataques externos e internos;

1.2.16.2. Manter a disponibilidade do ambiente de segurança da informação de forma ativa;

1.2.16.3. A proteção das estações de trabalho;

1.2.16.4. A proteção e o controle da Internet disponibilizada aos usuários;

1.2.16.5. Reduzir incidências de infecção causadas por Malwares e de indisponibilidades do serviço de acesso internet;

1.2.16.6. A proteção dos sistemas corporativos;

1.2.16.7. A possibilidade de realizar varreduras de vulnerabilidades; e

1.2.16.8. A possibilidade de realizar auditorias e verificações de conformidade.

1.2.16.9. Proporcionar proteção a dados e informações trafegados nas redes do Estado, garantindo verificação, possibilidade de liberação ou bloqueio de tráfego de dados; e

1.2.16.10. Aumentar confiabilidade dos dados disponibilizados aos públicos.

1.2.17. Este investimento manterá a capacidade e eficiência da Secretaria de Estado de Saúde de Mato Grosso do Sul no cumprimento efetivo de suas ações, assegurando a disponibilidade de seus inúmeros serviços por meio da infraestrutura de TIC, incluindo o atendimento a novas demandas que possam surgir.

1.3. CLASSIFICAÇÃO DO OBJETO COMO SOLUÇÃO DE TIC:

1.3.1. O Decreto Estadual n. 15.606 de 12 de fevereiro de 2021, em seu Art. 2°, III, assim considera: “Solução de Tecnologia da Informação e Comunicação (STIC): conjunto de bens e/ou de serviços que apoiam processos de negócio, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações”.

1.3.2. Em virtude disto, *o entendimento acerca da conceituação apresentada se baseia na* utilização *de bens* (hardware)*,* sistemas de informação (software) e/ou *serviços de TIC, tendo como finalidade* o processamento de dados e informações digitais para *o alcance dos resultado*s pretendidos pela contratação.

1.3.3. Considerando que a solução em estudo engloba elementos com as características descritas acima, de modo a atender à necessidade que a desencadeou, entende-se que esta contratação compreende uma solução de tecnologia, e assim sendo deverá seguir as diretrizes estabelecidas no Decreto Estadual supracitado.

## 2. DEMOSTRAÇÃO DA PREVISÃO NO PLANO DE CONTRATAÇÃO ANUAL

2.1. A presente contratação foi prevista no Plano de Contratação Anual (PCA) vigente para 2025, conforme já explicado e comprovado no documento de Solicitação de Abertura deste processo, juntado previamente a este instrumento.

| | Exercício | Descrição | Demandante | Elemento/Subelemento | Situação | Ações |
|---|---|---|---|---|---|---|
| ☐ | 2025 | Elaboração do Plano de Contratações Anual para o exercício de 2025 - Revisão | SSD - SES | 3390 - Serviços Técnicos Profissionais em TIC | Consolidado | |

## 3. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO

3.1. REQUISITOS NECESSÁRIOS

3.1.1. A aquisição presente compreende os requisitos inseridos na Tabela Descritiva abaixo, que são considerados necessários e indispensáveis para acatar a demanda solicitada.

| ITEM | DESCRIÇÃO | UNID. | QTD |
|---|---|---|---|
| 001 | Serviços Técnicos Especializados. | 1 - un | 01 |

| Item | Descrição Complementar | Unid. | Qtd. |
|---|---|---|---|
| 001 | Fornecimento de serviços de segurança da informação envolvendo solução de hardware, software, assinaturas de atualização, instalação, treinamento, customização e suporte técnico qualificado em proteção e inspeção de tráfego em redes corporativas, conforme especificações técnicas, incluindo os appliances necessários e suficientes para a prestação destes serviços, com o objetivo de garantir a proteção eficaz da rede de computadores, assim como a segurança das estações de trabalho, servidores de arquivos e dispositivos móveis, por meio de soluções antimalware endpoint com detecção e resposta de última geração. | Mês | 12 |

3.2. As especificações delineadas não restringem a competição, sendo possível atendimento por várias empresas atuantes no ramo.

3.3. REQUISITOS TÉCNICOS

3.3.1. Os requisitos mínimos exigidos neste subitem são justificados pelas necessidades de:

3.3.1.1. Contratar uma solução específica de mercado, com tecnologia construída para os fins a que se destinam, através de um processo de engenharia de qualidade, e não um produto adaptado em cima de um hardware ou software genérico, sem garantia de desempenho ou da qualidade de seus componentes; e

3.3.1.2. Garantir que o produto ofertado tenha as funcionalidades mínimas necessárias para qualquer hardware desta finalidade e que possam ser configurados de acordo com a especificidade da rede de dados corporativa da Secretaria de Estado de Saúde, independentemente de mudanças futuras na topologia da rede.

3.3.2. Deverão ser fornecidos equipamentos do tipo Appliances para solução de proteção de perímetro, conforme a figura a seguir do diagrama básico de rede, com no mínimo os seguintes requisitos técnicos:

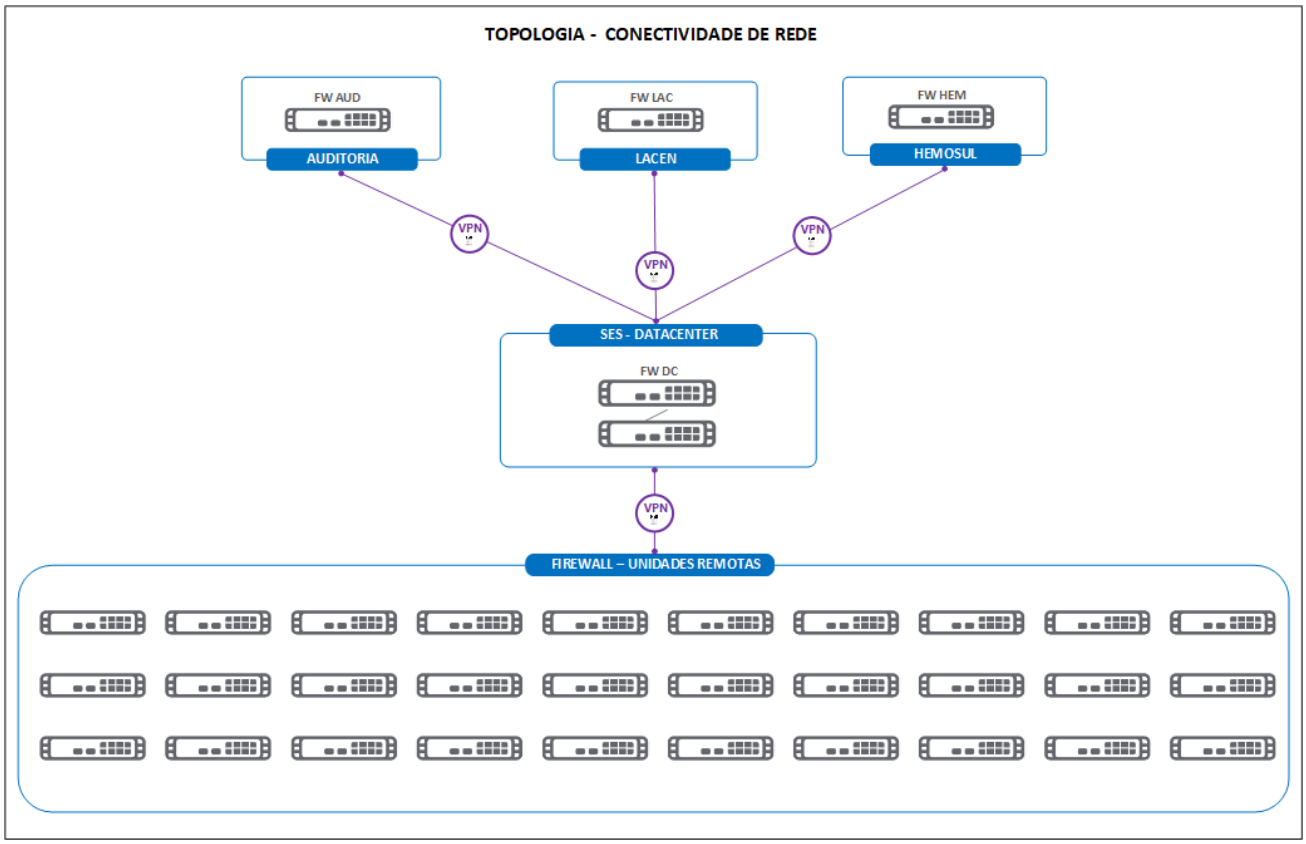



Figura 3 - Diagrama básico de rede

3.3.2.1. 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;

3.3.2.2. Deverá ser fornecido 01 (um) clusters de equipamentos para solução de proteção de perímetro Tipo I, formado por Appliances com no mínimo 02 (dois) nodes cada cluster, para implementação de proteção de perímetro no Data Center da Secretaria de Estado de Saúde de Mato Grosso do Sul.

3.3.2.3. Deverão ser fornecidos 03 (três) equipamentos para solução de proteção de perímetro Tipo II, formado por Appliances, para implementação de proteção de perímetro nas unidades de Auditoria, Lacen e Hemosul, vinculadas à da Secretaria de Estado de Saúde de Mato Grosso do Sul.

3.3.2.4. Deverão ser fornecidos 30 (trinta) equipamentos para solução de proteção de perímetro Tipo III, formado por Appliances, para implementação de proteção de perímetro nas unidades remotas de pequeno porte, vinculadas à da Secretaria de Estado de Saúde de Mato Grosso do Sul.

3.3.2.5. Deverá ser fornecida solução de Firewall de Aplicações Web – Web Application Firewall (WAF), para proteção de pelo menos 200 milhões de requisições WEB por ano, para implementação de proteção de aplicações no Data Center da Secretaria de Estado de Saúde de Mato Grosso do Sul.

3.3.2.6. Deverão ser fornecidos 2.000 (duas mil) licenças para Solução para Proteção de Endpoints, para implementação de proteção Endpoint, que serão instaladas nas estações de trabalho e servidores de rede da Secretaria de Estado de Saúde de Mato Grosso do Sul;

3.3.2.7. Deverão ser fornecidas 250 (duzentos e cinquenta) licenças de Módulo de Detecção e Resposta Gerenciada - MDR para Solução para Proteção de Endpoints.

3.3.3. Requisitos Gerais em Comum para solução de proteção de perímetro

3.3.3.1. A solução deve consistir em plataforma de proteção de rede baseada em Appliance com funcionalidades de Next Generation Firewall. O termo Next Generation Firewall doravante será empregado como NGFW ou simplesmente firewall.

3.3.3.2. Os appliances físicos devem ser novos e de primeiro uso e não constar em listas de *end-of-sale, end-of-support* e *end-of-life* do fabricante;

3.3.3.3. 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;

3.3.3.4. 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;

3.3.3.5. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

3.3.3.6. 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;

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

3.3.3.8. 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;

3.3.3.9. 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;

3.3.3.10. Deve fornece APIs para que os fornecedores externos de NAC possam transmitir o contexto de segurança aos firewalls e que esta funcionalidade seja compatível com a utilização simultânea de fornecedores externos distintos;

3.3.3.11. Os desempenhos apontados nos Requisitos de Capacidade e de Interfaces devem ser comprovados por documento de domínio público do fabricante. 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 documento.

3.3.3.12. 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;

3.3.3.13. Todos os produtos de hardware componentes da solução deverão ser homologados e certificados pela ANATEL, conforme preceitua o art. 19, incisos XIII e XIV, e art. 156 da Lei n. 9.472, de 16 de julho de 1997 e ainda pelos art. 55, art. 64, inciso II e art. 67, parágrafo 2° da Resolução ANATEL n. 715, de 23 de outubro de 2019.

3.3.3.13.1. A Resolução ANATEL nº 715 é um regulamento que estabelece as regras e os procedimentos gerais relativos à certificação e à homologação de produtos para telecomunicação, incluindo a avaliação da conformidade dos produtos para telecomunicação em relação à regulamentação técnica emitida ou adotada pela Anatel e os requisitos para a homologação de produtos para telecomunicação previstos no regulamento.

3.3.3.13.2. Desta forma, velando-se pela legalidade, a SES/MS não poderia admitir a utilização de uma solução que envolve características de tráfego em redes corporativas de comunicação de dados, que não atenda às exigências da ANATEL, o que poderia representar um prejuízo e que certamente estaria sujeito à sustação com o advento de qualquer atividade fiscalizadora da agência de regulação.

3.3.3.14. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.

3.3.4. Requisitos de Capacidade e de Interfaces para solução de proteção de perímetro

3.3.4.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de garantir que a solução ofertada possua: a) capacidade de operação redundante (energia e refrigeração) provendo resiliência e tolerância à falhas; b) processamento, largura de banda e taxa de transferência suficiente para suportar o alto volume de dados trafegados na rede da Secretaria de Estado de Saúde do Estado de Mato Grosso do Sul pelos diversos sistemas e softwares utilizados; e c) a quantidade de interfaces de rede necessárias para suportar toda a arquitetura do ambiente funcional da rede no núcleo da SES/MS, permitindo o devido gerenciamento, monitoramento e operação da solução sem necessidade de adaptações ou equipamentos sobressalentes;

3.3.4.2. Requisitos de Capacidade e de Interfaces para solução de proteção de perímetro Tipo I

3.3.4.2.1. Deve suportar, no mínimo, 27 Gbps de throughput com a funcionalidade de firewall habilitada;

3.3.4.2.2. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 14 Gbps ou superior;

3.3.4.2.3. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 6 Gbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item;

3.3.4.2.4. Desempenho mínimo de 15 Gbps de IPS;

3.3.4.2.5. Suporte mínimo de 4.500.000 conexões simultâneas/concorrente no modo SPI;

3.3.4.2.6. Suporte mínimo de 225.000 novas conexões por segundo;

3.3.4.2.7. Deve permitir armazenamento interno de no mínimo 128 GB e suportar expansão de armazenamento de até 1 TB;

3.3.4.2.8. Deve possuir uma fonte de alimentação "HotSwap" com chaveamento automático de 100-240 VAC redundante;

3.3.4.2.9. Deve possuir 06 interfaces de 10GbE padrão SFP+;

3.3.4.2.10. Deve possuir 02 interfaces 10 GbE padrão RJ-45;

3.3.4.2.11. Deve possuir 24 interfaces 1 GbE padrão RJ-45;

3.3.4.2.12. Deve possuir 01 interface do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento;

3.3.4.2.13. Deve possuir 2 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G;

3.3.4.2.14. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 1.500 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 3.500 usuários simultâneos;

3.3.4.2.15. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 1500 usuários simultâneos;

3.3.4.2.16. Deve suportar 5.000 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos;

3.3.4.2.17. Deve suportar, no mínimo, 14 Gbps de desempenho de VPN IPSEC;

3.3.4.3. Requisitos de Capacidade e de Interfaces para solução de proteção de perímetro Tipo II;

3.3.4.3.1. Deve suportar, no mínimo, 5 Gbps de throughput com a funcionalidade de firewall habilitada;

3.3.4.3.2. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 3.2 Gbps ou superior;

3.3.4.3.3. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 800 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item;

3.3.4.3.4. Desempenho mínimo de 3.5 Gbps de IPS;

3.3.4.3.5. Suporte mínimo de 1.800.000 conexões simultâneas/concorrente no modo SPI;

3.3.4.3.6. Suporte mínimo de 21.000 novas conexões por segundo;

3.3.4.3.7. Deve permitir armazenamento interno de no mínimo 128 GB e suportar expansão de armazenamento de até 256 Gb;

3.3.4.3.8. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC;

3.3.4.3.9. Deve possuir 06 interfaces de 10GbE padrão SFP+;

3.3.4.3.10. Deve possuir 04 interfaces de 5GbE padrão SFP+;

3.3.4.3.11. Deve possuir 24 interfaces 1 GbE padrão RJ-45;

3.3.4.3.12. Deve possuir 01 interface do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento;

3.3.4.3.13. Deve possuir 2 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G;

3.3.4.3.14. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 40 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 500 usuários simultâneos;

3.3.4.3.15. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 400 usuários simultâneos;

3.3.4.3.16. Deve suportar 2.500 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos;

3.3.4.3.17. Deve suportar, no mínimo, 2 Gbps de desempenho de VPN IPSEC;

3.3.4.4. Requisitos de Capacidade e de Interfaces para solução de proteção de perímetro Tipo III;

3.3.4.4.1. Deve suportar, no mínimo, 1,8 Gbps de throughput com a funcionalidade de firewall habilitada;

3.3.4.4.2. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 700 Mbps ou superior;

3.3.4.4.3. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 250 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item;

3.3.4.4.4. Desempenho mínimo de 900 Mbps de IPS;

3.3.4.4.5. Suporte mínimo de 700.000 conexões simultâneas/concorrente no modo SPI;

3.3.4.4.6. Suporte mínimo de 5.000 novas conexões por segundo;

3.3.4.4.7. Deve permitir expansão de armazenamento de até 256 Gb;

3.3.4.4.8. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC;

3.3.4.4.9. Deve possuir 08 interfaces 1 GbE padrão RJ-45;

3.3.4.4.10. Deve possuir 01 interface do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento;

3.3.4.4.11. Deve possuir 02 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G;

3.3.4.4.12. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 3 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 100 usuários simultâneos;

3.3.4.4.13. A VPN SSL deve ser licenciada para, no mínimo, 1 usuário. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 40 usuários simultâneos;

3.3.4.4.14. Deve suportar 50 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos;

3.3.4.4.15. Deve suportar, no mínimo, 700 Mbps de desempenho de VPN IPSEC;

3.3.5. REQUISITOS DE FIREWALL E SD-WAN PARA SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO

3.3.5.1. 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;

3.3.5.2. 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;

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

3.3.5.4. Deve possuir proteção anti-spoofing;

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

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

3.3.5.7. 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;

3.3.5.8. 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;

3.3.5.9. 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:

3.3.5.9.1. Latência;

3.3.5.9.2. Jitter;

3.3.5.9.3. Perda de pacotes;

3.3.5.10. 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;

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

3.3.5.12. A solução de SD-WAN deve permitir encaminhamento de trafego 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;

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

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

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

3.3.5.16. 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;

3.3.5.17. Deve suportar DHCP relay;

3.3.5.18. 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;

3.3.5.19. Deve permitir a utilização de regras de Antivírus, 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;

3.3.5.20. Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (Instant Messenger) incluindo, no mínimo, ICQ, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo;

3.3.5.21. 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;

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

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

3.3.5.24. Detectar e bloquear a origem de portscans;

3.3.5.25. Deve permitir o bloqueio de ataques;

3.3.5.26. Deve permitir o bloqueio de exploits conhecidos;

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

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

3.3.5.29. Implementar DSCP (Differentiated Services Code Points);

3.3.5.30. 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;

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

3.3.5.32. Implementar mecanismo de sincronismo de horário através do protocolo NTP;

3.3.5.33. Possuir suporte ao protocolo SNMP versões 2 e 3;

3.3.5.34. Possuir suporte a log via Syslog;

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

3.3.5.36. 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;

3.3.5.37. Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes;

3.3.5.38. 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;

3.3.5.39. Para tráfego criptografado SSL/TLS, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante;

3.3.5.40. Controle, inspeção e de-criptografia 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;

3.3.5.41. Deve permitir a funcionalidade de ARP bridging;

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

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

3.3.6. Requisitos de VPN (Virtual Private Network) para solução de proteção de perímetro

3.3.6.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade que a solução proporcione recursos de VPN, para interconexão das diversas localidades atendidas de maneira segura, provendo criptografia e sigilosidade no tráfego de dados entre o Data Center da SES, Data Center Estadual vinculado à STI/SETDIG/SEGOV, os demais sites da rede do Governo do Estado de Mato Grosso do Sul e outras instituições como bancos e SERPRO, através de tecnologia usual de mercado e não proprietária;

3.3.6.2. 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;

3.3.6.3. Suportar algoritmos de criptografia 3DES, AES 128, AES 256 e AESGCM16-256;

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

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

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

3.3.6.7. Autenticação via de tuneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site;

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

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

3.3.6.10. 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;

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

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

3.3.6.13. 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;

3.3.6.14. 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;

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

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

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

3.3.7. Requisitos de Alta Disponibilidade para solução de proteção de perímetro

3.3.7.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de garantia da disponibilidade da solução em caso de queda de um dos equipamentos instalados no Data Center da SES/MS, ou seja, a solução deve automaticamente se manter operacional na ocorrência de qualquer evento que ocasione a parada de um dos itens da solução;

3.3.7.2. Os requisitos de Alta Disponibilidade se aplicam somente à solução de proteção de perímetro Tipo I;

3.3.7.3. Devem ser fornecidos 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada;

3.3.7.4. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Passivo, com as implementações de Failover;

3.3.7.5. Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador;

3.3.7.6. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster;

3.3.7.7. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover;

3.3.7.8. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover;

3.3.7.9. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança;

3.3.7.10. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante;

3.3.7.11. A solução de HA deve permitir que o dispositivo primário trate todo o tráfego, mantendo o dispositivo secundário atualizado em tempo real sobre as informações de conexão de rede, garantindo uma transição transparente para o dispositivo secundário em caso de failover, sem que

haja perda das conexões de VPN, FTP, Oracle SQL*NET, RSTP, Real Audio, VPN Client, Dynamic Arp Objects, Informações de DHCP Server, Multicast , IGMP, Usuários ativos, RIP e OSPF;

3.3.8. Requisitos de Controle de Ameaças para solução de proteção de perímetro

3.3.8.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de proteger o ambiente de rede da Secretaria de Estado de Saúde do Estado de Mato Grosso do Sul de ataques dos tipos “vírus” e “botnets”, que podem acarretar na perda de informação crítica, roubo de dados sigilosos, degradação de serviços ou interrupção de funcionamento de sistemas de informações e equipamentos essenciais para continuidade dos serviços públicos prestados, e constituem especificações usuais e padrão de mercado para tecnologias com esta finalidade;

3.3.8.2. 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;

3.3.8.3. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;

3.3.8.4. 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;

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

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

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

3.3.8.8. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;

3.3.8.9. Implementar interface CLI segura através do protocolo SSH;

3.3.8.10. 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;

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

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

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

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

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

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

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

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

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

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

3.3.8.21. 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;

3.3.8.22. 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;

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

3.3.8.24. A solução deve 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;

3.3.9. Requisitos de Proteção Contra-Ataques Avançados para solução de proteção de perímetro

3.3.9.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de proteger o ambiente de rede corporativa de ataques dos tipos “APT Malware”, “ameaças de dia zero” e “ameaças não conhecidas”, através da inspeção avançada de tráfego, inclusive criptografado, detectando anomalias e comportamentos suspeitos de aplicações, e que também podem acarretar na perda de informação crítica, roubo de dados sigilosos, degradação de serviços ou interrupção de funcionamento de sistemas de informações e equipamentos essenciais para continuidade dos serviços públicos prestados, e constituem especificações usuais e padrão de mercado para tecnologias com esta finalidade;

3.3.9.2. 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”;

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

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

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

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

3.3.9.7. 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;

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

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

3.3.9.10. 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;

3.3.9.11. 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;

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

3.3.9.13. 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;

3.3.9.14. Conter ameaças avançadas de dia zero;

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

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

3.3.9.17. 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;

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

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

3.3.9.20. 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;

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

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

3.3.9.23. Implementar mecanismo de pesquisa por diferentes intervalos de tempo;

3.3.9.24. Mitigar ameaças de dia zero via tráfego de internet;

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

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

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

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

3.3.9.29. Conter e mitigar exploits avançados;

3.3.9.30. 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);

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

3.3.9.32. 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;

3.3.9.33. A solução de segurança de Firewalls deverá ter um sistema de inspeção baseado em fluxo que execute análises simultâneas de tráfego de entrada e saída em alta velocidade, sem proxying or buffering;

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

3.3.9.35. A solução deve descriptografar e inspecionar o tráfego criptografado, como HTTPS, SMTPS, NNTPS, etc., sem afetar o desempenho;

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

3.3.9.36.1. Inspeção profunda de memória em tempo real;

3.3.9.36.2. Inspeção profunda de pacotes livre de remontagem;

3.3.9.36.3. Descriptografia e inspeção TLS/SSL;

3.3.9.36.4. Inteligência e controle de aplicativos;

3.3.9.36.5. Recursos SD-WAN seguros;

3.3.10. Requisitos de Filtro de Conteúdo Web para solução de proteção de perímetro

3.3.10.1. Os requisitos mínimos exigidos neste subitem são necessários para prover recurso de controle e gerenciamento de sites Web visitados pelos usuários, proporcionando a criação de políticas de filtragem de conteúdo ilegal, imoral, indevido ou alheio a execução das atividades laborais, garantindo assim conformidade às políticas e normas de segurança e evitando desvios de conduta;

3.3.10.2. 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;

3.3.10.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, Active Directory e base de dados local;

3.3.10.4. 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;

3.3.10.5. Permitir a customização de página de bloqueio;

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

3.3.10.7. Deve permitir submissão de novos sites para categorização;

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

3.3.10.9. 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 de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.

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

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

3.3.11. Requisitos de autenticação para solução de proteção de perímetro

3.3.11.1. Os requisitos mínimos exigidos neste subitem são necessários para garantir autenticidade (controle de acesso), através da autenticação dos usuários da rede, evitando acesso indevido de usuários ou de equipamentos não autorizados às informações trafegadas entre as localidades da

rede corporativa da Secretaria de Estado de Saúde, e especificam tecnologias padrão de mercado e utilizadas no âmbito do parque computacional do Estado;

3.3.11.2. 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;

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

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

3.3.11.5. 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;

3.3.11.6. 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;

3.3.11.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW;

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

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

3.3.11.10. 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;

3.3.11.11. A solução deve possibilitar SSO via API;

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

3.3.12. Requisitos de Administração para solução de proteção de perímetro

3.3.12.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade da equipe técnica da DTI/SES/MS em administrar a solução instalada no Data Center da SES/MS, através de uma interface integrada e com todos os recursos e funcionalidades fornecidos pela solução, com disponibilidade de acesso local e/ou remoto e capacidade de gerenciar a todos os usuários

(colaboradores diretos e terceirizados) que utilizam a rede de dados da Secretaria de Estado de Saúde de Mato Grosso do Sul;

3.3.12.2. 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;

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

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

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

3.3.12.6. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP;

3.3.12.7. 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;

3.3.12.8. 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;

3.3.12.9. 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;

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

3.3.12.11. 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;

3.3.12.12. 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;

3.3.12.13. 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;

3.3.12.14. 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;

3.3.12.15. 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;

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

3.3.12.17. 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);

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

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

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

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

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

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

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

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

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

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

3.3.12.28. 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;

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

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

3.3.13. REQUISITOS DO SOFTWARE DE GERENCIAMENTO E RELATÓRIOS PARA SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO:

3.3.13.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade da equipe técnica da DTI/SES/MS em gerenciar todo o ambiente tecnológico fornecido pela solução nos sites instalados, através de uma interface integrada e com acesso à configuração e ao monitoramento de todos os recursos e funcionalidades fornecidos, com disponibilidade de acesso local e/ou remoto;

3.3.13.2. Deverá ser fornecido em conjunto com a solução, um software de gerenciamento e geração de relatórios de todo o conjunto de equipamentos, com no mínimo as características abaixo:

3.3.13.2.1. Os firewalls devem possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de toda a solução;

3.3.13.2.2. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções;

3.3.13.2.3. O gerenciamento centralizado poderá ser entregue como appliance físico ou appliance virtual, sendo todos do mesmo fabricante dos appliances, não sendo aceita solução de software livre;

3.3.13.2.4. Caso seja entregue em appliance virtual dever ser compatível com VMware ESXi ou Hyper-V ;

3.3.13.2.5. Caso seja entregue em appliance físico, o equipamento deve possuir fonte de chaveamento automático (100-240 VAC), com formato compatível para instalação em rack;

3.3.13.2.6. Deve suportar organizar os dispositivos administrados em grupos;

3.3.13.2.7. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;

3.3.13.2.8. Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

3.3.13.2.9. Deve permitir a centralização da administração de regras e políticas dos firewalls configurados de forma individual e em cluster;

3.3.13.2.10. O gerenciamento deve permitir/possuir:

3.3.13.2.10.1. Criação e administração de políticas de firewall e controle de aplicação;

3.3.13.2.10.2. A solução deve permitir acesso concorrente de administradores;

3.3.13.2.10.3. Deve permitir o provisionamento de configuração por "Zero-Toutch";

3.3.13.2.10.4. Deve permitir a integração com LDAP ou Radius;

3.3.13.2.11. A solução de gerenciamento deverá ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL;

3.3.13.2.12. 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;

3.3.13.2.13. A solução deve possuir tela situacional com todo o inventários de firewalls gerenciados centralizadamente, informando no mínimo para o administrador, nome do Hostname do firewall, número de série, modelo, versão do firmware e status da conectividade do equipamento com a gerência em online ou off-line;

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

3.3.13.2.15. A solução deve possuir Dashboard com sumario de alertas e informação de status de licença;

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

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

3.3.13.2.18. A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão na console de gerência local do firewall sem a necessidade do administrador utilizar endereço IP do dispositivo, URL ou FQDN;

3.3.13.2.19. A solução deve permitir a criação de modelos de configuração ou “Templates” para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls;

3.3.13.2.20. Os modelos de configuração ou “templates” devem suportar configurações de interfaces físicas ou virtuais;

3.3.13.2.21. 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;

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

3.3.13.2.23. De forma centralizada deve permitir gerenciar (mas não se limitando a) políticas de firewall, NAT, rotas, PBR (Policy Based Routing), configurar endereçamento IP das interfaces dos

equipamentos, criar e administrar políticas de IPS, configurar políticas de antivírus e antimalware, configurar e criar políticas de controle de URL, criar e configurar políticas de controle de aplicações, criar e configurar política de SANDBOX, criar e configurar políticas de controle de banda e criar e configurar os objetos necessários para configurar e criar as políticas;

3.3.13.2.24. Deverá possibilitar a criação de políticas SD-WAN, baseando-se em parâmetros de latência, perda de pacote e jitter, para a tomada de decisão de encaminhamento de tráfego no firewall;

3.3.13.2.25. 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;

3.3.13.2.26. Durante a alterações de políticas de segurança dos firewalls, 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;

3.3.13.2.27. Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, esse 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;

3.3.13.2.28. 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;

3.3.13.2.29. A solução deverá permitir visualizar sumario com as informações referentes as principais ameaças protegidas pelos firewalls;

3.3.13.2.30. Deverá suportar logs do tipo Netflow, IPFIX ou Syslog, para a gerar reports;

3.3.13.2.31. O operador da solução de relatórios poderá ter acesso a informações com buscas por um período prédefinido pela solução (última hora, ontem, última semana e último mês) ou customizados para um período específico definido pelo operador;

3.3.13.2.32. A solução deverá prover relatórios referente as atividades dos usuários;

3.3.13.2.33. A solução deverá prover relatórios referente ao uso de aplicações web, com no mínimo as seguintes informações: nome da aplicação, nível de ameaça, quantidade de conexões e quantidade de Megabytes trafegados;

3.3.13.2.34. A solução deverá possuir as informações de "Uptime" dos equipamentos;

3.3.13.2.35. A solução deverá prover relatórios referente ao consumo de rede por endereço IP, com no mínimo as seguintes informações: endereço IP, quantidade de conexões, Usuário, quantidade de Megabytes trafegados e Mac Address de origem;

3.3.13.2.36. A solução deverá prover relatórios referente aos acessos web com no mínimo informações referentes às categorias acessadas, quantitativo de acessos e megabytes transferidos;

3.3.13.2.37. A solução deverá permitir o agendamento para envio de relatórios periódicos, em formato PDF;

3.3.13.2.38. A solução deverá mostrar dados de uso de VPN, informando no mínimo dados como: IP de origem, usuário, conexões e quantidade de dado trafegado;

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

3.3.13.2.39.1. Lista de eventos correlacionados com opção de navegação "drilldown"; ou

3.3.13.2.39.2. Modo gráfico; ou

3.3.13.2.39.3. Lista de logs;

3.3.13.2.40. A solução deve possibilitar a criação de relatórios de uso de VPN.

3.3.14. REQUISITOS DE FIREWALL DE APLICAÇÕES WEB (WAF) PARA SOLUÇÃO DE PROTEÇÃO DE APLICAÇÕES

3.3.14.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade da adotar solução de proteção de aplicações que realize de forma eficiente a mitigação de vulnerabilidades conhecidas, proteção contra ataques comuns como SQL injection, filtragem de scripts maliciosos, bloqueios de inclusão de arquivos maliciosos de forma remota, proteção contra ataques de força bruta, proteção contra bots maliciosos, proteção contra exploits de dia zero e ataques de dia zero, prevenção a vazamento de dados e prevenção de fraudes.

3.3.14.2. Características Gerais

3.3.14.2.1. Suportar as seguintes tecnologias de proteção:

3.3.14.2.1.1. Web Application Protection;

3.3.14.2.1.2. API Security;

3.3.14.2.1.3. Bot Prevention;

3.3.14.2.1.4. Intrusion Prevention (IPS);

3.3.14.2.1.5. File Security;

3.3.14.2.2. A solução deve permitir uma quantidade ilimitada de aplicações ou largura de banda, uma vez que a solução fornecerá proteção a diferentes ambientes WEB e API e o número dessas

aplicações é muito dinâmico, bem como a quantidade de largura de banda e sua localização (nuvem/on-premise);

3.3.14.2.3. A solução deve, em conjunto, fornecer proteção de pelo menos 200 milhões de requisições WEB por ano;

3.3.14.2.4. A solução deve ser capaz de evitar ataques cibernéticos conhecidos e desconhecidos;

3.3.14.2.5. A implementação deve ser flexível e pode ser realizada em diferentes ambientes na nuvem e on-premises;

3.3.14.2.6. A solução deve ser gerenciada a partir de um portal em nuvem;

3.3.14.2.7. A solução deve ser capaz de proteger aplicações em diferentes ambientes e em qualquer arquitetura (on-premise, cloud, containers) gerenciada a partir de um único portal centralizado;

3.3.14.2.8. A solução deve ser capaz de analisar cada solicitação recebida, e esta solicitação deve ser analisada em contexto;

3.3.14.2.9. A solução deve ser capaz de realizar análise de risco, examinando parâmetros como:

3.3.14.2.9.1. Perfil do usuário;

3.3.14.2.9.2. Padrões observados na sessão do usuário;

3.3.14.2.9.3. A forma como outros usuários normalmente interage com a aplicação;

3.3.14.2.10. A solução deve fazer inspeção através de análise comportamental usando atributos como: reputação do usuário, conhecimento da aplicação e indicadores. Ou seja, a solução não deve ser baseada totalmente em assinaturas;

3.3.14.2.11. Deve ser capaz de se adaptar automaticamente às alterações da aplicação, analisando continuamente o perfil do usuário, aplicação e conteúdo;

3.3.14.2.12. A solução deve ser capaz de bloquear os seguintes tipos de ataques:

3.3.14.2.12.1. Cross Site Request Forgery;

3.3.14.2.12.2. XML External Entity;

3.3.14.2.12.3. Remote Code Execution;

3.3.14.2.12.4. Evasion Techniques;

3.3.14.2.12.5. LDAP Injection;

3.3.14.2.12.6. Path Traversal;

3.3.14.2.12.7. Vulnerability Scanning;

3.3.14.2.12.8. SQL Injection;

3.3.14.2.12.9. Métodos HTTP ilegais;

3.3.14.2.12.10. Entrada inválida para formulários;

3.3.14.2.12.11. Scraping Brute Force Attacks;

3.3.14.2.12.12. Pelo menos 2800 CVEs específicos da Web;

3.3.14.2.13. A solução deve ser capaz de configurar exceções como:

3.3.14.2.13.1. Uma expressão regular que determina o URI que deve coincidir. Por exemplo: /login/*;

3.3.14.2.13.2. Expressão regular e CIDR que determina o identificador de origem que deve corresponder. Por exemplo: 192.168.24.0/24 ou. * @ xxxx.com);

3.3.14.2.13.3. Um CIDR que determina o IP de origem física que deve coincidir. Por exemplo: 192.168.24.0/16;

3.3.14.2.13.4. Uma expressão regular que determina o nome do parâmetro que deve coincidir. Por exemplo: * Senha. *;

3.3.14.2.13.5. Uma expressão regular que determina o nome do parâmetro que deve coincidir. Por exemplo: ^ 4 [0-9] {12} (?: [0-9] {3})? $);

3.3.14.2.13.6. Um indicador que deve coincidir. Se necessário, usar uma lista separada por vírgulas;

3.3.14.2.14. A solução deve ser capaz de configurar exceções e modificar as ações tomadas pela ferramenta por padrão, e deve permitir a aceitação ou bloqueio do tráfego quando corresponder a algumas das condições mencionadas;

3.3.14.2.15. A solução deve permitir upload de certificados para proteger sites HTTPS da instituição.

3.3.14.2.16. A solução precisará incluir um mecanismo de aprendizagem que ajude a diminuir o número de eventos críticos e altos ao longo do tempo à medida que aprende o tráfego do site e entende o comportamento do usuário;

3.3.14.2.17. O aprendizado da solução deve funcionar continuamente e não apenas ter um "modo de aprendizagem";

3.3.14.2.18. A solução precisará classificar cada solicitação e decidir suas possibilidades de ataque através de um mecanismo inteligente de inteligência artificial;

3.3.14.2.19. As políticas de solução devem ser capazes de operar em pelo menos os seguintes modos:

3.3.14.2.19.1. Prevenção;

3.3.14.2.19.2. Aprendizado/Detecção;

3.3.14.2.19.3. Desabilitado;

3.3.14.2.20. A solução deve incluir políticas predefinidas que sejam práticas recomendadas (ou a prática recomendada pelo fabricante). Essas políticas devem ser editáveis, se necessário.

3.3.14.2.21. A solução deve ser capaz de ser instalada em diferentes ambientes, alguns atualmente implementados na instituição e outros que serão implementados no futuro, pelo menos ela deve ser capaz de ser instalado em:

3.3.14.2.21.1. Contêineres: Docker, Kubernetes, Kubernetes Ingress;

3.3.14.2.21.2. Um agente que funciona em NGINX Web Server ou em um proxy reverso NGINX;

3.3.14.2.21.3. Cloud: Amazon Web Services (AWS), Microsoft Azure, VMware;

3.3.14.2.22. A solução deve permitir que você aplique políticas para definir limites em mensagens de protocolo HTTP. Inclua pelo menos os seguintes parâmetros:

3.3.14.2.22.1. Tamanho do corpo — tamanho máximo do corpo da mensagem HTTP;

3.3.14.2.22.2. Tamanho do URL — Tamanho máximo de URL, isso inclui todos os campos de consulta;

3.3.14.2.22.3. Tamanho do cabeçalho (Header Size): tamanho máximo do cabeçalho HTTP;

3.3.14.2.22.4. Profundidade máxima do objeto: Tamanho máximo de profundidade do objeto JSON/XML, isso inclui XML incorporado no JSON e o oposto.;

3.3.14.2.22.5. Métodos de HTTP Válidos (RFP): Aceitar ou bloquear métodos http não padrão;

3.3.14.2.23. A solução deve suportar métodos para ser capaz de distinguir os usuários uns dos outros. Ele deve suportar pelo menos os seguintes mecanismos:

3.3.14.2.23.1. X-Forwarded-For;

3.3.14.2.23.2. IP Origem;

3.3.14.2.23.3. Cookie;

3.3.14.2.23.4. Header Only;

3.3.14.3. API Protection

3.3.14.3.1. A solução deve fornecer proteção proativa para potenciais vulnerabilidades de API através de um procedimento de validação de esquema;

3.3.14.3.2. A solução deve ser capaz de proteger APIs usando técnicas como validação automatizada usando arquivos de esquema OpenAPI;

3.3.14.3.3. Deve proteger pelo menos REST API e GraphQL;

3.3.14.3.4. Oferecer dois modelos de proteção:

3.3.14.3.4.1. O modelo positivo oferece proteção preventiva para possíveis vulnerabilidades de API por meio de um procedimento de validação de esquema. As solicitações de API recebidas são validadas nesses esquemas para bloquear todas as solicitações de API inválidas;

3.3.14.3.4.2. Baseado em aprendizado de máquina e detecta e bloqueia automaticamente payloads maliciosos na API;

3.3.14.3.5. A solução deve fornecer descoberta de API, fornecendo segurança por visibilidade. Deve fornecer esquema da API (API schema), conforme aprendido pelo mecanismo de descoberta de API, e análise do uso da API. A análise periódica das descobertas permite que o administrador de segurança acompanhe o rápido processo de desenvolvimento das APIs do servidor web, sem comprometer sua segurança;

3.3.14.3.6. O mecanismo de descoberta deve gerar os esquemas da API baseado em versão/revisão, e deve ser possível comparar as versões, para identificar alterações no esquema.

3.3.14.3.7. O mecanismo de aprendizado na descoberta deve:

3.3.14.3.7.1. Detectar a utilização de API usando aprendizado de máquina iterativo mecanismo que detecta o uso de APIs (uma combinação do método e do endpoint usado na solicitação). Vários endpoints diferentes podem ser unidos neste estágio a uma única API usando parâmetros do caminho utilizado;

3.3.14.3.8. Deve possuir mecanismo que analisa mais detalhadamente os parâmetros de consulta e o corpo da solicitação da API, para construir o esquema exato para cada API derivado de várias solicitações feitas a ela. Nesta fase, o uso de dados confidenciais também é detectado para cada API;

3.3.14.3.9. Deve fornecer validação de esquema de API – Assim há uma prevenção de tráfego que não esteja em conformidade com o esquema aprovado para as APIs do ativo de API Web. Para definição do uso do esquema da API, deverá suportar:

3.3.14.3.9.1. Deve prover mecanismo de descoberta, permitindo que o esquema continue a ser mantido e revisado, desta forma novas adições criarão versões deste esquema e que serão sugeridas para aprovação do administrador de segurança;

3.3.14.3.9.2. Deve ser possível usar o mecanismo de descoberta da API como base de aprendizado de como a API funciona, e prover possibilidade de alterações manuais;

3.3.14.3.9.3. Um arquivo de esquema aprovado, mantido e criado por seus próprios processos de desenvolvimento;

3.3.14.3.9.4. A descoberta de API ainda pode ser usada para revisar alterações sugeridas de acordo com o tráfego enviado ao servidor web e passando pela ferramenta de segurança;

3.3.14.3.10. A descoberta de API, deve identificar pelo menos os seguintes dados sensíveis que passam pela API:

3.3.14.3.10.1. UUID – Identificador Único universal;

3.3.14.3.10.2. Números de cartão de crédito;

3.3.14.3.10.3. Email;

3.3.14.3.10.4. IP e MAC Address;

3.3.14.3.10.5. Número de telefone;

3.3.14.3.10.6. IBAN;

3.3.14.3.10.7. Certificados;

3.3.14.3.10.8. Chave SSH;

3.3.14.3.11. A solução deverá utilizar mecanismo de inteligência artificial para indicar quando mover a API que foi descoberta para o método de prevenção;

3.3.14.3.12. A solução deve prover sugestões de ajuste na prevenção de anomalias/requisições para a API, está sugestão deve ser baseada no modelo Machine Learning, onde indicara a revisão de determinados eventos. Isso permite que o mecanismo de aprendizado de máquina atinja um nível de maturidade mais alto e, portanto, uma melhor precisão com mais rapidez com base na orientação humana, se necessário;

3.3.14.3.13. Deve possuir um dashboard observar todos os Endpoints relacionados;

3.3.14.4. Características Adicionais:

3.3.14.4.1. A solução precisará ser capaz de injetar scripts em páginas de aplicações Web, como páginas de login, ou usar algum outro mecanismo para coletar dados sobre padrões de entrada e sequências de digitação, movimentos do mouse. Isso para ser capaz de diferenciar um humano de um bot;

3.3.14.4.2. A solução deve ser capaz de identificar esses padrões no caso de um bot usá-los;

3.3.14.4.3. A solução deve ser capaz de tomar uma decisão se a entrada é inserida por um humano ou por um script automático (como um bot) e bloquear essa atividade;

3.3.14.4.4. O recurso IPS precisará fornecer proteções tradicionais baseadas em assinaturas para pelo menos 2800 CVEs baseados na Web (vulnerabilidades e exposições comuns);

3.3.14.4.5. A solução deve permitir criar regras de DLP (Data Loss Prevention), com o uso de assinaturas baseadas em expressões regulares customizadas;

3.3.14.4.6. A solução deve permitir criar assinaturas personalizadas de DLP com base em expressões regulares/REGEX;

3.3.14.4.7. A solução deve identificar e controlar o rate limit de requisições para as aplicações protegidas;

3.3.14.4.8. A solução deverá ter capacidade de controlar o rate limit com no mínimo os seguintes modos de operação, Ativo, Detecção/Aprendizado e modo Inativo;

3.3.14.4.9. A solução deverá ser capaz de analisar arquivos enviados para as aplicações protegidas;

3.3.14.4.10. A solução deverá ser capaz de validar a reputação dos arquivos submetidos para as aplicações classificados como malware;

3.3.14.4.11. A solução deverá ter capacidade de escanear arquivos compactados, permitindo definir limites de tamanho máximo de escaneamento;

3.3.14.4.12. A solução deverá analisar os arquivos em Sandboxing com no mínimo os seguintes tipos de arquivos, Word, Excel, PowerPoint, PDF e executáveis;

3.3.14.4.13. A solução de gerência deve ser baseada em nuvem ou através de appliance dedicado do próprio fabricante, não sendo soluções baseada em servidores abertos;

3.3.14.4.14. A gerência deve possuir visibilidade de todos os eventos de segurança e auditoria;

3.3.14.4.15. Deve gerenciar e administrar de forma centralizada, todas as soluções de proteção para aplicação do mesmo fabricante desde que não sejam software livre;

3.3.14.4.16. O licenciamento para armazenamento da solução deve suportar escalabilidade no volume de logs;

3.3.14.4.17. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pela solução de segurança;

3.3.14.4.18. Centralizar a administração de regras e políticas da solução de segurança, usando uma única interface de gerenciamento;

3.3.14.4.19. Deve permitir a visualização dos logs de uma regra específica na mesma tela de configuração da regra selecionada;

3.3.14.4.20. Suportar geração de logs de auditoria, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

3.3.14.4.21. A solução de gerência deve apresentar eventos em um único portal (dashboard), de todas as funcionalidades de segurança que estão ativadas. Sendo que deve possuir telas de apresentação onde consta todo os principais eventos de forma consolidada como: atividades maliciosas, linha do tempo dos principais incidentes, estatísticas das aplicações protegidas (assets), severidade dos ataques;

3.3.14.4.22. A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução;

3.3.14.4.23. Deve permitir a criação de filtros nos eventos encontrados, tais como a severidade do evento, nome da aplicação protegida, ação, tipo do ataque, origem, método HTTP, HTTP host e HTTP URI path;

3.3.14.4.24. A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

3.3.14.4.24.1. Visualizar quantidade de tráfego realizados nas aplicações;

3.3.14.4.24.2. Gráficos com principais eventos de segurança;

3.3.14.4.25. A solução deve notificar o administrador classificando a severidade do evento;

3.3.14.4.26. A notificação deve conter informações de forma clara, para que permita o administrador tomar uma ação para remediar o incidente ocorrido;

3.3.15. REQUISITOS TÉCNICOS PARA SOLUÇÃO PARA PROTEÇÃO DE ENDPOINTS

3.3.15.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de a solução possuir recursos mínimos de proteção de nível empresarial, contra ameaças de vírus, malwares, Worms, Backdoors, Ransomware, além de diversas ameaças virtuais existentes, para proteção do ambiente de rede corporativa da Secretaria de Estado de Saúde de Mato Grosso do Sul.

3.3.15.2. Requisitos Gerais

3.3.15.2.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:

3.3.15.2.1.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados;

3.3.15.2.2. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência;

3.3.15.2.3. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI);

3.3.15.2.4. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender;

3.3.15.2.5. A solução proposta deve suportar o subsistema Linux no Windows;

3.3.15.2.6. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

3.3.15.2.6.1. Proteção contra ameaças sem arquivos (Fileless);

3.3.15.2.6.2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

3.3.15.2.7. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;

3.3.15.2.8. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux;

3.3.15.2.9. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados;

3.3.15.2.10. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra-ataques remotos de criptografia;

3.3.15.2.11. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows;

3.3.15.2.12. A solução proposta deve fornecer análise comportamental baseada em machine learning;

3.3.15.2.13. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento;

3.3.15.2.14. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:

3.3.15.2.14.1. Controles de aplicativos;

3.3.15.2.14.2. Controle web e dispositivos;

3.3.15.2.14.3. HIPS e Firewall;

3.3.15.2.14.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;

3.3.15.2.14.5. Gerenciamento de criptografia de arquivos e discos;

3.3.15.2.14.6. Controle adaptativo para detecção de anomalias;

3.3.15.2.15. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor;

3.3.15.2.16. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema;

3.3.15.2.17. A solução proposta deve ter bancos de dados de reputação locais e globais;

3.3.15.2.18. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares;

3.3.15.2.19. A solução proposta deve incluir um módulo capaz, no mínimo, de:

3.3.15.2.19.1. Bloqueio de aplicativos com base em sua categorização;

3.3.15.2.19.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos;

3.3.15.2.19.3. A adição de sub-redes e a modificação de permissões de atividade;

3.3.15.2.20. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização;

3.3.15.2.21. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção;

3.3.15.2.22. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça;

3.3.15.2.23. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:

3.3.15.2.23.1. Modo silencioso;

3.3.15.2.23.2. Discos rígidos e dispositivos removíveis;

3.3.15.2.23.3. De todos as contas de usuários do dispositivo;

3.3.15.2.24. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:

3.3.15.2.24.1. Exclusão imediata de dados;

3.3.15.2.24.2. Exclusão de dados adiada;

3.3.15.2.25. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:

3.3.15.2.25.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;

3.3.15.2.25.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão;

3.3.15.2.26. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho;

3.3.15.2.27. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas;

3.3.15.2.28. A solução proposta deve incluir proteção contra-ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo;

3.3.15.2.29. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de

computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário;

3.3.15.2.30. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem;

3.3.15.2.31. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas;

3.3.15.2.32. A solução proposta deve ser capaz de descriptografar e verificar o tráfego de rede transmitido por conexões criptografadas;

3.3.15.2.33. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;

3.3.15.2.34. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;

3.3.15.2.35. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint;

3.3.15.2.36. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem;

3.3.15.2.37. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada;

3.3.15.2.38. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa;

3.3.15.2.39. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior;

3.3.15.2.40. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda;

3.3.15.2.41. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint;

3.3.15.2.42. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos;

3.3.15.2.43. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos;

3.3.15.2.44. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo;

3.3.15.2.45. A solução proposta deve ter categoria de detecção para bloquear banners de sites;

3.3.15.2.46. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;

3.3.15.2.47. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos;

3.3.15.2.48. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais;

3.3.15.2.49. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP;

3.3.15.2.50. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

3.3.15.2.51. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões;

3.3.15.2.52. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos;

3.3.15.2.53. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem;

3.3.15.2.54. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração;

3.3.15.2.55. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões;

3.3.15.2.56. A solução proposta deve suportar o controle de scripts executados em PowerShell.

3.3.15.2.57. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados;

3.3.15.2.58. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo;

3.3.15.2.59. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem;

3.3.15.2.60. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor;

3.3.15.2.61. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas;

3.3.15.2.62. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint;

3.3.15.2.63. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:

3.3.15.2.63.1. Filtro de anexos;

3.3.15.2.63.2. Verificação de mensagens de e-mail ao receber, ler e enviar;

3.3.15.2.64. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo;

3.3.15.2.65. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;

3.3.15.2.66. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);

3.3.15.2.67. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware;

3.3.15.2.68. A solução proposta deve fornecer proteção contra-ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio;

3.3.15.2.69. A solução proposta deve incluir suporte ao protocolo IPv6;

3.3.15.2.70. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente;

3.3.15.2.71. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

3.3.15.2.71.1. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo;

3.3.15.2.71.2. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários;

3.3.15.2.72. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar;

3.3.15.2.73. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha;

3.3.15.2.74. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística;

3.3.15.2.75. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail;

3.3.15.2.76. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária;

3.3.15.2.77. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows;

3.3.15.2.78. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados;

3.3.15.2.79. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia, bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça;

3.3.15.2.80. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft;

3.3.15.2.81. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização;

3.3.15.2.82. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.

3.3.15.2.83. A solução proposta deve suportar endereços IPv6;

3.3.15.2.84. A solução proposta deve suportar verificação em duas etapas (autenticação);

3.3.15.2.85. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento;

3.3.15.2.86. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração;

3.3.15.2.87. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente;

3.3.15.2.88. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes;

3.3.15.2.89. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware;

3.3.15.2.90. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas;

3.3.15.2.91. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas;

3.3.15.2.92. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos;

3.3.15.2.93. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet;

3.3.15.2.94. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor;

3.3.15.2.95. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes;

3.3.15.2.96. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS;

3.3.15.2.97. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentena em todos os recursos da rede onde o sensor de endpoint está instalado;

3.3.15.2.98. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração;

3.3.15.2.99. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos;

3.3.15.2.100. A solução proposta deve ter a capacidade de excluir atualizações baixadas;

3.3.15.2.101. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados;

3.3.15.2.102. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português;

3.3.15.2.103. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints;

3.3.15.2.104. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos;

3.3.15.2.105. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou;

3.3.15.2.106. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor;

3.3.15.2.107. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional;

3.3.15.2.108. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor;

3.3.15.2.109. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

3.3.15.2.109.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível;

3.3.15.2.109.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica;

3.3.15.2.110. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados;

3.3.15.2.111. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado;

3.3.15.2.112. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:

3.3.15.2.112.1. Ajuda on-line para administradores;

3.3.15.2.112.2. Ajuda on-line para melhores práticas de implementação;

3.3.15.2.112.3. Ajuda on-line para proteção de servidores de administração;

3.3.15.2.113. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware;

3.3.15.2.114. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

3.3.15.3. DO MÓDULO DE PROTEÇÃO DE ENDPOINT

3.3.15.3.1. A solução proposta deverá proteger os sistemas operacionais abaixo:

3.3.15.3.1.1. Windows 7;

3.3.15.3.1.2. Windows 8;

3.3.15.3.1.3. Windows 8.1;

3.3.15.3.1.4. Windows 10;

3.3.15.3.1.5. Windows 11;

3.3.15.3.2. Servidores

3.3.15.3.2.1. Windows Small Business Server 2011;

3.3.15.3.2.2. Windows MultiPoint Server 2011;

3.3.15.3.2.3. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022;

3.3.15.3.3. Servidores de terminal Microsoft

3.3.15.3.3.1. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022;

3.3.15.3.4. Sistemas operacionais Linux de 32 bits:

3.3.15.3.4.1. CentOS 6.7 e posterior;

3.3.15.3.4.2. Debian GNU/Linux 11.0 e posterior;

3.3.15.3.4.3. Debian GNU/Linux 12.0 e posterior;

3.3.15.3.4.4. Red Hat Enterprise Linux 6.7 e posterior;

3.3.15.3.5. Sistemas operacionais Linux de 64 bits:

3.3.15.3.5.1. Amazon Linux 2;

3.3.15.3.5.2. CentOS 6.7 e posterior;

3.3.15.3.5.3. CentOS 7.2 e posterior;

3.3.15.3.5.4. CentOS Stream 8;

3.3.15.3.5.5. CentOS Stream 9;

3.3.15.3.5.6. Debian GNU/Linux 11.0 e posterior;

3.3.15.3.5.7. Debian GNU/Linux 12.0 e posterior;

3.3.15.3.5.8. Linux Mint 20.3 e superior;

3.3.15.3.5.9. Linux Mint 21.1 e posterior;

3.3.15.3.5.10. OpenSUSE Leap 15.0 e posterior;

3.3.15.3.5.11. Oracle Linux 7.3 e posterior;

3.3.15.3.5.12. Oracle Linux 8.0 e posterior;

3.3.15.3.5.13. Oracle Linux 9.0 e posterior;

3.3.15.3.5.14. Red Hat Enterprise Linux 6.7 e posterior;

3.3.15.3.5.15. Red Hat Enterprise Linux 7.2 e posterior;

3.3.15.3.5.16. Red Hat Enterprise Linux 8.0 e posterior;

3.3.15.3.5.17. Red Hat Enterprise Linux 9.0 e posterior;

3.3.15.3.5.18. Rocky Linux 8.5 e posterior;

3.3.15.3.5.19. Rocky Linux 9.1;

3.3.15.3.5.20. SUSE Linux Enterprise Server 12.5 ou posterior;

3.3.15.3.5.21. SUSE Linux Enterprise Server 15 ou posterior;

3.3.15.3.5.22. Ubuntu 20.04 LTS;

3.3.15.3.5.23. Ubuntu 22.04 LTS;

3.3.15.3.5.24. Sistemas operacionais Arm de 64 bits;

3.3.15.3.5.25. CentOS Stream 9;

3.3.15.3.5.26. SUSE Linux Enterprise Server 15;

3.3.15.3.5.27. Ubuntu 22.04 LTS;

3.3.15.3.6. Sistemas operacionais MAC OS:

3.3.15.3.6.1. MacOS 12 – 14;

3.3.15.3.7. Ferramentas de virtualização MAC OS:

3.3.15.3.7.1. Parallels Desktop 16 para Mac Business Edition;

3.3.15.3.7.2. VMware Fusion 11.5 Professional;

3.3.15.3.7.3. VMware Fusion 12 Professional;

3.3.15.3.8. A solução proposta deverá suportar as seguintes plataformas virtuais:

3.3.15.3.8.1. VMware Workstation 17.0.2 Pro;

3.3.15.3.8.2. VMware ESXi 8.0 Update 2;

3.3.15.3.8.3. Microsoft Hyper-V Server 2019;

3.3.15.3.8.4. Citrix Virtual Apps e Desktop 7 2308;

3.3.15.3.8.5. Citrix Provisioning 2308Citrix Hypervisor 8.2 Update 1;

3.3.15.4. DO MÓDULO DE GERENCIAMENTO AVANÇADO

3.3.15.4.1. A solução proposta deve suportar arquitetura cloud-native e on-premisse;

3.3.15.4.2. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:

3.3.15.4.2.1. Amazon Web Services;

3.3.15.4.2.2. Microsoft Azure;

3.3.15.4.3. A solução proposta deve incluir as seguintes opções de integração SIEM:

3.3.15.4.3.1. HP (Microfoco) ArcSight;

3.3.15.4.3.2. IBM QRadar;

3.3.15.4.3.3. Splunk;

3.3.15.4.3.4. Kaspersky KUMA;

3.3.15.4.4. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes;

3.3.15.4.5. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

3.3.15.4.6. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos;

3.3.15.4.7. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede;

3.3.15.4.8. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros;

3.3.15.4.9. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador;

3.3.15.4.10. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento;

3.3.15.4.11. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização;

3.3.15.4.12. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis;

3.3.15.4.13. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem;

3.3.15.4.14. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que

possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

3.3.15.4.14.1. Status do dispositivo;

3.3.15.4.14.2. Tag;

3.3.15.4.14.3. Diretório ativo;

3.3.15.4.14.4. Proprietários de dispositivos;

3.3.15.4.14.5. Hardware;

3.3.15.4.15. A solução proposta deve suportar os seguintes canais de entrega de notificação:

3.3.15.4.15.1. E-mail;

3.3.15.4.15.2. Registro de sistema;

3.3.15.4.15.3. SMS;

3.3.15.4.16. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

3.3.15.4.16.1. Atributos de rede;

3.3.15.4.16.2. Nome;

3.3.15.4.16.3. Domínio e/ou Sufixo de Domínio;

3.3.15.4.16.4. Endereço de IP;

3.3.15.4.16.5. Endereço IP para servidor de gerenciamento;

3.3.15.4.16.6. Localização no Active Directory;

3.3.15.4.16.7. Unidade organizacional;

3.3.15.4.16.8. Grupo;

3.3.15.4.16.9. Sistema operacional:

3.3.15.4.16.9.1. Número do pacote de serviço;

3.3.15.4.16.9.2. Arquitetura Virtual;

3.3.15.4.16.9.3. Registro de aplicativos;

3.3.15.4.16.9.4. Nome da Aplicação;

3.3.15.4.16.9.5. Versão do aplicativo;

3.3.15.4.16.9.6. Fabricante;

3.3.15.4.16.9.7. Tipo e versão;

3.3.15.4.16.9.8. Arquitetura;

3.3.15.4.17. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão;

3.3.15.4.18. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública;

3.3.15.4.19. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

3.3.15.4.19.1. Dispositivos Desktop/Servidores;

3.3.15.4.19.2. Dispositivos móveis;

3.3.15.4.19.3. Dispositivos de rede;

3.3.15.4.19.4. Dispositivos virtuais;

3.3.15.4.19.5. Componentes OEM;

3.3.15.4.19.6. Periféricos de computador;

3.3.15.4.19.7. Dispositivos IoT conectados;

3.3.15.4.19.8. Telefones VoIP;

3.3.15.4.19.9. Repositórios de rede;

3.3.15.4.20. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

3.3.15.4.20.1. Nome da Aplicação;

3.3.15.4.20.2. Caminho do aplicativo;

3.3.15.4.20.3. Metadados do aplicativo;

3.3.15.4.20.4. Aplicativo Certificado digital;

3.3.15.4.20.5. Categorias de aplicativos predefinidas pelo fornecedor;

3.3.15.4.20.6. SHA256 e MD5;

3.3.15.4.21. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

3.3.15.4.21.1. Bluetooth;

3.3.15.4.21.2. Dispositivos móveis;

3.3.15.4.21.3. Modems externos;

3.3.15.4.21.4. CD/DVD;

3.3.15.4.21.5. Câmeras e scanners;

3.3.15.4.21.6. MTPs;

3.3.15.4.21.7. E a transferência de dados para dispositivos móveis;

3.3.15.4.22. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização;

3.3.15.4.23. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão;

3.3.15.4.24. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

3.3.15.4.24.1. Estruturas de domínios e grupos de trabalho do Windows;

3.3.15.4.24.2. Estruturas de grupos do Active Directory;

3.3.15.4.24.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador;

3.3.15.4.25. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização;

3.3.15.4.26. A solução proposta deve permitir realizar as seguintes ações para endpoints:

3.3.15.4.26.1. Verificação manual;

3.3.15.4.26.2. Verificação no acesso;

3.3.15.4.26.3. Verificação por demanda;

3.3.15.4.26.4. Verificação de arquivos compactados;

3.3.15.4.26.5. Verificação de arquivos individuais, pastas e unidades;

3.3.15.4.26.6. Bloqueio e verificação de scripts;

3.3.15.4.26.7. Proteção contra alteração de registros;

3.3.15.4.26.8. Proteção contra estouro de buffer;

3.3.15.4.26.9. Verificação em segundo plano/inativa;

3.3.15.4.27. Verificação de unidade removível na conexão com o sistema;

3.3.15.4.28. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware;

3.3.15.4.29. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas;

3.3.15.4.30. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade;

3.3.15.4.31. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc;

3.3.15.4.32. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração;

3.3.15.4.33. A solução proposta deve suportar Windows Failover Cluster;

3.3.15.4.34. A solução proposta deve ter um recurso de clustering integrado;

3.3.15.4.35. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus;

3.3.15.4.36. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia;

3.3.15.4.37. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança;

3.3.15.4.38. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo;

3.3.15.4.39. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux;

3.3.15.4.40. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB;

3.3.15.4.41. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB;

3.3.15.4.42. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes;

3.3.15.4.43. A solução proposta deverá possuir controles para download de DLL e drivers;

3.3.15.4.44. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão;

3.3.15.4.45. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável;

3.3.15.4.46. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log);

3.3.15.4.47. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server;

3.3.15.4.48. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory;

3.3.15.4.49. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las;

3.3.15.4.50. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior;

3.3.15.4.51. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários;

3.3.15.4.52. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração;

3.3.15.4.53. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários;

3.3.15.4.54. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail;

3.3.15.4.55. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados;

3.3.15.4.56. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração;

3.3.15.4.57. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal;

3.3.15.4.58. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc;

3.3.15.4.59. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada

automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis;

3.3.15.4.60. A solução proposta deve permitir ao administrador personalizar relatórios;

3.3.15.4.61. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado;

3.3.15.4.62. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor;

3.3.15.4.63. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento;

3.3.15.4.64. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento;

3.3.15.4.65. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico;

3.3.15.4.66. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos;

3.3.15.4.67. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;

3.3.15.4.68. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários;

3.3.15.4.69. A solução proposta deve suportar integração com solução APT;

3.3.15.4.70. A solução proposta deve suportar a integração com o serviço Managed Detection and Response;

3.3.15.4.71. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:

3.3.15.4.71.1. Windows;

3.3.15.4.71.2. Linux;

3.3.15.4.72. A solução proposta deverá suportar os seguintes servidores de banco de dados:

3.3.15.4.72.1. Windows;

3.3.15.4.72.2. Microsoft SQL Server;

3.3.15.4.72.3. Microsoft Banco de dados SQL do Azure;

3.3.15.4.72.4. MySQL Standard e Enterprise;

3.3.15.4.72.5. MariaDB;

3.3.15.4.72.6. PostgreSQL;

3.3.15.4.72.7. Linux:

3.3.15.4.72.7.1. MySQL;

3.3.15.4.72.7.2. MariaDB;

3.3.15.4.72.7.3. PostgreSQL;

3.3.15.4.73. A solução proposta deverá suportar as seguintes plataformas virtuais:

3.3.15.4.73.1. Windows:

3.3.15.4.73.2. VMware vSphere 6.7 e 7.0;

3.3.15.4.73.3. Estação de trabalho VMware 16 Pro;

3.3.15.4.73.4. Servidor Microsoft Hyper-V 2012 de 64 bits;

3.3.15.4.73.5. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;

3.3.15.4.73.6. Microsoft Servidor Hyper -V 2016 de 64 bits;

3.3.15.4.73.7. Servidor Microsoft Hyper-V 2019 de 64 bits;

3.3.15.4.73.8. Servidor Microsoft Hyper-V 2022 de 64 bits;

3.3.15.4.73.9. Citrix XenServer 7.1 LTSR;

3.3.15.4.73.10. Citrix XenServer 8.x;

3.3.15.4.73.11. Oracle VM VirtualBox 6.x;

3.3.15.4.74. Linux:

3.3.15.4.74.1. VMware vSphere 6.7, 7.0 e 8.0;

3.3.15.4.74.2. Estação de trabalho VMware 16 Pro e 17 Pro;

3.3.15.4.74.3. Servidor Microsoft Hyper-V 2012 de 64 bits;

3.3.15.4.74.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;

3.3.15.4.74.5. Microsoft Servidor Hyper -V 2016 de 64 bits;

3.3.15.4.74.6. Servidor Microsoft Hyper-V 2019 de 64 bits;

3.3.15.4.74.7. Servidor Microsoft Hyper-V 2022 de 64 bits;

3.3.15.4.74.8. Citrix XenServer 7.1 e 8.x;

3.3.15.4.74.9. Oracle VM VirtualBox 6.x e7.x;

3.3.15.4.75. A solução proposta deve suportar criptografia em vários níveis:

3.3.15.4.75.1. Criptografia completa do disco – incluindo disco do sistema;

3.3.15.4.75.2. Criptografia de arquivos e pastas;

3.3.15.4.75.3. Criptografia de mídia removível;

3.3.15.4.75.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2;

3.3.15.4.76. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:

3.3.15.4.76.1. A criptografia de arquivos em unidades de computador locais;

3.3.15.4.76.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões;

3.3.15.4.76.3. A criação de listas criptografadas de pastas em unidades de computador locais;

3.3.15.4.77. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:

3.3.15.4.77.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis;

3.3.15.4.77.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais;

3.3.15.4.78. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:

3.3.15.4.78.1. A criptografia de todos os arquivos armazenados em unidades removíveis;

3.3.15.4.78.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis;

3.3.15.4.79. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia;

3.3.15.4.80. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis;

3.3.15.4.81. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado;

3.3.15.4.82. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido;

3.3.15.4.83. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais;

3.3.15.4.84. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia;

3.3.15.4.85. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados;

3.3.15.4.86. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema;

3.3.15.4.87. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado;

3.3.15.4.88. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário;

3.3.15.4.89. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados;

3.3.15.4.90. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos;

3.3.15.4.91. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação;

3.3.15.4.92. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. Independentemente da localização e/ou usuário;

3.3.15.4.93. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização;

3.3.15.4.94. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker;

3.3.15.4.95. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:

3.3.15.4.95.1. Uso do Trusted Platform Module e configurações de senha;

3.3.15.4.95.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível;

3.3.15.4.96. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets);

3.3.15.4.97. A solução proposta deve suportar criptografia em Microsoft Surface Tablets;

3.3.15.4.98. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, tais como:

3.3.15.4.98.1. Instalação remota de software de terceiros;

3.3.15.4.98.2. Relatórios sobre software e hardware existentes;

3.3.15.4.98.3. Monitoramento para instalação de software não autorizado;

3.3.15.4.98.4. Remoção de software não autorizado;

3.3.15.4.99. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados;

3.3.15.4.100. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints;

3.3.15.4.101. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade;

3.3.15.4.102. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais;

3.3.15.4.103. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches;

3.3.15.4.104. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade;

3.3.15.4.105. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros;

3.3.15.4.106. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança;

3.3.15.4.107. A solução proposta deve permitir ao administrador aprovar atualizações;

3.3.15.4.108. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes;

3.3.15.4.109. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias;

3.3.15.4.110. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis;

3.3.15.4.111. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.

3.3.15.4.112. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos;

3.3.15.4.113. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências);

3.3.15.4.114. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações;

3.3.15.4.115. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.

3.3.15.4.116. A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’;

3.3.15.4.117. A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”;

3.3.15.4.118. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft;

3.3.15.4.119. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários;

3.3.15.4.120. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes;

3.3.15.4.121. A solução proposta deve apoiar a implantação do sistema operacional;

3.3.15.4.122. A solução proposta deve suportar Wake-on LAN e UEFI;

3.3.15.4.123. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server;

3.3.15.4.124. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações;

3.3.15.4.125. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador;

3.3.15.4.126. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente;

3.3.15.4.127. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros;

3.3.15.4.128. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas;

3.3.15.4.129. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota;

3.3.15.4.130. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis;

3.3.15.4.131. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros;

3.3.15.4.132. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:

3.3.15.4.132.1. Inicie a instalação ao reiniciar ou desligar o computador;

3.3.15.4.132.2. Instale o gerador necessário todos os pré-requisitos do sistema;

3.3.15.4.132.3. Permitir a instalação de novas versões de aplicativos durante as atualizações;

3.3.15.4.132.4. Baixe atualizações para o dispositivo sem instalá-las;

3.3.15.4.133. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas;

3.3.15.4.134. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais;

3.3.15.4.135. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:

3.3.15.4.135.1. CEF;

3.3.15.4.135.2. LEEF;

3.3.15.4.136. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais;

3.3.15.4.137. O relatório da solução proposta deve conter informações CVE;

3.3.15.4.138. A solução proposta deve suportar instalação de aplicações e software de terceiros;

3.3.15.5. DO MÓDULO DE GERENCIAMENTO SIMPLIFICADO

3.3.15.5.1. A solução proposta deve suportar arquitetura cloud;

3.3.15.5.2. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional;

3.3.15.5.3. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos;

3.3.15.5.4. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint;

3.3.15.5.5. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS;

3.3.15.5.6. A solução proposta deve incluir informações do endpoint:

3.3.15.5.6.1. IP público de internet;

3.3.15.5.6.2. IP interno do dispositivo;

3.3.15.5.6.3. Versão do agente de proteção;

3.3.15.5.6.4. Última comunicação com a console, contendo data e hora;

3.3.15.5.6.5. Informações do sistema operacional;

3.3.15.5.7. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365;

3.3.15.5.8. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365;

3.3.15.5.9. A solução proposta deve incluir treinamento em segurança cibernética;

3.3.15.6. Do Módulo de Gerenciamento de Dispositivos Móveis

3.3.15.6.1. O modulo deve ser integrado a console de gerenciamento;

3.3.15.6.2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

3.3.15.6.2.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition);

3.3.15.6.3. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

3.3.15.6.3.1. iOS 10–17 ou iPadOS 13–17;

3.3.15.6.4. A solução proposta deve oferecer suporte a dispositivos Android Device Owner;

3.3.15.6.5. A solução proposta deve suportar dispositivos iOS supervisionados;

3.3.15.6.6. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador;

3.3.15.6.7. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras;

3.3.15.6.8. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões;

3.3.15.6.9. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais);

3.3.15.6.10. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário;

3.3.15.6.11. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps;

3.3.15.6.12. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado;

3.3.15.6.13. A solução proposta deve ter recursos de conteinerização para dispositivos Android.

3.3.15.6.14. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:

3.3.15.6.14.1. Dados em contêineres;

3.3.15.6.14.2. Contas de e-mail corporativo;

3.3.15.6.14.3. Configurações para conexão à rede Wi-Fi corporativa e VPN;

3.3.15.6.14.4. Nome do ponto de acesso (APN);

3.3.15.6.14.5. Perfil do Android for Work;

3.3.15.6.14.6. Recipiente KNOX;

3.3.15.6.14.7. Chave do gerenciador de licença KNOX;

3.3.15.6.15. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:

3.3.15.6.15.1. Todos os perfis de configuração instalados;

3.3.15.6.15.2. Todos os perfis de provisionamento;

3.3.15.6.15.3. O perfil iOS MDM;

3.3.15.6.16. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas;

3.3.15.6.17. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo;

3.3.15.6.18. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:

3.3.15.6.18.1. Critérios de verificação do dispositivo;

3.3.15.6.18.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;

3.3.15.6.19. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc;

3.3.15.6.20. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:

3.3.15.6.20.1. Cartões de memória e outras unidades removíveis;

3.3.15.6.20.2. Câmera do dispositivo;

3.3.15.6.20.3. Conexões Wi-Fi;

3.3.15.6.20.4. Conexões Bluetooth;

3.3.15.6.20.5. Porta de conexão infravermelha;

3.3.15.6.20.6. Ativação do ponto de acesso Wi-Fi;

3.3.15.6.20.7. Conexão de área de trabalho remota;

3.3.15.6.20.8. Sincronização de área de trabalho;

3.3.15.6.20.9. Definir configurações da caixa de correio do Exchange;

3.3.15.6.20.10. Configurar caixa de e-mail em dispositivos iOS MDM;

3.3.15.6.20.11. Configure contêineres Samsung KNOX;

3.3.15.6.20.12. Defina as configurações de restrição de conteúdo de mídia;

3.3.15.6.20.13. Definir configurações de proxy no dispositivo móvel;

3.3.15.6.20.14. Configurar certificados e SCEP;

3.3.15.6.21. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay;

3.3.15.6.22. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:

3.3.15.6.22.1. Huawei App Gallery e Apple App Store;

3.3.15.6.22.2. Portal de inscrição móvel KNOX;

3.3.15.6.22.3. Pacotes de instalação pré-configurados independentes;

3.3.15.6.23. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel;

3.3.15.6.24. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente;

3.3.15.6.25. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:

3.3.15.6.25.1. VMware AirWatch 9.3 ou posterior;

3.3.15.6.25.2. MobileIron 10.0 ou posterior;

3.3.15.6.25.3. IBM MaaS360 10.68 ou posterior;

3.3.15.6.25.4. Microsoft Intune 1908 ou posterior;

3.3.15.6.25.5. SOTI MobiControl 14.1.4 (1693) ou posterior;

3.3.15.6.26. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo;

3.3.15.6.27. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:

3.3.15.6.27.1. Galeria de aplicativos Huawei;

3.3.15.6.27.2. Loja de aplicativos da Apple;

3.3.15.6.28. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo;

3.3.15.6.29. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo;

3.3.15.6.30. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento;

3.3.15.6.31. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena;

3.3.15.6.32. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos;

3.3.15.6.33. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente;

3.3.15.6.34. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores;

3.3.15.6.35. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente;

3.3.15.6.36. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel;

3.3.15.6.37. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis;

3.3.15.6.38. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel;

3.3.15.6.39. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido;

3.3.15.6.40. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;

3.3.15.6.41. A solução proposta deve proteger contra ameaças online em dispositivos iOS;

3.3.15.7. DO MÓDULO DE EDR

3.3.15.7.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos: Conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta;

3.3.15.7.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados;

3.3.15.7.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;

3.3.15.7.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

3.3.15.7.5. Deve apresentar informações detalhadas contendo:

3.3.15.7.5.1. Usuário que executou a ação;

3.3.15.7.5.2. Informações acesso privilegiado;

3.3.15.7.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas;

3.3.15.7.7. A solução proposta deve suportar integração com serviço de reputação em nuvem;

3.3.15.7.8. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.);

3.3.15.7.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único);

3.3.15.7.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;

3.3.15.7.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem;

3.3.15.7.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção;

3.3.15.7.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta;

3.3.15.7.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados;

3.3.15.7.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador;

3.3.15.7.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede;

3.3.15.7.17. A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas;

3.3.15.7.18. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC;

3.3.15.7.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint;

3.3.15.7.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada;

3.3.15.7.21. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque);

3.3.15.7.22. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional;

3.3.15.7.23. Informações gerais sobre a detecção, incluindo modo de detecção;

3.3.15.7.24. Alterações no registro associadas à detecção;

3.3.15.7.25. Histórico da presença de arquivos no dispositivo;

3.3.15.7.26. Ações de resposta executadas pela aplicação;

3.3.15.7.27. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc;

3.3.15.7.28. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:

3.3.15.7.28.1. Processo;

3.3.15.7.28.2. Conexões de rede;

3.3.15.7.28.3. Alterações no registro;

3.3.15.7.28.4. Detalhes do download de objeto;

3.3.15.7.29. A solução proposta deve fornecer orientação de resposta (resposta guiada);

3.3.15.7.30. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente;

3.3.15.7.31. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:

3.3.15.7.31.1. Impedir a execução de objetos;

3.3.15.7.31.2. Isolamento de host;

3.3.15.7.31.3. Excluir objeto do host ou grupo de hosts;

3.3.15.7.31.4. Encerrar um processo no dispositivo;

3.3.15.7.31.5. Colocar um objeto em quarentena;

3.3.15.7.31.6. Execute a verificação do sistema;

3.3.15.7.31.7. Execução remota de programa/processo/comando;

3.3.15.7.31.8. Iniciar a varredura IoC para um grupo de hosts;

3.3.15.8. Do Módulo de Detecção e Resposta Gerenciada - MDR

3.3.15.8.1. Do monitoramento, identificação e investigação dos eventos de segurança cibernética:

3.3.15.8.1.1. O serviço de monitoramento deverá utilizar informações extraídas de registros gerados pelos sistemas monitorados;

3.3.15.8.1.2. Deverá ser instalado agentes específicos nos servidores e desktops, objetivando coletar informações mais detalhadas para o serviço de monitoramento, desde que seja plenamente compatível com o sistema onde será instalado e não afete o desempenho dos serviços;

3.3.15.8.1.3. A análise das informações correlacionadas deve ser realizada com auxílio de bases globais de inteligência cibernética em conjunto com a expertise dos profissionais do fabricante, com vistas a reduzir ao máximo os falsos positivos;

3.3.15.8.1.4. É obrigatório que a comunicação entre equipamentos e soluções do fabricante instalados nos dispositivos e qualquer infraestrutura onde esses dados sejam processados ocorra de forma segura, utilizando algoritmos criptográficos para preservar o sigilo das informações;

3.3.15.8.1.5. Deverá ser feita a investigação e a classificação dos eventos monitorados, aplicando os principais frameworks de gestão de incidentes de segurança cibernética bem como boas práticas de mercado na detecção e triagem dos eventos de segurança, objetivando minimizar a presença de falsos positivos na abertura de incidentes de segurança;

3.3.15.8.1.6. O serviço de monitoramento deverá ser capaz de coletar e realizar a correlação de eventos dos sistemas e ativos monitorados, permitindo uma visão mais abrangente do alcance das ações maliciosas, bem como de possível movimentação lateral do atacante dentro da rede;

3.3.15.8.1.7. O monitoramento deverá ser capaz de identificar as principais ameaças, bem como táticas, técnicas e procedimentos de ataque descritos na base de conhecimento MITRE ATT&CK, sem prejuízo do uso de outras bases de conhecimento ou serviços de inteligência de ameaças, para complementação da capacidade de identificação de atividades maliciosas;

3.3.15.8.1.8. Deverá monitorar e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média e identificando comportamentos anômalos, visando antecipar a identificação de incidentes de segurança;

3.3.15.8.1.9. A solução deverá prover inteligência de proteção contra-ataques cibernéticos a nível global, sendo responsável por pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança monitorados;

3.3.15.8.1.10. O fabricante deverá utilizar solução para registro de incidente de segurança, acessível pela equipe técnica da Contratante, para indicar ações de contenção, comunicar à equipe da Contratante sobre o andamento do tratamento dos incidentes;

3.3.15.8.2. Da compatibilidade:

3.3.15.8.2.1. É suportada por qualquer um dos seguintes navegadores:

3.3.15.8.2.1.1. Apple Safari versões mais recentes;

3.3.15.8.2.1.2. Google Chrome versões mais recentes;

3.3.15.8.2.1.3. Microsoft Edge;

3.3.15.8.2.1.4. Mozilla Firefox versões mais recentes;

3.3.15.8.3. Deverá suportar os requisitos de carga de rede:

3.3.15.8.3.1. Em condições médias de carga: um canal full-duplex com largura de banda de pelo menos 1,7 Kbps para cada ativo;

3.3.15.8.3.2. Em condições de carga máxima: um canal full-duplex com largura de banda de pelo menos 2,7 Kbps para cada ativo;

3.3.15.8.4. Compatibilidade de sensor de endpoint:

3.3.15.8.4.1. O agente de endpoint deve ser compatível com os seguintes sistemas operacionais, para no mínimo a coleta e envio dos dados/telemetria ao SOC do fabricante:

3.3.15.8.4.1.1. Microsoft Windows 7 e superiores;

3.3.15.8.4.1.2. MacOS 10.14-11;

3.3.15.8.4.1.3. CentOS 6.7 ou superior;

3.3.15.8.4.1.4. Debian GNU / Linux 9.4 ou superior;

3.3.15.8.4.1.5. Linux Mint 19 ou superior;

3.3.15.8.4.1.6. Oracle Linux 7.3 ou superior;

3.3.15.8.4.1.7. Red Hat Enterprise Linux 6.7 ou superior;

3.3.15.8.4.1.8. SUSE Linux Enterprise Server 12 SP5 ou superior;

3.3.15.8.4.1.9. Ubuntu 18.04 LTS ou superior;

3.3.15.8.5. Capacidades técnicas:

3.3.15.8.5.1. Deve possuir console web própria do serviço, além de integração nativa com a console do “software de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets”;

3.3.15.8.5.2. A console deve possuir dashboards com as informações principais, apresentando no mínimo:

3.3.15.8.5.2.1. Número de incidentes e status;

3.3.15.8.5.2.2. Quantidade de dispositivos monitorados;

3.3.15.8.5.3. Deve possuir mecanismo de notificações, com no mínimo as seguintes opções:

3.3.15.8.5.3.1. E-mail;

3.3.15.8.5.3.2. Telegram;

3.3.15.8.5.4. Deve permitir o envio de relatórios;

3.3.15.8.5.5. O agente deve enviar a telemetria em tempo real para o SoC do fabricante;

3.3.15.8.5.6. O serviço deve compreender monitoramento dos dados enviados e alertas gerados em um regime 24x7x265;

3.3.15.8.5.7. O envio e armazenamento da telemetria, devem respeitar as principais legislações de proteção de dados, como GDPR e LGPD;

3.3.15.8.5.8. O SoC do fabricante deve possuir datacenters em pelo menos duas localidades em diferentes países;

3.3.15.8.5.9. O SoC do fabricante deve possuir equipes de analistas em pelo menos 3 regiões (países) incluindo Brasil;

3.3.15.8.5.10. Os dados coletados devem passar por no mínimo:

3.3.15.8.5.10.1. Modelos de Machine Learning/Inteligência Artificial;

3.3.15.8.5.10.2. Análise humana;

3.3.15.8.5.10.3. Correlação com IoA’s (indicadores de ataque);

3.3.15.8.5.10.4. Emulação em sandbox (quando necessário);

3.3.15.8.5.11. Após análise, informações sobre atividades potencialmente maliciosas, devem ser apresentadas no portal como “Incidentes”

3.3.15.8.5.12. O Incidente deve possuir no mínimo as seguintes informações:

3.3.15.8.5.12.1. Resumo;

3.3.15.8.5.12.2. Prioridade (Baixa, Média e Alta);

3.3.15.8.5.12.3. Recomendação;

3.3.15.8.5.12.4. Data de criação e data de atualização;

3.3.15.8.5.12.5. Correlacionamento com táticas/técnicas do Framewok MITRE ATT&CK;

3.3.15.8.5.12.6. Dispositivos afetados;

3.3.15.8.5.12.7. IoC's de host e de rede;

3.3.15.8.5.12.8. Descrição completa em linha do tempo;

3.3.15.8.5.13. O incidente pode receber ações de resposta recomendada disparadas pela equipe de SoC, compreendendo no mínimo as seguintes ações:

3.3.15.8.5.13.1. Transferir arquivo para o SoC;

3.3.15.8.5.13.2. Isolar um dispositivo;

3.3.15.8.5.13.3. Desabilitar isolamento de dispositivo;

3.3.15.8.5.13.4. Deletar chave de registro;

3.3.15.8.5.13.5. Dump de memória;

3.3.15.8.5.14. As ações devem ser aprovadas no portal por profissional da contratante, com a opção de habilitar aprovação automática;

3.3.15.8.6. Agente de endpoint

3.3.15.8.6.1. As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;

3.3.15.8.6.2. A solução deve oferecer módulo focado em capacidades de EDR "Endpoint Detection and Response", incluindo no mínimo as seguintes capacidades:

3.3.15.8.6.2.1. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça;

3.3.15.8.6.2.2. Deve fornecer graficamente a visualização da cadeia do ataque;

3.3.15.8.6.2.3. Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC);

3.3.15.8.6.2.4. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:

3.3.15.8.6.2.4.1. Isolar o host;

3.3.15.8.6.2.4.2. Iniciar uma varredura nas áreas críticas;

3.3.15.8.6.2.4.3. Quarentenar o objeto.

3.3.15.8.6.3. A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

3.3.15.8.6.3.1. Detecções provenientes da solução de endpoint;

3.3.15.8.6.3.2. Processos;

3.3.15.8.6.3.3. Alterações de registro;

3.3.15.8.6.3.4. Conexões remotas;

3.3.15.8.6.3.5. Criação de arquivos;

3.3.15.8.6.4. Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador;

3.3.15.8.6.5. Possibilidade de exportar os indicadores de comprometimento (IoC) gerados a partir da solução;

3.3.15.8.6.6. A solução deve oferecer no mínimo as seguintes opções de resposta:

3.3.15.8.6.6.1. Prevenir a execução de um arquivo;

3.3.15.8.6.6.2. Quarentenar um arquivo;

3.3.15.8.6.6.3. Iniciar uma varredura por IoC;

3.3.15.8.6.6.4. Parar um processo;

3.3.15.8.6.6.5. Executar um processo;

3.3.15.8.6.7. Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:

3.3.15.8.6.7.1. A opção de isolamento deve estar disponível junto a visualização do incidente;

3.3.15.8.6.7.2. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após a ativação da regra;

3.4. CONDIÇÕES DE ENTREGA OU DA PRESTAÇÃO DO SERVIÇO

3.4.1. A Contratada deverá realizar os procedimentos de transbordo, descarga e armazenamento dos equipamentos (com as embalagens originais) no local indicado para a entrega.

3.4.2. A Contratada deverá providenciar equipamentos e/ou mão de obra necessários para a descarga, que será acompanhada e fiscalizada por servidor devidamente designado.

3.4.3. A verificação quanto ao estado dos produtos após o transporte será de exclusiva responsabilidade da Contratada, sendo que, quaisquer danos ocorridos no transporte dos equipamentos e observados a qualquer tempo, deverão ser reparados pela Contratada, sem qualquer ônus para o Contratante.

3.4.4. Todos os softwares, firmwares e drivers de controle necessários ao perfeito funcionamento da solução, na última versão disponível;

3.4.5. Todas as licenças de utilização definitivas para os softwares, firmwares e drivers fornecidos;

3.4.6. Todos os cabos e acessórios necessários para a perfeita instalação, configuração e uso da solução;

3.4.7. Toda a documentação técnica da solução fornecida, completa e atualizada, contendo manuais, guias de instalação e outros pertinentes, referente a equipamentos e procedimentos que a

compõem, todos originais e redigidos em português ou inglês, não sendo aceitas cópias. A documentação técnica poderá ser entregue, também, em meio eletrônico;

3.4.8. Acesso para o CONTRATANTE à base de conhecimento do fabricante, incluindo documentação e download de atualizações.

3.4.9. Todas as peças e componentes necessários ao perfeito funcionamento de toda a solução, quando necessário devem ser substituídos pela CONTRATADA, sem nenhum custo adicional a CONTRATANTE.

3.5. DA IMPLEMENTAÇÃO DA SOLUÇÃO

3.5.1. Para todo os conjuntos (hardware ou software), deverá ser fornecido um Serviço Especializado de Instalação e Customização para a realização de serviços especializados.

3.5.2. Entende-se por serviço especializado de instalação e customização de equipamentos, a montagem física dos equipamentos e seus respectivos acessórios pela CONTRATADA, bem como a configuração lógica de todos os equipamentos e softwares envolvidos, de acordo com o cenário requerido pela CTEC/SES/MS.

3.5.3. Este serviço trata do “Projeto Executivo” e tem como objetivo a instalação física dos equipamentos, sua conectividade com a rede de dados e a configuração das características listadas pelo CONTRATANTE. A CONTRATADA deverá ser responsável pela definição, planejamento e execução de todas as informações a serem configuradas, após terem sido previamente aprovadas pelo CONTRATANTE.

3.5.4. Para a execução do serviço especializado de instalação e configuração, a CONTRATADA entregará, para validação do CONTRATANTE, um Plano de Implementação da Solução composto por, pelo menos, o conteúdo definido a seguir:

3.5.4.1. Plano de Entrega e Instalação dos Produtos – neste documento deverá constar, no mínimo, a relação completa dos equipamentos e softwares a serem fornecidos, discriminando detalhadamente a finalidade de cada um. O plano deverá contemplar e detalhar todos os serviços de instalação e configuração, bem como estabelecer procedimentos de testes de conexão e desempenho da rede para cada etapa de instalação e configuração concluída. Deverá ser informado o prazo para a conclusão de cada etapa do serviço de entrega e instalação. O plano de instalação dos produtos deverá contemplar obrigatoriamente os seguintes itens: endereçamento IP, políticas de VLANs, políticas de segurança, políticas de balanceamento de carga, roteamento, QoS, filtros, alarmes, relatórios a serem configurados e documentação da rede, conforme as features determinadas previamente pelo CONTRATANTE;

3.5.4.2. Projeto Executivo – este documento constitui-se no detalhamento da documentação necessária a correta configuração e parametrização dos equipamentos a serem fornecidos pela CONTRATADA. Neste documento deverão constar todas as informações geradas pela CONTRATADA, abordando os aspectos de arquitetura implantada, configuração, testes, migração e integração ao ambiente de rede do CONTRATANTE.

3.6. REQUISITOS DE TREINAMENTO/CAPACITAÇÃO

3.6.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de não somente implantar a solução, porém mantê-la em funcionamento ininterrupto, provendo disponibilidade e desempenho durante toda a execução do contrato, através de equipe técnica especializada e apoio do fabricante na análise de problemas e atualização de seus produtos quanto à evolução tecnológica, correção de erros e vulnerabilidades e adaptação às mudanças de ambiente;

3.6.2. Deverá ser oferecido treinamento da solução ofertada para, no mínimo, 04 (quatro) participantes;

3.6.3. O treinamento deverá ser realizado na sede da CTEC/SES/MS ou em outro local apropriado, a ser acordado entre as partes, no município de Campo Grande/MS;

3.6.4. Deverá ser distribuído material de apoio a cada participante, que poderá ser, preferencialmente, em português ou inglês;

3.6.5. O conteúdo do treinamento deverá ser organizado em módulos, sequenciados logicamente, visando o conhecimento cumulativo, contendo, ao final de cada módulo, exercícios práticos com laboratórios para fixação;

3.6.6. A Contratada deverá prover os equipamentos que irão compor o laboratório do treinamento, que deverão ser equivalentes aos fornecidos para a CTEC/SES/MS ou, quando não for possível, por equipamentos similares com as mesmas funcionalidades;

3.6.7. O instrutor deverá ministrar o treinamento em português com carga horária de, no mínimo, 20 (vinte) horas, abordando obrigatoriamente o seguinte conteúdo:

3.6.7.1. Instalação do produto;

3.6.7.2. Utilização da interface gráfica simples;

3.6.7.3. Configuração dos parâmetros básicos e gerenciamento de usuários;

3.6.7.4. Melhores práticas de utilização da solução;

3.6.7.5. Integração com ambientes de virtualização;

3.6.7.6. Criação de regras personalizadas (firewall, antivírus, VPN, IPS, MTA, QoS, Aceleração e outras essenciais para ativação das funcionalidades principais);

3.6.7.7. Criação de perfis de aceleração e otimização de rede e aplicações;

3.6.7.8. Configuração de ambiente de alta disponibilidade (cluster);

3.6.7.9. Configuração de parâmetros para balanceamento de carga de serviços;

3.6.7.10. Conceitos de monitoramento;

3.6.7.11. Processamento de tráfego SSL na solução.

3.6.8. A CTEC/SES/MS poderá, a seu critério, em qualquer tempo, durante o treinamento, contestar a prestação do serviço, solicitando a troca de instrutor ou equipamentos de laboratório;

3.6.9. Caso a deficiência não possa ser sanada sem prejuízo para o andamento do treinamento, esse será suspenso pela CTEC/SES/MS, devendo a Contratada agendar novo treinamento, sem ônus adicional para a Contratante.

3.7. CONDIÇÕES DE EXECUÇÃO DO SERVIÇO E METODOLOGIA DE TRABALHO:

3.7.1. A Contratada deverá designar profissionais conforme as necessidades que se verificarem com acompanhamento da equipe técnica exigida para esta contratação em observância ao volume e complexidade dos trabalhos, além das características decorrente da metodologia de trabalho.

3.7.2. Todas as atividades técnicas serão desempenhadas de acordo com o ambiente tecnológico do Governo do Estado do Mato Grosso do Sul, devendo, portanto, haver compatibilidade do perfil do profissional exigido para o desempenho da atividade.

3.7.3. Os serviços serão realizados no ambiente físico da Contratada que possibilitara todos os meios necessários para a Contratante acompanhar os trabalhos por meio do Gestor do Contrato designado ou qualquer outro servidor designado.

3.7.4. Quando os serviços forem realizados no ambiente físico da Contratante, os profissionais deverão executá-los conforme jornada de trabalho da CTEC/SES/MS, o que será controlado pela Contratada e supervisionado pela CTEC/SES/MS.

3.7.5. A Contratada não poderá subcontratar, subempreitar, ceder ou transferir, total ou parcialmente o objeto da presente licitação descrita neste Estudo Técnico Preliminar.

3.7.6. A instalação dos equipamentos e a sua colocação em funcionamento correrão por conta e responsabilidade da Contratada;

3.7.7. Todos os itens necessários à instalação da solução correrão por conta da Contratada, como cabos, conectores e demais acessórios;

3.7.8. A solução deverá ser instalada em rack de piso, padrão 19”, com medidas adequadas para acomodação da solução;

3.8. CONDIÇÕES DE GARANTIA E SUPORTE TÉCNICO

3.8.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de não somente implantar a solução, porém mantê-la em funcionamento ininterrupto, provendo disponibilidade e desempenho durante toda a execução do contrato, através de equipe técnica especializada e apoio do fabricante na análise de problemas e atualização de seus produtos quanto à evolução tecnológica, correção de erros e vulnerabilidades e adaptação às mudanças de ambiente;

3.8.2. Quanto ao serviço de prestação dos serviços de Suporte Técnico Especializado, reforçamos que, apesar de fundamentalmente tratar-se de outsourcing de solução de tecnologia da informação, é evidente que o suporte técnico é primordial para a manutenção da plataforma de gerenciamento, proteção e inspeção de tráfego em redes corporativas, conforme justificamos abaixo:

3.8.2.1. O ambiente de rede corporativa e o ambiente de rede do Datacenter da SES/MS a ser suportado pela solução a ser contratada, é crítico para manutenção dos serviços públicos da Secretaria de Estado de Saúde. Qualquer evento que ocasione a parada ou mal funcionamento do ambiente computacional assegurado pela tecnologia em questão poderá causar prejuízos diretos e indiretos para o Estado, incluindo a interrupção da rede de dados em todos ou em parte dos sistemas de informação, nos serviços públicos prestados em formato digital, ou consequências mais críticas como a perda ou roubo de dados críticos e/ou sigilosos, ataques de vírus, hackers e outras ameaças virtuais, e ainda a completa paralização da prestação de serviços públicos mantidos pelo ambiente de tecnologia em questão;

3.8.2.2. Considerando que as atividades desta Coordenadoria de Tecnologia são realizadas ininterruptamente, não se justifica que os serviços de suporte técnico sejam prestados somente em horário comercial, bem como que não haja meios digitais para que estes sejam solicitados. Ademais, o atendimento local é essencial, considerando que problemas que demandem intervenção física nas plataformas são comumente necessários;

3.8.2.3. Desta forma, os serviços de Suporte Técnico Especializado, Manutenção e Apoio deverão ser prestados pela empresa contratada na forma *"on-site"* ou remoto, no regime 24X7, incluindo a atualização de softwares e bases de dados de conhecimento as suas expensas, e, sempre que for necessário ao bom funcionamento da solução adquirida;

3.8.2.4. Destacamos que o modelo de assistência local e ininterrupta não se trata de novação, sendo que é comum no mercado que as empresas que possuem produtos desta natureza, equivalentes ao esperado neste processo, prestem os serviços almejados dentro dos requisitos estabelecidos;

3.8.3. Todos os serviços de Suporte Técnico Especializado, Manutenção e Apoio deverão ser executados por técnicos qualificados e com certificação comprovada pelo fabricante da Solução,

pertencentes ao quadro de funcionários da CONTRATADA, sem custos adicionais para o CONTRATANTE, durante todo o período de garantia, sendo indispensável a apresentação de documentação original do fabricante que comprove a validade da certificação.

3.8.4. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL DA EQUIPE DE SUPORTE TÉCNICO

3.8.4.1. A CONTRATADA deverá prover suporte técnico especializado para a solução ofertada através de equipe técnica especializada e devidamente capacitada;

3.8.4.2. A equipe deverá ser composta por profissionais com as seguintes especialidades:

3.8.4.2.1. No mínimo 02 (dois) profissionais com as seguintes especialidades:

| **PERFIL 01 – Suporte Técnico e Manutenção para solução de proteção de perímetro** | |
|---|---|
| Responsável por realizar todas as atividades relacionadas à suporte técnico e manutenção da solução de proteção de perímetro ofertada, conforme as normas, padrões e diretrizes da fabricante. | |
| **Experiência/Qualificação** | **Modo de Comprovação** |
| - Qualificação para prestar serviços de suporte técnico ou manutenção nas soluções do fabricante da solução de proteção de perímetro. | - Certificado de conclusão de capacitação fornecido pelo fabricante da solução de proteção de perímetro, com o nível de certificação *Administrator, Professional* ou superior, dentro do período de validade; |
| **Formação** | **Modo de Comprovação** |
| - Formação de nível superior completa nas áreas correlatas de TIC, graduação ou pós-graduação nas áreas correlatas de TIC com carga horária mínima de 360 (trezentos e sessenta) horas. | - Diploma fornecido por instituição reconhecida pelo Ministério da Educação (MEC). |

3.8.4.2.2. No mínimo 02 (dois) profissionais com as seguintes especialidades:

| **PERFIL 02 – Suporte Técnico e Manutenção para solução de proteção e segurança para endpoints** | |
|---|---|
| Responsável por realizar todas as atividades relacionadas à suporte técnico e manutenção da solução de proteção e segurança para endpoints ofertada, conforme as normas, padrões e diretrizes da fabricante. | |
| **Experiência/Qualificação** | **Modo de Comprovação** |
| - Qualificação para prestar serviços de suporte | - Certificado de conclusão de capacitação fornecido |

| | |
|---|---|
| técnico ou manutenção nas soluções do fabricante da solução de proteção e segurança para endpoint com EDR. | pelo fabricante da solução de proteção e segurança para endpoint com EDR, com o nível de certificação *Administrator, Professional* ou superior, dentro do período de validade; |
| **Formação** | **Modo de Comprovação** |
| - Formação de nível superior completa nas áreas correlatas de TIC, graduação ou pós-graduação nas áreas correlatas de TIC com carga horária mínima de 360 (trezentos e sessenta) horas. | - Diploma fornecido por instituição reconhecida pelo Ministério da Educação (MEC). |

3.8.4.2.3. No mínimo 01 (um) profissional com as seguintes especialidades:

| **PERFIL 03 – Suporte Técnico e Monitoramento de Rede** | |
|---|---|
| Responsável por monitorar os ativos e a gestão dos eventos de TI da solução ofertada, focados na administração e no monitoramento de rede e dos equipamentos que compõem a solução. | |
| **Experiência/Qualificação** | **Modo de Comprovação** |
| - Certificação no software de monitoramento utilizado pelo SNOC. | - Certificado de conclusão de capacitação fornecido por instituto credenciado, dentro do período de validade. |
| **Formação** | **Modo de Comprovação** |
| - Formação de nível superior completa nas áreas correlatas de TIC, graduação ou pós-graduação nas áreas correlatas de TIC com carga horária mínima de 360 (trezentos e sessenta) horas. | - Diploma fornecido por instituição reconhecida pelo Ministério da Educação (MEC). |

3.8.4.2.4. No mínimo 01 (um) profissional com as seguintes especialidades:

| **PERFIL 04 – Analista de gerenciamento de serviços de TI** | |
|---|---|
| Responsável por estabelecer os processos que garantem organização e controle para cumprimento dos objetivos dos serviços contratados, alinhando assim a execução das atividades de TI aos processos de negócios de forma a garantir a execução contratual de forma plena. | |
| **Experiência/Qualificação** | **Modo de Comprovação** |

| | |
|---|---|
| - Certificação ITIL (v4 ou superior) e Certificação ISO/IEC 20000. | - Certificado de conclusão ITIL (v4 ou superior), fornecido por instituto credenciado, dentro do período de validade.<br>- Certificado de conclusão ISO/IEC 20000, fornecido por instituto credenciado, dentro do período de validade. |
| **Formação** | **Modo de Comprovação** |
| - Formação de nível superior completa nas áreas correlatas de TIC, graduação ou pós-graduação nas áreas correlatas de TIC com carga horária mínima de 360 (trezentos e sessenta) horas. | - Diploma fornecido por instituição reconhecida pelo Ministério da Educação (MEC). |

3.8.4.2.5. No mínimo 02 (dois) profissionais com as seguintes especialidades:

| **PERFIL 05 – Analistas SNOC** | |
|---|---|
| Responsável pela configuração, administração e operação de plataformas do SNOC e pelo gerenciamento, detecção e resposta aos incidentes de segurança da informação. Os analistas SNOC deverão executar as atividades de forma presencial, nas dependências da Contratante, em regime 8x5, observando os Níveis de Serviços dispostos no Acordo de Nível de Serviços exigidos. | |
| **Experiência/Qualificação** | **Modo de Comprovação** |
| - Experiência mínima de 4 (quatro) anos em operação de plataformas de NOC e/ou SOC/SIEM e gerenciamento, detecção e resposta aos incidentes de segurança da informação. | - Currículo do profissional. |
| **Formação** | **Modo de Comprovação** |
| - Formação de nível superior completa nas áreas correlatas de TIC, graduação ou pós-graduação nas áreas correlatas de TIC com carga horária mínima de 360 (trezentos e sessenta) horas. | - Diploma fornecido por instituição reconhecida pelo Ministério da Educação (MEC). |

3.8.5. TIPOS DE SERVIÇOS DE SUPORTE TÉCNICO E MANUTENÇÃO:

3.8.5.1. Manutenção Preventiva: Compreende visitas periódicas, conforme política definida pelo fabricante, no ambiente da Contratante, programadas a fim de verificar a saúde do equipamento e mitigar riscos devido ao uso continuado dos serviços, incluindo:

3.8.5.1.1. Procedimentos técnicos destinados a prevenir a ocorrência de erros e defeitos de forma proativa;

3.8.5.1.2. Realização de inspeções nos equipamentos, componentes, dispositivos e softwares de configuração gerenciam a solução;

3.8.5.1.3. Verificação geral com vistas a manter sua plena funcionalidade e saúde dos equipamentos;

3.8.5.1.4. Analisar logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta. A equipe técnica da Contratante decidirá sobre a aplicação ou não das recomendações;

3.8.5.1.5. Sugerir, preventivamente, a aplicação de novas correções, patches, fixes, updates, service packs, novas releases, versions, builds e upgrades.

3.8.5.2. Manutenção Corretiva: Compreende visitas pontuais, a partir de abertura de chamados advindos do Contratante, a fim de atuar em incidentes ou problemas identificados que impeça o seu funcionamento regular e requeira uma intervenção técnica especializada, na localidade de instalação da solução, incluindo:

3.8.5.2.1. Reinstalação de hardwares e softwares, configuração, gerenciamento, com vistas a normalidade da operação dos serviços prestados;

3.8.5.2.2. Reparar, corrigir, remover, refazer ou substituir, no todo ou em parte, os serviços, peças ou materiais em que se verificarem imperfeições, vícios, defeitos ou incorreções, dentro dos prazos estabelecidos nos demais subitens do presente estudo;

3.8.5.2.3. Corrigir defeitos de fabricação ou projeto;

3.8.5.2.4. Acondicionar adequadamente os equipamentos cujo reparo não possa ser realizado nas dependências da CTEC/SES/MS, de forma a permitir sua completa segurança e identificação durante o transporte, responsabilizando-se pela sua remoção e devolução ao local em que deve ser instalado e pelas despesas operacionais decorrentes;

3.8.5.2.5. Substituir os equipamentos que apresentarem defeito de fabricação, dentro dos prazos estabelecidos;

3.8.5.2.6. Detectar problemas e limitações de desempenho da solução relacionados a softwares e/ou firmware instalados nos elementos que fazem parte do objeto desta contratação, substituindo-os por nova versão que implemente suas correções;

3.8.5.2.7. Substituir software e/ou firmware instalados nos elementos que fazem parte do objeto desta contratação por nova versão eventualmente lançada, quando esta implementar correções a possíveis problemas ou limitações de desempenho da solução.

3.8.6. SUPORTE TÉCNICO ESPECIALIZADO E MANUTENÇÃO PRESTADOS PELA CONTRATADA:

3.8.6.1. A contratada deverá apresentar declaração de que proverá suporte técnico on-site disponível 24 horas por dia, 07 dias por semana.

3.8.6.2. A contratada deverá apresentar declaração de que possui plataforma de suporte técnico para abertura de chamados disponível através de internet (WEB), telefone ou e-mail.

3.8.6.3. A Contratada deverá, de acordo com as políticas de assistência técnica do fabricante da solução, prestar os serviços de suporte técnico especializado e manutenção para toda a solução de hardware e software, para orientação de uso e administração, atualização de versões, patchs e correções de bugs, configuração e parametrização.

3.8.6.4. O funcionamento da solução deverá ser garantido pela Contratada, que deverá se valer dos meios necessários para manter a solução operacional;

3.8.6.5. Poderão ser prestados pela empresa Contratada em ambiente on-site ou remoto, no regime 24X7, incluindo a atualização de softwares e bases de dados de conhecimento as suas expensas, e, sempre que for necessário ao bom funcionamento da solução adquirida;

3.8.6.6. Deverão ser executados por técnicos qualificados, conforme previsto nos requisitos de qualificação da equipe técnica presentes neste documento;

3.8.6.7. Quando realizados presencialmente, deverão ser prestados no endereço indicado pelo Contratante;

3.8.6.8. Todas as peças e componentes necessários ao perfeito funcionamento de toda a solução, quando necessário, devem ser substituídos pela Contratada, sem nenhum custo adicional a Contratante;

3.8.6.9. A Contratada deverá cumprir rigorosamente todos os procedimentos de manutenção definidos pela CTEC/SES/MS, como horário estabelecido para parada dos equipamentos, autorizações de acesso, entre outros;

3.8.6.10. Quando a intervenção implicar interrupção da solução, mesmo que parcial, a CTEC/SES/MS poderá determinar que a Contratada a execute fora do horário de expediente do órgão, inclusive em finais de semana, sem qualquer ônus adicional a Contratante;

3.8.6.11. Fica vedada a desativação de hardware, software ou quaisquer recursos computacionais da Contratante, sem prévio conhecimento e autorização expressa da Administração;

3.8.6.12. Caso seja necessária a desativação de hardware, software ou quaisquer recursos computacionais da CTEC/SES/MS, a Contratada deverá disponibilizar equipamento de redundância com capacidade igual ou superior ao que será desativado, até que o problema seja sanado, sob pena de inexecução parcial do contrato;

3.8.6.13. Em caso de retirada do equipamento, a CTEC/SES/MS poderá, a seu critério, reter as unidades de memória física dos equipamentos, sem custo adicional;

3.8.6.14. Havendo necessidade de substituição de hardware (equipamentos), a Contratada deverá efetuar a substituição por mesmo modelo de peça, ou por modelo superior em características técnicas, do mesmo fabricante, sem ônus para o Contratante, quando comprovados defeitos que comprometem seu desempenho, obedecendo os critérios abaixo, sem prejuízo de outras situações que caracterizem necessidade de troca:

3.8.6.14.1. Caso ocorram 04 (quatro) ou mais defeitos que comprometam seu uso normal, dentro de qualquer intervalo de 30 (trinta) dias;

3.8.6.14.2. O equipamento (hardware) empregado em substituição ao equipamento defeituoso deverá ter os mesmos serviços de suporte técnico e manutenção durante toda a vigência restante do contrato;

3.8.6.14.3. No caso de problema recorrente no mesmo hardware, seja na restauração ou substituição das peças, em um período inferior a 2 (dois) meses, a Contratada deverá substituir o equipamento.

3.8.6.15. Quando solicitado pela CTEC/SES/MS, a Contratada deverá fornecer, em até 3 (três) dias úteis, manuais, documentação de operação, documentos de troubleshooting e/ou qualquer outro tipo de documento técnico de administração, customização, operação e monitoração dos equipamentos e softwares instalados na CTEC/SES/MS;

3.8.6.16. As atualizações de versões de todos os componentes da solução (major, minor, patches e fixes) deverão estar disponíveis para uso da CTEC/SES/MS durante toda a prestação do serviço sem custo adicional, podendo ser realizado download diretamente do sítio oficial do fabricante, devendo ser entregue, sempre a última versão mais atualizada.

3.8.7. SUPORTE TÉCNICO ESPECIALIZADO E MANUTENÇÃO PRESTADOS PELO FABRICANTE:

3.8.7.1. A prestação destes serviços deve ainda contemplar o suporte técnico direto do fabricante da solução, a ser utilizado sempre que necessário, com, no mínimo, as seguintes características:

3.8.7.1.1. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento, 24 horas por dia e 7 dias por semana. Para atendimento telefônico, deve operar em língua portuguesa, pelo menos em regime 8x7 (oito horas por dia, sete dias por semana);

3.8.7.1.2. Deve-se assegurar a utilização de novas versões de software da solução sem ônus, sempre que esta estiver disponível;

3.8.7.1.3. Deve-se permitir o acesso à base de conhecimento da solução.

3.8.7.2. Sempre que solicitado pela Contratante, deve-se informar o estado do chamado aberto, por telefone da central de atendimento e/ou por sistema de controle de chamados da Contratada disponibilizado pela internet:

3.8.7.3. Caso o chamado seja repassado pela Contratada ao fabricante, o CTEC/SES/MS deverá ter capacidade visualizar diretamente no sítio do fabricante o andamento desse chamado;

3.8.7.4. Deverão ser fornecidas permissões de acesso no sítio do fabricante e da Contratada para acompanhamento de chamados, download e acesso a documentação, patches, fixes, firmwares, arquivos de qualquer tipo e/ou qualquer outro material referente à solução.

3.8.8. Núcleo de Operações, Controle e Segurança:

3.8.8.1. A Contratada deverá manter um SNOC (Centro de Operações de Segurança e Redes), nas dependências da Contratante, para diagnosticar preventivamente e corretivamente problemas nas soluções fornecidas e tomar as decisões de intervenção para a devida assistência técnica.

3.8.8.2. O SNOC deverá ser composto por ambiente de monitoramento das soluções e deverá ser mantido pela Contratada em regime 24 x 7 (vinte e quatro horas por dia, sete dias por semana), durante a vigência do contrato, para prestar o pronto-atendimento as solicitações de suporte de primeiro e segundo nível identificadas no SNOC e/ou usuários finais da solução;

3.8.8.3. A contratada deverá implantar, monitorar e administrar os serviços de monitoração da solução implementada, com as atividades de coleta de dados, gerenciamento de configuração de *templates* e gatilhos nas plataformas de monitoramento Zabbix e Grafana, atualmente utilizadas pela SES/MS para monitoramento de sua infraestrutura de TIC como um todo.

3.8.8.4. A contratada deverá monitorar e analisar toda a infraestrutura da Secretaria de Estado de Saúde de Mato Grosso do Sul, utilizando-se de análise dos logs disponibilizados em tempo real através da Plataforma de SIEM/SOAR que deverá ser fornecida pela Contratada. Para o devido dimensionamento do esforço de trabalho necessário, a Plataforma de SIEM/SOAR deverá coletar eventos que representam aproximadamente 2.000 EPS;

3.8.8.5. A estrutura de SNOC é comumente utilizada em ambientes de tecnologia e de comunicação, com o objetivo de exercer gerenciamento proativo, o monitoramento da qualidade, desempenho e nível de serviços e a resposta à incidentes ocorridos ou iminentes.

3.8.8.6. Neste aspecto, a existência de um SNOC é essencial para ambientes que possuam soluções complexas ou críticas para continuidade de negócio, o que se configura na contratação em

tela, considerando que a solução em questão manterá o gerenciamento de tráfego de aplicações e que envolvem a segurança dos dados e informações críticos, sigilosos e de alto valor para os entes que almejam sua contratação.

3.8.8.7. Longe de configurar inovação, os ambientes de SNOC são corriqueiramente utilizados por empresas que prestam tais serviços, visto que os incidentes envolvidos em ambientes não monitorados por vezes gera impacto maior do que o próprio custo da manutenção do núcleo.

3.8.8.8. Por fim, esclarecemos que a planilha de composição de custos prevê os valores referentes ao "serviço de suporte 24x7", sendo que os custos para manutenção do SNOC estão incluídos neste quesito, pois o ambiente em questão é voltado para o suporte técnico das soluções.

3.9. ACORDOS DE NÍVEL DE SERVIÇOS

3.9.1. Para a prestação dos serviços de Suporte Técnico Especializado, Manutenção e Apoio:

3.9.2. A CONTRATADA deverá cumprir rigorosamente todos os procedimentos de manutenção definidos pela CTEC/SES/MS, como horário estabelecido para parada dos equipamentos, autorizações de acesso, entre outros.

3.9.3. Quando a intervenção implicar interrupção da solução, mesmo que parcial, a CTEC/SES/MS poderá determinar que a CONTRATADA a execute fora do horário de expediente do órgão, inclusive em finais de semana, sem qualquer ônus adicional à CTEC/SES/MS.

3.9.4. Fica vedada a desativação de hardware, software ou quaisquer recursos computacionais da CONTRATANTE, sem prévio conhecimento e autorização expressa da Administração;

3.9.5. Caso seja necessária a desativação de hardware, software ou quaisquer recursos computacionais da CTEC/SES/MS, a CONTRATADA deverá disponibilizar equipamento de redundância com capacidade igual ou superior ao que será desativado, até que o problema seja sanado.

3.9.6. Em caso de retirada do equipamento, a CTEC/SES/MS poderá, a seu critério, reter as unidades de memória física dos equipamentos, sem custo adicional.

3.9.7. Havendo necessidade de substituição de hardware (equipamentos), a Contratada deverá efetuar a substituição por mesmo modelo de peça, ou por modelo superior em características técnicas, do mesmo fabricante, sem ônus para o Contratante, quando comprovados defeitos que comprometem seu desempenho, obedecendo os critérios abaixo, sem prejuízo de outras situações que caracterizem necessidade de troca:

3.9.7.1. Caso ocorram 04 (quatro) ou mais defeitos que comprometam seu uso normal, dentro de qualquer intervalo de 30 (trinta) dias;

3.9.7.2. O(s) equipamento(s) (hardware) empregado em substituição ao equipamento defeituoso deverá possuir prazo equivalente ao período que for acordado.

3.9.7.3. No caso de problema recorrente no mesmo hardware, seja na restauração ou substituição das peças, em um período inferior a 02 (dois) meses, a CONTRATADA deverá substituir o equipamento.

3.9.8. Mensalmente, deverá ser entregue um “Relatório de Atividades Técnicas” indicando todos os eventos de suporte técnico e manutenção atendidos no período. O Relatório deverá conter no mínimo:

3.9.8.1. Identificação de cada chamado;

3.9.8.2. Identificação do tipo de atendimento;

3.9.8.3. Data de atendimento (abertura e conclusão);

3.9.8.4. Descrição do atendimento;

3.9.8.5. Procedimentos adotados para a solução do problema;

3.9.9. Sem prejuízo da entrega do Relatório Gerencial, a CONTRATANTE poderá solicitar, em formato digital, informações analíticas e sintéticas dos chamados técnicos abertos e fechados no período;

3.9.10. Quando solicitado pela CTEC/SES/MS, a CONTRATADA deverá fornecer, em até 03 (três) dias úteis, manuais, MIB de monitoração, documentação de interfaces API, documentos de troubleshooting e/ou qualquer outro tipo de documento técnico de administração, customização, operação e monitoração dos equipamentos e softwares instalados na CTEC/SES/MS.

3.9.11. As atualizações de versões de todos os componentes da solução (major, minor, patches e fixes) deverão estar disponíveis para uso da CTEC/SES/MS durante todo período contratual e sem custo adicional, podendo ser realizado download diretamente do sítio oficial do fabricante, devendo ser entregue, a última versão vigente na data do término do contrato.

3.9.12. A CONTRATADA deverá apresentar declaração de que cumprirá os tempos para resolução de chamados abertos, seguindo as seguintes premissas de S.L.A. (Acordos de Níveis de Serviços):

3.9.13. O tempo de solução será contabilizado entre a abertura do chamado e restabelecimento do sistema em sua totalidade, bem como se entende por término do reparo do equipamento a sua disponibilidade para uso em perfeitas condições de funcionamento no local onde está instalado.

3.9.14. O tempo de atendimento inicia-se com a primeira intervenção pelo representante da CONTRATADA, local ou remotamente.

3.9.15. A contratada deverá se adequar aos seguintes níveis de serviço quando ocorrerem os chamados para Suporte Técnico Especializado, Manutenção e Apoio:

| MANUTENÇÃO PREVENTIVA |
|---|

| | | | | | |
|---|---|---|---|---|---|
| Indicador | Tipo do Chamado | Descrição | Inicio do atendimento | Prazo de Solução | Multa por descumprimento % em relação a fatura de suporte |
| N01 | Manutenção Programada | Suporte programado para verificação da saúde dos equipamentos e proposição de melhorias. | Na data Programada mensalmente conforme cronograma | Execução dentro do período programado no chamado | 2% por mês em que houver descumprimento por não atendimento. |
| MANUTENÇÃO CORRETIVA | | | | | |
| Indicador | Tipo do Chamado | Descrição | Inicio do atendimento | Prazo de Solução | Multa por descumprimento % em relação a fatura de suporte |
| N02 | Urgente | Solução parada, no todo ou em parte, no ambiente de produção provocando uma indisponibilidade parcial ou total do ambiente de produção da CONTRATANTE durante programas de governo em período de sazonalidade. | Em até 02 (duas) horas | Em até 06 (seis) horas | 2% por hora para as 4 primeiras horas que excederem o prazo;<br>4% por hora para as demais horas que excederem as primeiras 4 horas de descumprimento prazo. |
| N03 | Alto Impacto | Solução parada, no todo ou em parte, no ambiente de produção provocando ao menos uma indisponibilidade parcial do ambiente de | Em até 04 (quatro) horas | Em até 12 (doze) horas | 1% por hora para as 4 primeiras horas que excederem o prazo;<br>2% por dia que exceder o descumprimento prazo de solução. |

| | | | | | |
|---|---|---|---|---|---|
| | | produção da CONTRATANTE. | | | |
| N04 | Muito Importante | Erros ou problemas reincidentes que impactam o ambiente de produção. | Em até 08 (quatro) horas | Em até 24 (vinte e quatro) horas | 1% por dia que exceder o descumprimento do prazo de solução. |
| N05 | Importante | Problemas contornáveis que não causem lentidão ou indisponibilidade dos serviços ou aqueles para os quais houver solução de contorno. | Em até 24 (vinte e quatro) horas | Em até 2 dias | 0,5% dia que exceder o descumprimento do prazo de solução. |

| NÍVEL DE SERVIÇO PARA A DOCUMENTAÇÃO DE TODOS OS SERVIÇOS | | |
|---|---|---|
| Indicador | Descrição | Multa por descumprimento<br>% em relação a fatura de suporte |
| N06 | Relatório de Atendimento Técnico não entregue | 0,25% em relação ao valor do equipamento por dia ocorrência ou documento. |
| N07 | Reincidência na entrega de Relatório de Atendimento Técnico | 1 % por ocorrência ou documento reincidente. Caso exceda 3 ocorrências, de forma cumulativa ou não, será considerado inexecução parcial do objeto. |

3.9.16. Somente será admitido pedido de prorrogação dos prazos descritos na tabela de níveis de serviços mediante justificativas por escrito, plenamente fundamentadas e entregues à Administração dentro do período correspondente ao atendimento ou resolução do chamado aberto;

3.9.17. A não resolução dos chamados dentro do prazo acima estipulado ensejará às multas e sanções previstas. Após o limite estabelecido para aplicação das multas a CONTRATADA deverá substituir os equipamentos conforme prazos e condições descritas abaixo, sob pena de incorrer em inexecução dos serviços acordados:

3.9.17.1. Se o atendimento classificado como **URGENTE** não for resolvido dentro do prazo estabelecido, mesmo após a execução dos serviços de reparo (atualização de softwares/substituição de peças de hardware), o equipamento deverá ser integralmente substituído no prazo máximo de 02 (dois) dias, segundo as características técnicas e de desempenho iguais ou superiores ao bem

anterior de modo que não cause nenhum impacto no serviço sustentado pelos equipamentos, sem ônus para a CONTRATANTE, sob pena de caracterizar inexecução dos serviços;

3.9.17.2. Se o problema identificado como **ALTO IMPACTO** persistir pós-atendimento técnico, e não for resolvido de forma definitiva pela empresa contratada dentro do prazo estabelecido, podendo ser prorrogado por igual período (corrido), desde que justificado, o produto deverá ser integralmente substituído no prazo máximo de 04 (quatro) dias, segundo as características técnicas e de desempenho iguais ou superiores ao bem anterior, sem ônus para a CONTRATANTE, sob pena de caracterizar inexecução parcial dos **serviços**;

3.9.17.3. Se o problema identificado como **MUITO IMPORTANTE** persistir pós-atendimento técnico, e não for resolvido de forma definitiva pela empresa contratada dentro do prazo estabelecido, podendo ser prorrogado por igual período (corrido), desde que justificado, o produto deverá ser integralmente substituído no prazo máximo de 07 (sete) dias, segundo as características técnicas e de desempenho iguais ou superiores ao bem anterior, sem ônus para a CONTRATANTE, sob pena de caracterizar inexecução parcial dos **serviços;**

3.9.17.4. Se o problema identificado como **IMPORTANTE** não for resolvido de forma definitiva pela empresa contratada dentro do prazo estabelecido, podendo ser prorrogado por igual período (corrido), desde que justificado, a partir do sétimo dia, será aplicada glosa de 1% (um por cento) ao dia sobre o valor do faturamento mensal até que o problema seja integralmente sanado, limitado a 30 (trinta) dias, após esse prazo será caracterizado inexecução parcial dos serviços;

3.9.17.5. Se após 30 (trinta) dias a contar da notificação de aplicação da multa por inexecução parcial do contrato a CONTRATADA não substituir os equipamentos, será caracterizado inexecução total do contrato, sem prejuízo da continuidade do suporte técnico dos demais equipamentos em garantia;

3.9.18. Sempre que a CTEC/SES/MS solicitar, o estado do chamado aberto com a CONTRATADA deverá ser informado por telefone da central de atendimento e/ou por sistema de controle de chamados da CONTRATADA disponibilizado pela internet.

3.9.19. Caso o chamado seja repassado pela CONTRATADA ao fabricante, a CTEC/SES/MS deverá ter capacidade visualizar diretamente no sítio do fabricante o andamento desse chamado.

3.9.20. Deverão ser fornecidas permissões de acesso no sítio do fabricante e da CONTRATADA para acompanhamento de chamados, download e acesso a documentação, patches, fixes, firmwares, arquivos de qualquer tipo e/ou qualquer outro material referente à solução.

3.9.21. Todos os firmwares publicados deverão estar disponíveis para consulta e download pela CTEC/SES/MS diretamente no sítio do fabricante.

3.9.22. Quanto ao serviço de Suporte Técnico Especializado, reforçamos que é evidente que os serviços de suporte técnico a serem prestados pela empresa Contratada são primordiais para a manutenção da plataforma de gerenciamento de tráfego de aplicações e aceleração web, conforme justificativa abaixo:

3.9.22.1. O ambiente suportado pelas soluções de gerenciamento de tráfego de aplicações e aceleração web a serem contratadas é crítico para manutenção dos serviços públicos dos entes em questão. Qualquer evento que ocasione a parada ou mal funcionamento do ambiente computacional assegurado pela tecnologia em questão poderá causar prejuízos diretos e indiretos para o Estado, incluindo a interrupção da rede de dados dos órgãos atendidos, a perda ou roubo de dados críticos e/ou sigilosos, ataques de vírus, hackers e outras ameaças virtuais, e ainda a completa paralização da prestação de serviços públicos mantidos pelo ambiente de tecnologia em questão.

3.9.22.2. Considerando que as atividades da CTEC/SES/MS são realizadas ininterruptamente, não se justifica que os serviços de suporte técnico sejam prestados somente em horário comercial, bem como não haja meios digitais para que estes sejam solicitados. Ademais, o atendimento local é essencial, considerando que problemas que demandem intervenção física nas plataformas são comumente necessários.

3.9.22.2.1. Destacamos que o modelo de assistência local e ininterrupta não se trata de novação, sendo que é comum no mercado que as empresas que possuem produtos de gerenciamento de tráfego de aplicações e aceleração web equivalentes ao esperado neste processo prestem os serviços almejados dentro dos requisitos estabelecidos.

## 3.10. REQUISITOS LEGAIS

3.10.1. A contratação será regida pelas seguintes normas legais (requisitos de legalidade):

3.10.1.1. Lei Federal n°. 14.133/2021 – Lei de licitações e contratos administrativos, que estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios;

3.10.1.2. Lei Federal nº 6.938 - Dispõe sobre a Política Nacional do Meio Ambiente, seus fins e mecanismos de formulação e aplicação, e dá outras providências.

3.10.1.3. Decreto Estadual nº 16.121, de 9 de março de 2023, que “dispõe sobre o Plano de Contratação Anual, no âmbito dos órgãos da Administração Direta e das entidades autárquicas e fundacionais do Poder Executivo Estadual, nos termos da Lei Federal nº 14.133, de 1º de abril de 2021, e dá outras providências”.

## 3.11. REQUISITOS TEMPORAIS E CONDIÇÕES DE ENTREGA/PRESTAÇÃO DE SERVIÇOS

3.11.1. Cada entrega deverá ser efetuada mediante solicitação por escrito, formalizada pela contratante, dela devendo constar: a data, o valor unitário da entrega, a quantidade pretendida, o local para a entrega, o prazo, o carimbo e a assinatura do responsável, sendo efetuada diretamente pelo órgão/entidade requisitante, devidamente autorizado pela autoridade superior, e ainda acompanhada pela nota de empenho ou instrumento equivalente.

3.11.2. O prazo para início da execução dos serviços deverá ser de até 30 dias (trinta) dias contados do recebimento da nota de empenho, assinatura do contrato ou instrumento equivalente.

3.11.3. Caso não seja possível a entrega/execução na data assinalada, a contratada deverá comunicar as suas razões, com a devida comprovação, com pelo menos 05 (cinco) dias de antecedência, para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

3.11.4. A contratada obriga-se a entregar os serviços em conformidade com as especificações descritas na Proposta de Preços e neste instrumento, sendo de sua inteira responsabilidade a substituição, caso não esteja em conformidade com as referidas especificações.

3.11.5. Todas as despesas relativas aos objetos contratados, bem como todos os impostos, taxas e demais despesas decorrentes do contrato correrão por conta exclusiva da contratada.

3.11.6. O recebimento do serviço se efetivará em conformidade com o art. 140 da Lei 14.133/2021, mediante recibo, nas seguintes condições:

3.11.7. Os serviços serão recebidos provisoriamente, de forma sumária, no prazo de até 05 (cinco) dias úteis, pelo responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste instrumento e na proposta.

3.11.8. Para os fins do disposto no subitem 3.12.6., o termo sumário corresponde ao atesto no verso do documento fiscal ou equivalente, conforme art. 19 do Decreto nº 15.938, de 26 de maio de 2022.

3.11.9. Os serviços poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes neste instrumento e na proposta, devendo ser substituídos no prazo de 10 (dez) dias corridos, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

3.11.10. Os serviços serão recebidos definitivamente, por servidor ou comissão designada pela autoridade competente, no prazo de 10 (dez) dias úteis, contados do recebimento provisório, mediante preenchimento de termo detalhado que comprove o atendimento das exigências contratuais.

3.11.11. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

3.11.12. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal pertinente à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

3.11.13. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço, nem a responsabilidade ético-profissional pela perfeita execução do contrato.

3.11.14. O objeto do contrato poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o edital, ou/e que estejam inadequados para o uso.

3.11.15. Os itens serão entregues de forma virtual, devendo estar de acordo com as especificações descritas.

3.12. DA SUSTENTABILIDADE

3.12.1. Os serviços deverão ser prestados de acordo com os critérios de sustentabilidade ambiental contidos no Art. 5º da Instrução Normativa n° 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento Orçamento e Gestão — SLTI/MPOG e no Decreto n° 7.746/2012, da Casa Civil, da Presidência da República, no que couber.

3.12.2. Deverão ser cumpridas, no que couber, as exigências:

3.12.2.1. Do inciso XI, art. 7º da Lei 12.305, de 02 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos — PNRS;

3.12.2.2. Do art. 6º da Instrução Normativa MPOG n° 01, de 19 de janeiro de 2010, que estabelece as práticas de sustentabilidade na execução dos serviços.

3.12.2.3. Da Portaria N° 170, de 10 de abril de 2012 do Instituto Nacional de Metrologia, Qualidade e Tecnologia — INMETRO.

## 4. LEVANTAMENTO DE MERCADO

4.1. Dadas as necessidades apresentadas no presente estudo, foram analisadas as seguintes alternativas para atendimento às necessidades elencadas, alternativas estas que são as formas mais comuns de contratação:

4.1.1. **Cenário (1):** Outsourcing da solução de segurança da informação: **incluindo o fornecimento de toda solução como serviço,** ou seja, envolvendo hardware, software, assinaturas de atualização,

instalação, treinamento, customização, suporte técnico e manutenção. Contratação pelo período de 12 meses, de caráter continuado.

4.1.2. **Cenário (2)**: Aquisição da solução de segurança da informação: inclui a **aquisição** de todos os equipamentos e dos softwares, sem a contratação dos serviços de assinaturas de atualização, instalação, treinamento, customização, suporte técnico e manutenção, estes ficando a cargo da Administração, ou seja, todos os serviços a serem prestados em razão da aquisição de hardware e software deverão ser contratados à parte, através de novo processo.

4.1.3. **Cenário (3): Modelo Híbrido (Aquisição + Serviços Gerenciados):** A Administração adquire os equipamentos e softwares, mas contrata, junto ao fornecedor, um **pacote de serviços gerenciados** que inclui suporte técnico, atualizações, treinamento e manutenção, garantindo a continuidade operacional da solução.

4.2. A análise comparativa das soluções observou as seguintes diretrizes:

| Diretriz | Cenário 1 | Cenário 2 | Cenário 3 |
|---|---|---|---|
| Disponibilidade de solução de TIC similar em outro órgão ou entidade da Administração Pública | Encontramos a utilização deste modelo de solução de TIC em diversos outros editais e contratos da Administração Pública. | Encontramos a utilização deste modelo de solução de TIC em diversos outros editais e contratos da Administração Pública. | Não encontramos a utilização deste modelo de solução de TIC. |
| Alternativas do mercado, inclusive quanto a existência de software livre ou gratuito | Não se aplica. | Não se aplica. | Não se aplica. |
| A Solução está disponível no Portal do Software Público Brasileiro? (Quando se tratar de software) | Não se aplica. | Não se aplica. | Não se aplica. |
| A Solução é composta por software livre ou software público? (Quando se tratar de software) | Não se aplica. | Não se aplica. | Não se aplica. |
| A Solução é aderente às | Não se aplica. | Não se aplica. | |

| | | | |
|---|---|---|---|
| políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG? | | | Não se aplica. |
| Solução é aderente às regulamentações da ICP-Brasil? (Quandohouver necessidade de certificação digital) | Não se aplica. | Não se aplica. | Não se aplica. |
| A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (Quandoo objetivo da solução abranger documentos arquivísticos) | Não se aplica. | Não se aplica. | Não se aplica. |
| Necessidades de adequação do ambiente | Não é necessário adequar o ambiente do órgão ou entidade para implantar a solução. | Não é necessário adequar o ambiente do órgão ou entidade para implantar a solução. | Não é necessário adequar o ambiente do órgão ou entidade para implantar a solução. |
| Diferentes modelos de prestação dos serviços | Este modelo preconiza a contratação de solução através dos conceitos atuais de IAAS (infraestrutura como serviço). Tem sido amplamente utilizada, é estabelece a terceirização integral dos serviços.<br>Com esse modelo temos a atualização constante dos softwares, capacitação e atualização do time envolvido nos processos | Este modelo é estabelece a aquisição de toda a solução, agregando os equipamentos e softwares ao patrimônio, e mantém o encargo de gestão e controle da solução para o Estado.<br>O órgão não dispõe de equipe capacitada e em quantidade suficiente para a instalação, manutenção e operação dos equipamentos e | Este modelo é estabelece a aquisição de **PARTE** solução, agregando **PARTE** dos equipamentos e softwares ao patrimônio, e mantém o encargo de gestão e controle da solução para o Estado.<br>Dificuldade em coordenar fornecedores diferentes: A administração terá que gerenciar contratos distintos para |

| | | | |
|---|---|---|---|
| | de negócio, suporte 7 X 24 por conta do CONTRATADO, entre outros. | serviços necessários para esta contratação.<br>A SES/MS não dispõe de servidores com função de analistas de segurança da informação, que façam a pesquisa, investigação, desenvolvimento e homologação de soluções avançadas de segurança de rede, o que justifica buscar empresa especializada no mercado para esta finalidade;<br>O alto custo para fazer todo o serviço de suporte técnico, customização e manutenção da solução, a parte da aquisição dos hardwares e softwares, inviabiliza a solução. | equipamentos e serviços, o que pode gerar problemas de compatibilidade, responsabilidades fragmentadas e disputas contratuais.<br>Possíveis falhas na integração: Dependendo do nível de customização necessário, pode haver dificuldades na integração entre hardware, software e serviços gerenciados.<br>Aquisição inicial mais cara: Como a Administração está adquirindo os ativos, o investimento inicial pode ser mais alto do que um modelo totalmente terceirizado.<br>Custos de serviços podem escalar: Se os serviços forem contratados de forma avulsa ou por demanda, pode haver um custo acumulado maior ao longo do tempo, principalmente se houver necessidade de suporte especializado inesperado.<br>Possíveis dificuldades |

| | | | |
|---|---|---|---|
| | | | em trocas de fornecedores: Se a contratação dos serviços não for bem planejada, pode ocorrer uma dependência excessiva do mesmo fornecedor para suporte e manutenção. |
| Diferentes tipos de soluções em termos de especificação, composição ou características | Independente da solução a ser adotada, todas deverão possuir especificação e características semelhantes. Ou seja, os mesmos modelos de hardware e software, bem como dos serviços envolvidos, mudando apenas a forma de contratação das soluções. | Independente da solução a ser adotada, todas deverão possuir especificação e características semelhantes.<br>Ou seja, os mesmos modelos de hardware e software, bem como dos serviços envolvidos, mudando apenas a forma de contratação das soluções. | Independente da solução a ser adotada, todas deverão possuir especificação e características semelhantes.<br>Ou seja, os mesmos modelos de hardware e software, bem como dos serviços envolvidos, mudando apenas a forma de contratação das soluções. |
| Possibilidade de aquisição na forma de bens ou contratação como serviço | A solução prevê a contratação integralmente como serviço. | A solução prevê a aquisição (fornecimento) de bens, com prestação de serviços ( manutenções, suporte técnico, etc) feitos à parte (nova contratação). | A solução prevê a aquisição (fornecimento) de bens, com prestação de serviços ( manutenções, suporte técnico, etc). No modelo Hibrido. |
| Ampliação ou substituição da solução implantada | Ampliação e substituição viável, através de nova contratação ou aditivo ao contrato de prestação de serviços. Essa forma de contratação possibilita a | Ampliação viável, através de aquisição de novos bens. A substituição irá demandar nova aquisição e substituição de todo o patrimônio | Ampliação viável, através de aquisição de novos bens. Atualizações e evolução tecnológica não garantidas: Se o contrato de serviços gerenciados não prever |

| | | | |
|---|---|---|---|
| | atualização constante dos softwares envolvidos na solução, bem como dos servidores envolvidos no processo.<br>Tendo os serviços embutidos (manutenção, suporte técnico, customizações, etc, agregados à contratação de hardware e software possibilita ao estado uma redução nos custos operacionais, bem como facilitam a gestão e acompanhamento dos fiscais e gestores da contratação. | adquirido.<br>Necessário a aquisição de licenças a cada 12 ou 36 meses para manutenção do ambiente em funcionamento. | claramente atualizações contínuas de software e segurança, a Administração pode ficar com uma solução rapidamente defasada.<br>Obsolescência do hardware: Como a Administração compra os equipamentos, há o risco de a tecnologia se tornar obsoleta antes do fim da vida útil prevista, exigindo novos investimentos. |
| A solução possui gerenciamento simplificado centralizado com funções básicas de relatórios e histórico. | A solução atende a esse requisito | A solução atende a esse requisito | A solução atende a esse requisito |
| Interface WEB de gerência e configuração de toda solução. | A solução atende a esse requisito | A solução atende a esse requisito | A solução atende a esse requisito |
| Compatibilidade com software de gerência e análise de logs. | A solução atende a esse requisito | A solução atende a esse requisito | A solução atende a esse requisito |
| Suporte oficial do fabricante. | A solução atende a esse requisito | A solução não atende a esse requisito, devendo o serviço de suporte ser contratado a parte. | A solução não atende a esse requisito, devendo o serviço de suporte ser contratado a parte. |
| Garantia de funcionamento. | A solução atende a esse requisito | A solução atende a esse requisito | A solução atende a esse requisito |

| | | | |
|---|---|---|---|
| A solução é ou está defasada tecnologicamente ou não é adequada para a Administração Pública. | A solução é atual e adequada à administração pública | A solução é atual e adequada à administração pública | A solução é atual e adequada à administração pública |
| Treinamento e implantação oficial da solução | A solução atende a esse requisito | A solução não atende a esse requisito, devendo o serviço de treinamento e implantação ser contratado à parte. | A solução não atende a esse requisito, devendo o serviço de treinamento e implantação ser contratado à parte. |
| Suporte técnico especializado à solução | A solução atende a esse requisito | A solução não atende a esse requisito, devendo o serviço de suporte técnico especializado ser contratado à parte. | A solução atende a esse requisito |
| Manutenção preventiva, corretiva ou evolutiva da solução | A solução atende a esse requisito | A solução não atende a esse requisito, devendo o serviço de manutenção ser contratado à parte. | A solução atende PARTE desse requisito, devendo o serviço de manutenção ser contratado à parte. |

4.3. ANÁLISE COMPARATIVA DE CUSTOS

4.3.1. Uma vez detalhado o escopo, cenário ideal e requisitos técnicos mínimos para a solução de TIC em questão, foi realizada uma rápida pesquisa de contratações similares para os itens desta contratação. Bem, tem-se que para efetuar as pesquisas de preços devemos seguir algum ou todos os itens abaixo:

4.3.1.1. Composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços, observado o índice de atualização de preços correspondente;

4.3.1.2. Contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 01 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;

4.3.1.3. Dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 06 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso; ou

4.3.1.4. Pesquisa direta com, no mínimo, 03 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 06 (seis) meses de antecedência da data de divulgação do edital;

4.3.2. Vale destacar que a prática nos leva a priorizar os dois primeiros mecanismos. Lembremos, porém, que neste momento estamos, em princípio, realizando estudo preliminar, de forma que podemos utilizar quaisquer desses parâmetros, ou uma combinação deles, zelando sempre para que as estimativas estejam próximas à realidade do mercado. Independentemente, uma pesquisa de preços completa será formalizada, nos autos do processo quando da estimativa do preço final da contratação.

4.3.3. Abaixo, segue a tabela com contratações similares, à guisa de ilustrar as possibilidades de contratação:

| Pregão Eletrônico | Órgão | Objeto | Complemento | Valor de Referência | Vigência do Contrato | Tipo | Valor Anual (12 meses) |
|---|---|---|---|---|---|---|---|
| PREGÃO ELETRÔNICO N. 0006/2021 | SEFAZ/MS | O objeto da presente licitação é a contratação de empresa especializada em para fornecimento de solução envolvendo hardware, software, assinaturas de atualização, instalação, treinamento, customização e suporte em proteção e otimização de tráfego em redes wan e proteção multicamadas contra ameaças avançadas em mensagens | Contratação de solução envolvendo hardware, software, assinaturas de atualização, instalação, treinamento, customização e suporte em proteção e otimização de tráfego em redes wan e proteção multicamadas contra ameaças avançadas em mensagens | R$ 2.504.736,00 | 12 (doze) meses | **Locação** | R$ 2.504.736,00 |
| PREGÃO ELETRÔNICO Nº 09/2023 | Ministério da Justiça e Segurança Pública (UASG 200005) | O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses, com vistas a atender às necessidades do Ministério da Justiça e Segurança Pública - MJSP. | Contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses.<br>09 Appliances de Firewall NGFW com aquisição de suporte e garantia, 01 Appliance de Análise de Tráfego de Dados e 01 Appliance Virtual de Gerenciamento Centralizado. | R$ 6.007.067,50 | 12 (doze) meses | **Aquisição** | R$ 6.007.067,50 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PREGÃO ELETRÔNICO Nº 106/2024 | Secretaria Municipal de Tecnologia e Inovação - SEMTI | Registro de Preços para eventual contratação de empresa(s) especializada(s) em Soluções de Segurança para Perímetro de Rede e Defesa Cibernética (Firewall) e Contratação de Serviços de Centro de Operações de Segurança (Security Operations Center - SOC) para atendimento das necessidades tecnológicas e de segurança do ambiente de rede da Prefeitura Municipal de Vila Velha – PMVV. | Lote 01: Aquisição de Solução de Segurança de Proteção do Perímetro de Rede com características de Next Generation Firewall (NGFW).<br>Lote 02: Contratação de Serviços de Centro de Operações de Segurança (Security Operations Center - SOC).<br>Todas as soluções deverão ter garantia de 36 meses. | R$ 23.791.446,32 | ARP 12 (doze) meses Contrato 36 (trinta e seis) meses | **Aquisição** | R$ 7.930.482,11 |
| PREGÃO ELETRÔNICO Nº 48/2024 | Tribunal de Contas da União - TCU | Contratação de serviços gerenciados de segurança, incluindo administração, monitoramento, resposta a incidentes de segurança da informação e capacitação, por 60 (sessenta) meses. | Serviços de Firewall Externo e Interno, Firewall em Site Remoto, Firewall em Nuvem, Firewall de Aplicação Externo e Interno, Firewall de Aplicação em Nuvem, Monitoramento e Resposta a Incidentes de Segurança, Inteligência e Desenvolvimento em SIEM, Capacitação em Firewall e Capacitação em Firewall de Aplicação. | R$ 31.811.220,81 | 60 (sessenta) meses | **Locação** | R$ 6.362.244,16 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS Nº 034/2021 | Serviço de Apoio às Micro e Pequenas Empresas de São Paulo - SEBRAE-SP | Contratação de empresa especializada em serviço de operação e monitoramento da solução de segurança da informação do SISTEMA SEBRAE, compreendendo serviço de gestão de vulnerabilidades, serviço de monitoramento de ataques cibernéticos, serviço de respostas aos incidentes de segurança e de privacidade, serviço de operações e respostas às requisições, serviço de governança, risco e conformidade de segurança e privacidade em ti, serviço de continuidade de negócio, serviço de testes de invasão, serviço de criptografia de disco, serviço de prevenção contra vazamento de informações em endpoints, serviço de controle de acesso à rede, serviço de descoberta e mapeamento de dados pessoais e sensíveis, serviço de gestão de consentimento e cookies, serviço de distribuição inteligente de fluxo de aplicações e segurança de aplicações web, serviço de anonimização e proteção de dados, serviço de inteligência aplicado à segurança e serviços técnicos especializados, por 12 (doze) meses | Outsourcing da solução de segurança da informação: incluindo o fornecimento de toda solução como serviço | R$ 149.914.775,16 | 12 (doze) meses | **Serviço** | R$ 12.492.897,93 |

4.3.4. Conforme apresentado no quadro acima, a opção de locação de equipamentos associada à serviços é a que apresenta a maior vantajosidade econômica, onde a média de valores praticados se encontra bem abaixo dos valores praticados na forma de aquisição de equipamentos. Também é importante frisar, que a locação de equipamentos associada a serviços é prática usual de mercado.

## 5. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

5.1. SOLUÇÃO ADOTADA

5.1.1. Dentre as soluções passíveis de atendimento as necessidades levantadas, optamos pela constante no **Cenário 1**: Outsourcing da solução de segurança da informação: incluindo o fornecimento de solução como serviço, envolvendo hardware, software, assinaturas de atualização, instalação, treinamento, customização, suporte técnico e manutenção.

5.1.2. O outsourcing de segurança refere-se à prática de delegar a terceiros a responsabilidade pela proteção de redes e sistemas de informação de uma organização. Essa abordagem permite que as empresas se concentrem em suas atividades principais, enquanto especialistas em segurança gerenciam e monitoram suas infraestruturas de TI.

5.1.3. O outsourcing pode incluir serviços como monitoramento de redes, resposta a incidentes, gerenciamento de vulnerabilidades e conformidade com regulamentações de segurança, além da locação dos equipamentos necessários para a prestação destes serviços.

5.1.4. Um dos principais benefícios do outsourcing de segurança é a redução de custos operacionais. Ao contratar provedores especializados, as empresas podem evitar os altos custos associados à contratação e treinamento de uma equipe interna de segurança. Além disso, esses provedores geralmente têm acesso a tecnologias avançadas e conhecimentos atualizados sobre as últimas ameaças, o que pode melhorar significativamente a postura de segurança da organização.

5.2. Descrição do objeto:

5.2.1. Contratação de empresa especializada para fornecimento de serviços de segurança da informação envolvendo solução de hardware, software, assinaturas de atualização, instalação, treinamento, customização e suporte técnico qualificado em proteção e inspeção de tráfego em redes corporativas, conforme especificações técnicas, incluindo os appliances necessários e suficientes para a prestação destes serviços, com o objetivo de garantir a proteção eficaz da rede de computadores, assim como a segurança das estações de trabalho, servidores de arquivos e dispositivos móveis, por meio de soluções antimalware endpoint com detecção e resposta de última geração, para atender a demanda da Secretaria de Estado de Saúde de Mato Grosso do Sul, SES/MS, pelo período de 12 (doze) meses.

5.3. JUSTIFICATIVA DA ESCOLHA DA SOLUÇÃO

5.3.1. A solução escolhida é a proposta no Cenário 1, que é o outsourcing da solução de segurança da informação, pois a alternativa observada no Cenário 2, Aquisição da solução de segurança da informação, não se mostra vantajosa nos seguintes aspectos:

5.3.1.1. As tecnologias de informação, no caso as de proteção e segurança da informação são constantemente atualizadas, com novas assinaturas de combate e prevenção de ameaças, disponibilização de novos recursos, atualização dos recursos existentes e atualização dos filtros de conteúdo. Adquirir os equipamentos não garante essa atualização constante, o que em curto período de tempo tornariam os ativos adquiridos obsoletos e inservíveis, obrigando a SES/MS a substituir constantemente a tecnologia já implantada, sob o risco de não garantir a proteção e continuidade de serviços necessária;

5.3.1.2. Os licenciamentos dos equipamentos que compõem a solução possuem validade de 12 (doze) até 36 (trinta e seis) meses, o que demandaria após essa janela de período, abertura de outro processo para aquisição de novas licenças, garantindo, desta forma, o pleno funcionamento da solução de segurança da informação.

5.3.1.3. Caso os equipamentos permaneçam sem a devida licença durante um determinado período, poderia comprometer todo o ambiente de TIC desta Coordenadoria de Tecnologia de Informática e Informação, tornando-o mais vulnerável perante aos diversos tipos de ataques, tentativas de invasões e tentativas de sequestro de dados que são realizadas diuturnamente aos mais diversos órgãos públicos que ofertam serviços de TI por meio da rede mundial de computadores.

5.3.1.4. A Solução a ser contratada, constante nesse estudo, tem caráter continuado, tendo em vista que se trata de objeto com características intrínsecas de essencialidade e habitualidade, cuja eventual paralisação da atividade contratada implica em prejuízo ao exercício das atividades da Contratante. Neste aspecto, o objeto contratado é configurado pela necessidade de prestação de modo permanente, e a necessidade desta estende-se continuamente, por mais de um exercício financeiro.

5.3.2. Por outro lado, a contratação da solução por meio de outsourcing, Cenário 1, garantirá inúmeros benefícios, podendo citar alguns:

5.3.2.1. Proporcionar a gestão efetiva do serviço de locação de acordo com a demanda, que, em consequência, possibilita a obtenção de indicadores de qualidade, desempenho, disponibilidade, utilização de recursos e custos de forma mais ágil e exata, permitindo melhor planejamento, tomadas de decisão e ações rápidas, cada vez mais demandadas pelas Unidades, especialmente aquelas finalísticas;

5.3.2.2. Reduzir de forma drástica as interrupções do serviço devido as manutenções corretivas, através da implantação e aplicação de acordos de níveis de serviço (Service Level Agreement - SLA);

5.3.2.3. Proporcionar o licenciamento de todos os equipamentos e softwares durante toda a vigência contratual, sendo de responsabilidade da empresa contratada efetuar a aplicação das licenças necessárias durante esse período;

5.3.2.4. O serviço de operação, manutenção e monitoramento da solução ofertada, neste caso, ficará a cargo da contratada, que alocará os técnicos especializados e treinados na solução para realizar as atividades de instalação, manutenção, operação e troubleshooting. Ficando a cargo da SES/MS, a fiscalização dos serviços prestados e gestão do contrato.

5.4. BENEFÍCIOS A SEREM ALCANÇADOS

5.4.1. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

5.4.2. Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;

5.4.3. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;

5.4.4. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.

5.4.5. Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.

5.4.6. Criação de políticas de proteção da rede contra eventuais ataques de usuários mal-intencionados através do fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;

5.4.7. Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);

5.4.8. Melhor filtro de conteúdo URL, sancionando acesso a sites indesejados de conteúdo ilícito.

5.4.9. A Solução a ser contratada, constante nesse estudo, tem caráter continuado, tendo em vista que se trata de objeto com características intrínsecas de essencialidade e habitualidade, cuja eventual paralisação da atividade contratada implica em prejuízo ao exercício das atividades da Contratante. Neste aspecto, o objeto contratado é configurado pela necessidade de prestação de modo permanente, e a necessidade desta estende-se continuamente, por mais de um exercício financeiro.

## 6. ESTIMATIVA DAS QUANTIDADES

6.1. O dimensionamento da solução pretendida foi realizado com base no cenário levando em consideração as necessidades atuais da infraestrutura e com provisionamento para futuras ampliações no ambiente da CTEC/SES/MS.

6.2. Para todos os serviços pretendidos, foram elencadas capacidades mínimas requeridas, em termos de disponibilidade, funcionalidades e desempenho. Assim, o desempenho dos equipamentos e softwares alocados deverão atender as exigências especificadas com todas as funcionalidades habilitadas. Por outro lado, a capacidade de processamento de tráfego de rede foi levantada em consideração, estimando o crescimento esperado em um horizonte de 60 (sessenta) meses, em termos de volume e complexidade de tratamento.

6.3. As quantidades a serem contratadas foram definidas da seguinte forma:

6.3.1. 01 (um) cluster de equipamentos do Tipo I, formado por Appliances NGFW com no mínimo 02 (dois) nodes cada cluster, em ambiente de alta disponibilidade (High-availability clusters), implementação de proteção de perímetro no Data Center da SES/MS, utilizado para acesso aos serviços públicos digitais, que fazem o uso dos serviços públicos digitais prestados pela Secretaria de Estado de Saúde de Mato Grosso do Sul, com aplicação de filtro de conteúdo, regras de firewall, inspeção de tráfego SSL/TLS, proteção anti-maware, anti-spyware, prevenção de intrusão e VPN Site-to-Site, SSL, Client-to-Site;

6.3.1.1. Para o cluster será exigido no mínimo 02 (dois) nodes, em ambiente de alta disponibilidade (High-availability clusters), devido à criticidade do ambiente a ser mantido, considerando que a totalidade dos serviços públicos da Secretaria de Estado de Saúde de Mato Grosso do Sul serão protegidos pela solução proposta. Neste cenário, caso um equipamento apresente falha de funcionamento, o outro assumirá a operação integralmente e manterá a disponibilidade dos serviços, sem gerar qualquer interrupção no funcionamento e acesso aos serviços públicos disponibilizados via internet.

6.3.2. 03 (três) equipamentos para solução de proteção de perímetro Tipo II, formado por Appliances, para implementação de proteção de perímetro nas unidades de Auditoria, Lacen e Hemosul, vinculadas à da Secretaria de Estado de Saúde de Mato Grosso do Sul, utilizado para promover o acesso dos servidores públicos à rede mundial de computadores, Internet, com aplicação de filtro de conteúdo, regras de firewall, inspeção de tráfego SSL/TLS, proteção anti-maware, anti-spyware, prevenção de intrusão e VPN Site-to-Site, SSL, Client-to-Site.

6.3.3. 30 (trinta) equipamentos para solução de proteção de perímetro Tipo III, formado por Appliances, para implementação de proteção de perímetro nas unidades remotas de pequeno porte, vinculadas à da Secretaria de Estado de Saúde de Mato Grosso do Sul, utilizado para promover o acesso dos servidores públicos à rede mundial de computadores, Internet, com aplicação de filtro de

conteúdo, regras de firewall, inspeção de tráfego SSL/TLS, proteção anti-maware, anti-spyware, prevenção de intrusão e VPN Site-to-Site, SSL, Client-to-Site;

6.3.4. Solução de Firewall de Aplicações Web – Web Application Firewall (WAF), para proteção de pelo menos 200 milhões de requisições WEB por ano, para implementação de proteção de aplicações no Data Center da Secretaria de Estado de Saúde de Mato Grosso do Sul, utilizado para implementação de proteção de aplicações e prevenção de ataques como SQL injection, filtragem de scripts maliciosos, bloqueios de inclusão de arquivos maliciosos de forma remota, proteção contra ataques de força bruta, proteção contra bots maliciosos, proteção contra exploits de dia zero e ataques de dia zero, prevenção a vazamento de dados e prevenção de fraudes;

6.3.5. 2.000 (duas mil) licenças para Solução para Proteção de Endpoints, para implementação de proteção Endpoint, que serão instaladas nas estações de trabalho e servidores de rede da Secretaria de Estado de Saúde de Mato Grosso do Sul, considerando que a SES/MS possui cerca de 1.750 (mil e setecentos e cinquenta) computadores em seu parque de equipamentos de informática, e 250 (duzentos e cinquenta) licenças de Módulo de Detecção e Resposta Gerenciada - MDR para Solução para Proteção de Endpoints, a ser utilizada especificamente para os servidores de rede da SES/MS, que conta atualmente com 250 (duzentos e cinquenta) servidores de rede, entre físicos e virtuais, em seu parque de equipamentos de informática.

6.3.5.1. Parque de computadores, também conhecido como parque tecnológico, é a estrutura de TI de uma empresa ou órgão, que inclui hardwares, softwares, redes, sistemas de armazenamento e bancos de dados, ou seja diz respeito a toda estrutura de TI que uma empresa tem em suas mãos.

6.3.6. O licenciamento para todas as Soluções de Proteção de Perímetro, Solução para Proteção de Endpoints e Solução de Firewall de Aplicações Web deverão permanecer válidas durante toda a vigência do contrato;

## 7. ESTIMATIVA DO VALOR DA CONTRATAÇÃO E DOTAÇÃO ORÇAMENTÁRIA

7.1. A definição e documentação da estimativa de preços referenciais foram baseadas na média de valores encontradas para o tipo de aquisição que se pretende (apresentados no item 4.3.3), que são:

| Pregão Eletrônico | Órgão | Objeto | Tipo | Valor Anual (12 meses) |
|---|---|---|---|---|
| PREGÃO ELETRÔNICO N. 0006/2021 | SEFAZ/MS | O objeto da presente licitação é a contratação de empresa especializada em para fornecimento de solução envolvendo hardware, software, assinaturas de atualização, instalação, treinamento, customização e suporte em proteção e otimização de tráfego em redes wan e proteção multicamadas contra ameaças | Locação | R$ 2.504.736,00 |

| | | | | |
|---|---|---|---|---|
| | | avançadas em mensagens | | |
| PREGÃO ELETRÔNICO Nº 48/2024 | Tribunal de Contas da União - TCU | Contratação de serviços gerenciados de segurança, incluindo administração, monitoramento, resposta a incidentes de segurança da informação e capacitação, por 60 (sessenta) meses. | Locação | R$ 6.362.244,16 |
| Pregão Eletrônico N° 90026/2024 | INST.NAC.DE METROLOGIA QUALIDADE E TECNOLOGIA | Subscrições e expansão das soluções de Next Generation Firewall (NGFW) com Serviços de Operação de Segurança | Locação | R$ 3.383.880,6400 |

7.2. O valor global previamente estimado da presente contratação, através da média de valores obtidos em processos de mesma natureza, é de R$4.083.620,27 (Quatro Milhões, oitenta e três mil, seiscentos e vinte reais e vinte e sete centavos).

7.3. O valor previamente estimado procede do parâmetro de pesquisa (mapa comparativo de preços) previsto na legislação estadual regulamentadora dos procedimentos básicos para a realização da pesquisa de preços para a aquisição de bens e contratação de serviços em geral para o Estado do Mato Grosso do Sul (Decreto n. 15.940/2022). Ao passo que, utilizando-se recursos da União decorrentes de transferências voluntárias, será observado o disposto na IN SEGES/ME nº 65, de 7 de julho de 2021.

7.4. As despesas decorrentes da contratação da presente licitação correrão à conta da seguinte Dotação Orçamentária:

| Funcional Programática | Natureza de Despesa | Fonte de Recurso | Exercício |
|---|---|---|---|
| 20.27901.10.302.2200.6009.0002 | 33904057 | 50010021 | 2025 |

7.5. A Contratante reserva-se no direito de, a seu critério, utilizar ou não a totalidade da reserva orçamentária prevista.

7.6. As despesas efetuadas no próximo exercício correrão à conta do respectivo orçamento, dentro da mesma programação financeira.

## 8. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

8.1. É sabido que o parcelamento da solução é a regra, devendo a licitação ser realizada por item sempre que o objeto for divisível, desde que se verifique não haver prejuízo para o conjunto da

solução ou perda de economia de escala, visando propiciar a ampla participação de licitantes, que embora não disponham de capacidade para execução da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas.

8.2. Contudo, a contratação dos serviços em apreço em item único sem parcelamento é a que melhor atende as necessidades da Secretaria de Estado de Saúde de Mato Grosso do Sul (SES/MS), pelas razões seguintes:

8.2.1. A solução deve ser contratada de maneira completa, pois perfazem uma única solução, uma vez que os equipamentos devem ser compatíveis entre si e com os softwares de gerenciamento. Ao fragmentar as contratações, não será possível garantir a compatibilidade dos itens de hardware e dos softwares a serem instalados;

8.2.2. Por se tratar de uma solução integrada, constituída por funcionalidades e serviços intrinsecamente ligados entre si, e considerando que todos os componentes devem ser de um mesmo fabricante, bem como, o serviço de suporte que devem ser realizados por profissional especializado na solução, não há viabilidade técnica para o parcelamento da solução por itens;

8.2.3. Não avaliamos restrição de mercado ao adquirir a solução de maneira global, visto que individualmente tratam-se de bens e materiais de uso comum e de requisitos padronizados, não havendo dificuldade das empresas em providenciar os bens e prestar os serviços requisitados;

8.2.4. No caso em análise, os serviços citados são indivisíveis, não havendo possibilidade de contratar o suporte técnico e a manutenção de fornecedores diferentes, tendo em vista que são serviços caracterizados pela interoperabilidade e interdependência, pois corriqueiramente as manutenções realizadas derivam de suporte técnico demandado, ou que demandam suporte técnico para sua correta implantação.

8.3. CONSÓRCIO

8.3.1. Não será permitida a participação de empresas reunidas em consórcio, pelas seguintes razões:

8.3.1.1. O presente certame licitatório tem por objeto contratação de solução de hardware, software, assinaturas de atualização, instalação, treinamento, customização e suporte técnico qualificado em proteção e inspeção de tráfego em redes corporativas, no valor estimado de R$4.083.620,27 (quatro milhões, oitenta e três mil, seiscentos e vinte reais e vinte e sete centavos), tratando-se de serviço comum (art. 6ª, inciso XIII[1], da Lei Federal n. 14.133/2021) e o valor estimado de cada item não se enquadrar no conceito de grande vulto (art.6ª, inciso XXII[1], da Lei Federal n. 14.133/2021);

8.3.1.2. A permissão de participação de empresas e consórcio é recomendável quando diante de objeto complexo, vultoso, que exija alta capacidade técnica ou econômico-financeira.

8.3.1.3. Inclusive, nesse sentido mantém-se o entendimento da doutrina brasileira, como bem destacado por Marcelo Loureiro:

> *"A participação dos consórcios em licitações públicas sempre deve ser analisada tomando-se como norte a competição. Recomenda-se tal permissão em caso de objeto complexo, vultoso, que exija alta capacidade técnica ou econômico-financeira. (Tratado da Nova Lei de Licitações e Contratos Administrativos: Lei 14133/21 comentada por advogados públicos." Organizador Leandro Sarai. 2 ed. São Paulo: Juspodvm,* 2022, p. 305-306).

8.3.1.4. Ademais, como bem destacado no Parecer PGE/MS/CJUR-SEL n. 009/2023 (aprovado pela Decisão PGE/MS/GAB n. 101/2023), podem ser verificados efeitos negativos e positivos na utilização do consórcio, já que essa adoção pode propiciar dominação de mercado, em oportunidades nas quais empresas se aliam para diminuir a competitividade do certame, dificultando ou, até mesmo, impedindo a participação de outras empresas; bem como pode ser instrumento necessário para permitir uma competição mais saudável, ao facultar a conjugação de esforços no caso de empresas que disponham de expertise em apenas um dos ramos necessários para execução do objeto.

8.3.1.5. No presente caso, está-se diante de uma licitação que tem por objeto contratação de solução tecnológica através de pregão, portanto, não serão executadas atividades de ramos distintas, razão pela qual a participação de empresas em consórcio não é a medida mais adequada para concretização do princípio da ampla competividade. Ao contrário, a previsão de empresas reunidas em consórcio para consecução do objeto que pretende contratar poderá ensejar o domínio no mercado e culminar contratação desvantajosa para a Administração Pública.

8.3.1.6. Ademais, na presente contratação, não se está se exigindo alta capacidade técnica ou econômico-financeira por parte do licitante a justificar a reunião das empresas em consórcio.

8.3.1.7. Assim, a participação de consórcio não garante e/ou amplia a competitividade, ao contrário, pode até restringir a concorrência em razão (i) da inexistência de complexidade do objeto que se propõe a contratar (ou seja, cuida-se de bem comum), (ii) de não se estar diante de futura contratação enquadrada no conceito como "de grande vulto", (iii) do fato de o objeto a ser contratado não envolver ramos de atividades diversos.

8.3.1.8. Sendo assim, cuida-se o presente certame licitatório de aquisição de bem comum e não se enquadrando no conceito legal de contratação de grande vulto, será vedada a participação de empresas em consórcio.

8.4. SUBCONTRATAÇÃO

8.4.1. NÃO será admitida a subcontratação do objeto contratual.

8.4.1.1. A decisão de não permitir a subcontratação para o objeto em questão, qual seja, a contratação de serviços especializados em segurança da informação para a Secretaria de Estado de Saúde de Mato Grosso do Sul (SES/MS), fundamenta-se em uma análise técnica criteriosa à luz da Lei nº 14.133/2021, especificamente em seu artigo 72, § 4º, inciso II.

8.4.1.2. Considerando a natureza intrinsecamente especializada e predominantemente intelectual dos serviços a serem contratados, entende-se que a execução integral do objeto requer um nível de expertise, conhecimento técnico específico e experiência comprovada que, em sua totalidade, justificam a vedação da subcontratação.

8.4.1.3. Os serviços de segurança da informação, conforme detalhado no Termo de Referência, abrangem desde a implementação de soluções complexas de hardware e software até a customização, treinamento e suporte técnico qualificado em proteção e inspeção de tráfego em redes corporativas. A eficácia dessas soluções e a segurança dos dados sensíveis da Secretaria de Saúde dependem diretamente da capacidade e da qualificação da empresa contratada em todas as etapas do serviço.

8.4.1.4. Permitir a subcontratação, mesmo que parcial, poderia comprometer a qualidade, a segurança e a integridade dos serviços prestados, pelos seguintes motivos:

8.4.1.4.1. **Serviços Técnicos Especializados de Natureza Predominantemente Intelectual:** A atividade principal deste contrato reside na aplicação de conhecimento técnico especializado em segurança da informação, envolvendo análise de riscos, configuração de sistemas complexos, implementação de políticas de segurança, detecção e resposta a ameaças cibernéticas. Estas são atividades de natureza eminentemente intelectual que exigem um corpo técnico altamente qualificado e com experiência comprovada na área.

8.4.1.4.2. **Confiança e Responsabilidade:** A segurança da informação de uma instituição como a Secretaria de Estado de Saúde envolve a proteção de dados sensíveis e críticos. A relação de confiança e a responsabilização pela integridade e confidencialidade desses dados devem recair diretamente sobre a contratada, selecionada por suas qualificações e capacidade técnica. A subcontratação poderia diluir essa responsabilidade e dificultar a fiscalização e a responsabilização em caso de falhas de segurança.

8.4.1.4.3. **Treinamento e Customização Específicos:** O treinamento e a customização das soluções de segurança são partes integrantes e cruciais para o presente estudo. Estes exigem um profundo conhecimento das especificidades da rede e dos sistemas da SES/MS, bem como da solução implementada. A subcontratação dessas etapas poderia levar a uma perda de sinergia e de qualidade na entrega final.

8.4.1.4.4. **Suporte Técnico Qualificado:** O suporte técnico qualificado é essencial para a manutenção da segurança e para a resolução de incidentes. A subcontratação desta etapa poderia resultar em um atendimento menos eficiente e com menor conhecimento específico sobre a solução implementada, impactando a capacidade da SES/MS de responder a ameaças de forma ágil e eficaz.

8.4.1.4.5. **Seleção do Licitante:** A escolha da empresa vencedora do processo licitatório se baseia na avaliação de suas qualificações técnicas, sua experiência e sua proposta de solução.

Permitir a subcontratação poderia desvirtuar o processo seletivo, permitindo que uma empresa que não possua as qualificações necessárias execute parte significativa do contrato.

8.4.1.5. Diante do exposto, e considerando a criticidade dos serviços de segurança da informação para a Secretaria de Estado de Saúde de Mato Grosso do Sul, a não aceitação da subcontratação se mostra como medida essencial para garantir a execução adequada, segura e eficaz do objeto contratual, em consonância com o interesse público e com a legislação vigente.

## 9. CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES

9.1. Não se aplica contratações correlatas e/ou interdependentes.

## 10. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO

10.1. Não foram identificadas necessidades de adequação do ambiente para execução contratual, em relação ao modelo que já é adotado.

## 11. POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS DE TRATAMENTO

11.1. Embora não se identifiquem riscos ambientais diretos e significativos nesta aquisição, é importante ressaltar que a CONTRATADA deverá estar ciente da legislação ambiental pertinente e que deverá adotar as melhores práticas para mitigar qualquer potencial impacto que possa surgir, mesmo que de baixa probabilidade.

11.2. As principais leis que regem os possíveis impactos ambientais e as respectivas medidas de tratamento, são:

11.2.1. Lei Federal nº 6.938/81 (Política Nacional do Meio Ambiente):

11.2.1.1. Esta é a lei fundamental que estabelece a Política Nacional do Meio Ambiente, seus princípios, objetivos e instrumentos para a preservação e melhoria da qualidade ambiental. Embora o objeto da contratação não envolva atividades industriais diretas de grande impacto, esta lei é a base para qualquer discussão sobre responsabilidade ambiental e a necessidade de adoção de práticas sustentáveis. O princípio da precaução, norteador desta lei, implica que mesmo diante da incerteza científica sobre potenciais impactos, medidas preventivas devem ser consideradas.

11.2.1.2. Possíveis Impactos Ambientais:

11.2.1.2.1. Geração de Resíduos de Equipamentos Eletroeletrônicos (REEE): A substituição e descarte dos equipamentos de hardware (appliances, estações de trabalho, servidores, dispositivos móveis) ao final de sua vida útil ou em caso de atualização tecnológica podem gerar REEE, que contêm substâncias tóxicas e exigem tratamento e destinação adequados.

11.2.1.2.2. Consumo de Energia Elétrica: A operação dos equipamentos de hardware (servidores, appliances) e das estações de trabalho consome energia elétrica, cuja geração pode ter impactos ambientais (emissão de gases de efeito estufa, uso de recursos naturais).

11.2.1.2.3. Embalagens: O fornecimento dos equipamentos e softwares pode envolver a utilização de embalagens, cuja produção e descarte também geram impactos ambientais.

11.2.1.3. Medidas de Tratamento:

11.2.1.3.1. **Gerenciamento Adequado de REEE:** A contratada e a Secretaria de Estado de Saúde devem garantir que o descarte dos equipamentos obsoletos seja realizado de acordo com a legislação específica, como a Lei nº 12.305/10 (Política Nacional de Resíduos Sólidos) e seus regulamentos. Isso inclui a destinação para reciclagem ou para empresas especializadas em tratamento de REEE.

11.2.1.3.2. **Eficiência Energética:** Priorizar a aquisição de equipamentos com certificações de eficiência energética (como o selo Procel) pode reduzir o consumo de energia elétrica e, consequentemente, o impacto ambiental indireto. Otimizar a configuração dos equipamentos e adotar práticas de uso consciente da energia também são medidas importantes.

11.2.1.3.3. **Minimização e Destinação Correta de Embalagens:** Incentivar o uso de embalagens recicláveis e a correta separação para coleta seletiva, tanto por parte da empresa contratada no fornecimento dos produtos quanto pela Secretaria no descarte.

11.2.2. Lei Federal nº 12.305/10 (Política Nacional de Resíduos Sólidos):

11.2.2.1. Esta lei estabelece princípios, objetivos, instrumentos e diretrizes relativos à gestão e ao gerenciamento de resíduos sólidos, incluindo os REEE. Ela prevê a responsabilidade compartilhada pelo ciclo de vida dos produtos e a logística reversa, que pode ser aplicável ao descarte dos equipamentos eletrônicos.

11.2.2.2. **Possíveis Impactos Ambientais:** (Já mencionados acima, relacionados à geração e descarte inadequado de REEE)

11.2.2.3. Medidas de Tratamento:

11.2.2.3.1. **Implementação de Programas de Logística Reversa:** A Secretaria de Estado de Saúde, em conjunto com a contratada, pode implementar programas de logística reversa para o recolhimento e destinação ambientalmente adequada dos equipamentos eletrônicos ao final de sua vida útil.

11.2.2.3.2. **Priorização de Fornecedores com Práticas Sustentáveis:** Ao selecionar a empresa contratada, a Secretaria pode considerar critérios de sustentabilidade, como a adoção de práticas de gestão ambiental e a comprovação da destinação correta de resíduos.

11.3. Em suma**,** embora o objeto principal da contratação seja a segurança da informação, existem potenciais impactos ambientais indiretos relacionados ao ciclo de vida dos equipamentos eletrônicos e ao consumo de energia. A observância da Lei nº 6.938/81 e da Lei nº 12.305/10, juntamente com a legislação estadual e municipal pertinente, é crucial para garantir que a aquisição e a prestação dos serviços sejam realizadas de forma ambientalmente responsável, adotando as melhores práticas para

mitigar quaisquer impactos potenciais. A menção dessas leis no documento demonstra a preocupação e o compromisso da Secretaria de Estado de Saúde com a sustentabilidade.

## 12. MODELO DE GESTÃO E FISCALIZAÇÃO DO CONTRATO

12.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo gestor e fiscal do contrato, ou pelos respectivos substitutos, observado o disposto no art. 117 da Lei Federal nº 14.133, de 2021 e o respectivo regulamento do Decreto Estadual nº 15.938, de 2022.

12.2. Compete ao gestor do contrato o exercício das atribuições descritas no art. 15 do Decreto Estadual nº 15.938, de 2022.

12.3. Compete ao fiscal do contrato o exercício das atribuições descritas no art. 16 do Decreto Estadual nº 15.938, de 2022.

12.4. Os responsáveis pela gestão e fiscalização do contrato serão designados nos termos do art. 6º, 7º e 8º, todos do Decreto Estadual nº 15.938, de 2022.

12.5. São indicados para posterior designação e publicação em Diário Oficial Eletrônico, os seguintes servidores:

| ***Gestor de Contrato*** | ***Fiscal de Contrato*** |
|---|---|
| Nome: Marcos Espindola de Freitas<br>Cargo: Coordenado de Tecnologia da Informação<br>Matrícula: 56325023<br>E-mail: marcos.freitas @saude.ms.gov.br | Nome: Alessandro V. Fernandes<br>Cargo: Assistente de Serv. de Saúde<br>Matrícula: 129943024<br>E-mail: afernandes@saude.ms.gov.br |
| ***Substituto do Gestor*** | ***Substituto do Fiscal*** |
| Nome: Susi Meire Cabrera G. Massulo<br>Cargo: Gestor Serv. Saúde/Analista de Sistemas.<br>Matrícula: 89859021<br>E-mail: susi.massulo @saude.ms.gov.br | Nome: José Horácio P. Figueredo<br>Cargo: Analista de Tecn. da Informação<br>Matrícula: 71701024<br>E-mail: jose.figueredo@saude.ms.gov.br |

12.6. Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas:

12.7. No cumprimento de suas funções e/ou obrigações, o gestor e o fiscal deverão observar as disposições do Decreto Estadual n. 15.938/2022 e da Lei 14.133/2021.

12.8. O contratado será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante, conforme dispõe o art. 120, da Lei n. 14.133/2021.

12.9. O fiscal do contrato anotará em registro próprio todas ocorrências relacionadas com a execução do contrato, determinando o que for necessário para a regularização das faltas ou dos defeitos observados, conforme dispõe o art. 117, § 1° da Lei n. 14.133/2021.

12.10. O fiscal do contrato informará a seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência.

12.11. A eventual contratação de terceiros não eximirá de responsabilidade o fiscal do contrato, nos limites das informações recebidas do terceiro contratado.

12.12. A contratada permitirá e oferecerá condições para a mais ampla e completa fiscalização, durante a vigência do contrato, fornecendo informações, propiciando o acesso à documentação pertinente e atendendo às observações e exigências apresentadas pela fiscalização.

12.13. A Contratada se obriga a permitir que a auditoria interna da Contratante e/ou auditoria externa por ela indicada tenha acesso a todos os documentos que digam respeito ao Contrato.

12.14. A Contratante realizará avaliação da qualidade do objeto contratado, dos resultados concretos dos esforços despendidos pela Contratada e dos benefícios decorrentes da contratação.

12.15. A avaliação será considerada pela Contratante para aquilatar a necessidade de solicitar à Contratada que melhore a qualidade dos serviços prestados, para decidir sobre a conveniência de renovar ou, a qualquer tempo, rescindir o Contrato ou, ainda, para fornecer, quando solicitado pela Contratada, declarações sobre seu desempenho, a fim de servir de prova de capacitação técnica em contratações públicas.

## 13. CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

13.1. A licitação será realizada em único item.

13.2. O critério de julgamento adotado será o menor preço do item/maior desconto, observadas as exigências contidas no Edital e seus Anexos quanto às especificações do objeto.

## 14. DECLARAÇÃO DA VIABILIDADE OU NÃO DA CONTRATAÇÃO

14.1. Conforme observado nos elementos expostos acima neste Estudo, verifica-se que há viabilidade técnica e econômica na contratação do serviço especificados no item 3.2, por meio de processo de licitação, a qual atenderá às necessidades já elencadas no item 1. No que tange à modalidade de contratação do objeto escolhido, é considerada dotada de viabilidade a contratação na modalidade Pregão Eletrônico.

14.2. A escolha do pregão como modalidade licitatória decorre do fato de que o serviço a ser contratado, classifica-se como comum, pois possuem especificações usuais de mercado e padrões de qualidade definidos neste instrumento, nos termos do art. 6º, inciso XIII, da Lei n. 14.133/2021. Portanto, a utilização da modalidade de Pregão Eletrônico se impõe em razão do disposto no art. 2º, do Decreto n. 16.118/2023 e art. 6º, inciso XLI da Lei n. 14.133/2021.

## 15. ANÁLISE DE RISCOS

15.1. Riscos da contratação

| Risco 01 | Problemas no processo de licitação para contratação | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Atraso no processo de contratação. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Cumprimento dos prazos para contratação, revisar e acompanhar as mudanças nos documentos de planejamento da contratação que influenciam no descumprimento do cronograma. | Equipe de Planejamento da Contratação |
| 2. | Elaborar os documentos de planejamento da contratação com estrita observância à legislação e normativos complementares. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Dedicação exclusiva da equipe de planejamento para minimizar os impactos. | Equipe de Planejamento da Contratação |

| Risco 02 | Contingenciamento orçamentário | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Descontinuidade dos serviços. | Alto |
| 2. | Redução da qualidade dos serviços entregues. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Verificar outras possibilidades de orçamento para realizar a contratação. | Equipe de Planejamento da Contratação |
| | Demonstrar a necessidade e a relevância do contrato para manutenção e/ou sustentação dos serviços públicos. | Gestor do Contrato |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Demonstrar claramente à alta gestão a importância da contratação. | Equipe de Planejamento da Contratação |
| 2. | Caso seja extremamente necessário o contingenciamento no contrato, Identificar os pontos que causarão menor impacto caso sejam suprimidos. | Gestor do Contrato |

| Risco 03 | Falha na caracterização do objeto | |
|---|---|---|
| **Probabilidade** | Baixa | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Não atendimento das necessidades da contratação. | Alto |
| 2. | Rescisão contratual | Alto |
| 3. | Descontinuidade dos Serviços | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Definir requisitos técnicos alinhados às necessidades do negócio e aos objetivos da contratação. | Equipe de Planejamento da Contratação |
| 2. | Revisar os artefatos de planejamento da contratação para avaliar se atendem às necessidades e aos objetivos propostos. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Corrigir os artefatos de planejamento da contratação para resolver as falhas identificadas. | Equipe de Planejamento da Contratação |

| | | |
|---|---|---|
| 2. | Aperfeiçoar a elaboração dos documentos de planejamento da contratação detalhando minuciosamente as características do objeto da contratação. | Equipe de Planejamento da Contratação |

| **Risco 04** | **Falha na justificativa para escolha da solução** | |
|---|---|---|
| **Probabilidade** | Baixa | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Não atendimento ao princípio da motivação dos atos administrativos. | Alto |
| 2. | Impossibilidade de contratação. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Justificar a necessidade dos requisitos técnicos exigidos, alinhando-se às necessidades da contratação, principalmente quando implicarem em redução da competitividade do processo seleção do fornecedor. | Equipe de Planejamento da Contratação |
| 2. | Avaliar se os requisitos exigidos são os estritamente necessários e justificáveis para o atendimento das expectativas da contratação proposta. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Justificar a necessidade perante órgãos de controle. | Equipe de Planejamento da Contratação |
| 2. | Caso seja negada a continuidade da contratação, instituir nova equipe de planejamento da contratação e promover uma nova contratação | Autoridade Superior da UG |
| 3. | Aperfeiçoar a elaboração dos documentos de planejamento da contratação exigindo apenas os requisitos estritamente necessários e justificáveis para o atendimento das expectativas da contratação proposta. | Equipe de Planejamento da Contratação |

| **Risco 05** | **Restrição à competitividade** | |
|---|---|---|
| **Probabilidade** | Baixa | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Elevação do preço da contratação. | Alto |
| 2. | Suspensão da contratação. | Alto |
| 3. | Direcionamento indevido do objeto. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Evitar a inclusão de requisitos excessivos e que restringem a competitividade, se atentando apenas aos requisitos estritamente necessários para atender o objetivo da contratação. | Equipe de Planejamento da Contratação |
| 2. | Avaliar se os requisitos exigidos são os estritamente necessários e justificáveis para o atendimento das expectativas da contratação proposta. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Supressão dos critérios restritivos. | Equipe de Planejamento da Contratação |
| 2. | Aperfeiçoar a elaboração dos documentos de planejamento da contratação exigindo apenas os requisitos estritamente necessários e justificáveis para | Equipe de Planejamento da Contratação |

| | | |
|---|---|---|
| | o atendimento das expectativas da contratação proposta. | |

| **Risco 06** | **Falha na pesquisa de preços** | |
|---|---|---|
| **Probabilidade** | Médio | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Elevação dos preços ou inexequibilidade das propostas. | Alto |
| 2. | Impossibilidade de contratação. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Seguir os procedimentos normatizados para a realização de pesquisa de preços. | Equipe de Planejamento da Contratação |
| 2. | Ampliar a pesquisa de preços, não se restringindo a apenas três propostas. | Equipe de Planejamento da Contratação |
| 3. | Avaliar se os procedimentos adotados estão de acordo com os requisitos normativos. | Unidade Administrativa da UG |
| 4. | Levar em consideração os questionamentos das empresas concorrentes. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Refazer a pesquisa de preços precedidas de uma consulta pública para esclarecimentos ou correção de distorções. | Equipe de Planejamento da Contratação |

| **Risco 07** | **Impugnações ou interposição de recurso** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Atraso no processo de contratação. | Alto |
| 2. | Suspensão da contratação. | Alto |
| 3. | Impossibilidade de contratação. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Elaborar e revisar criteriosamente os artefatos de planejamento da contratação de acordo com os normativos vigentes. | Equipe de Planejamento da Contratação |
| 2. | Avaliar e realizar os ajustes recomendados pela Consultoria Jurídica para sanar inconformidades dos documentos de planejamento da contratação com a legislação vigente. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Empenhar-se no atendimento aos pedidos de esclarecimento buscando nos repositórios legais e jurisprudenciais os elementos de sustentação das opções adotadas para a contratação. | Equipe de Planejamento da Contratação |
| 2. | Caso seja negada a continuidade da contratação, instituir nova equipe de planejamento da contratação e promover uma nova contratação. | Autoridade Superior da UG |
| 3. | Aperfeiçoar a elaboração dos documentos de planejamento da contratação com estrita observância à legislação e normativos complementares. | Equipe de Planejamento da Contratação |

| **Risco 12** | **Custo do objeto licitado superior ao estimado para a contratação dos serviços** | |
|---|---|---|
| **Probabilidade** | Baixa | |
| **Id.** | **Dano** | **Impacto** |

| | | |
|---|---|---|
| 1. | Comprometimento da economicidade da contratação. | Alto |
| 2. | Não adjudicação do objeto. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Revisar as estimativas dos custos estimados do estudo técnico. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Não havendo possibilidade de redução dos valores negociados, deve-se suspender o certame com vistas redefinição de escopo do objeto e do processo de Planejamento da Contratação. | Autoridade Superior da UG |

| **Risco 13** | **Atraso no processo de contratação da solução** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Descontinuidade dos serviços de infraestrutura de TI. | Alto |
| 2. | Comprometimento dos serviços prestados. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Cumprimento dos prazos para contratação, revisar e acompanhar as mudanças nos documentos de planejamento da contratação que influenciam no descumprimento do cronograma. | Equipe de Planejamento da Contratação |
| 2. | Elaborar os documentos de planejamento da contratação com estrita observância à legislação e normativos complementares. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Dedicação exclusiva da equipe de planejamento para minimizar os impactos. | Equipe de Planejamento da Contratação |
| 2. | Renovação do contrato de suporte e garantia com a atual contratada por mais 12 meses com a possibilidade de rescisão contratual por parte da contratante a qualquer momento. | Autoridade Superior da UG |

15.1.1. Riscos da gestão contratual:

| **Risco 08** | **Descumprimento de cláusulas contratuais pela Contratada** | |
|---|---|---|
| **Probabilidade** | Média | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Não entrega dos serviços e equipamentos. | Alto |
| 2. | Atraso na entrega dos serviços e equipamentos. | Alto |
| 3. | Baixa qualidade dos serviços e equipamentos entregues. | Alto |
| 4. | Descontinuidade dos serviços. | Alto |
| 5. | Falta de efetividade da contratação. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Acompanhar a execução dos serviços aferindo se os requisitos exigidos no contrato estão sento cumpridos de acordo com a qualidade exigida. | Fiscal e Gestor do Contrato |
| 2. | Avaliar se os serviços prestados estão atendendo as expectativas da contratação. | Fiscal e Gestor do Contrato |
| 3. | Dimensionamento adequado do corpo de fiscalização e gestão contratual. | Autoridade Superior da UG |

| | | |
|---|---|---|
| 4. | Capacitação de equipe de fiscalização e gestão contratual. | Autoridade Superior da UG |
| 5. | Intensificação no processo de fiscalização e gestão contratual | Fiscal e Gestor do Contrato |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Notificar formalmente a Contratada quando cláusulas do contrato forem descumpridas. | Fiscal e Gestor do Contrato |
| 2. | Aplicar glosas e penalidades previstas no instrumento convocatório, de forma a coibir a reincidência. | Fiscal e Gestor do Contrato |
| 3. | Instituir nova equipe de planejamento da contratação e promover uma nova contratação para evitar o comprometimento da continuidade dos serviços sustentados pela solução de TIC, em caso de dificuldade de resolução das inconformidades. | Autoridade Superior da UG |

| **Risco 09** | **Irregularidade no cumprimento de questões trabalhistas** | |
|---|---|---|
| **Probabilidade** | Média | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Desmotivação dos profissionais prestadores de serviços. | Alto |
| 2. | Aumento da rotatividade dos profissionais. | Médio |
| 3. | Baixa qualidade dos serviços entregues. | Alto |
| 4. | Corresponsabilização de equipe de gestão e fiscalização. | Alto |
| 5. | Descontinuidade dos serviços. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Elaborar lista de verificação que deverá ser observada pela fiscalização administrativa, durante a execução do contrato. | Fiscal e Gestor do contrato |
| 2. | Realizar a fiscalização do cumprimento das obrigações trabalhistas, conforme legislação vigente. | Fiscal e Gestor do contrato |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Notificar formalmente a Contratada quando forem identificadas irregularidades trabalhistas. | Fiscal e Gestor do Contrato |
| 2. | Aplicar glosas e penalidades previstas no instrumento convocatório. | Fiscal e Gestor do Contrato |
| 3. | Instituir nova equipe de planejamento da contratação e promover uma nova contratação para evitar o comprometimento da continuidade dos serviços sustentados pela Solução de TIC. | Autoridade Superior da UG |

| **Risco 10** | **Vazamento de dados e informações pelos funcionários da contratada** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Divulgação de informações privilegiadas e restritas. | Alto |
| 2. | Quebra de confidencialidade de dados, informações e documentos | Alto |
| 3. | Redução da credibilidade do órgão/entidade. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Exigir dos funcionários da contratada assinatura de Termo de Compromisso de obediência às normas de segurança e Sigilo do órgão/entidade. | Fiscal e Gestor do Contrato |

| | | |
|---|---|---|
| 2. | Estabelecer o Gerenciamento de Configuração e Ativo de Serviço para controlar os recursos computacionais, incluindo a concessão de acesso aos recursos. | Unidade de Tecnologia da Informação da UG |
| 3. | Manter a contratada e seus profissionais cientes e da Política de Segurança da Informação. | Fiscal e Gestor do Contrato |
| 4. | Estabelecer, conscientizar e divulgar os procedimentos de controle de permissões e perfis de acesso, principalmente para terceiros que podem ter alta rotatividade. | Unidade de Tecnologia da Informação da UG |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Aplicar sanções administrativas, cíveis e criminais | Unidade Administrativa e/ou Jurídica da UG |
| 2. | Exigir reparação do dano, quando aplicável. | Unidade Administrativa e/ou Jurídica da UG |

| **Risco 11** | **Alta rotatividade de funcionários da contratada** | |
|---|---|---|
| **Probabilidade** | Média | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Ingressos frequentes de mais pessoas estranhas à organização. | Alto |
| 2. | Falta de conhecimento do ambiente e integração com os demais colaboradores. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Determinar de forma precisa e clara as especificações técnicas do contrato bem como os requisitos de qualificação técnica dos colaboradores da Contratada, definindo as atividades, papéis e responsabilidades com vistas a possibilitar a transparência e a vantajosidade técnica e econômica da licitação. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Promover ações de construção, manutenção e atualização das bases de conhecimento, de modo a facilitar a substituição de técnicos. | Equipe de Fiscalização do Contrato |

15.2. Riscos que comprometem a Solução de Tecnologia da Informação e Comunicação

| **Risco 01** | **Interrupção da execução contratual ou rescisão do contrato** | |
|---|---|---|
| **Probabilidade** | Média | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Descontinuidade dos serviços sustentados pela STIC. | Alto |
| 2. | Comprometimento dos serviços prestados pela UG. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Acompanhar a execução dos serviços aferindo criteriosamente se os requisitos estão sento cumpridos de acordo com a qualidade exigida, buscando identificar qualquer problema de execução em sua origem para não permitir maiores impactos no contrato. | Fiscal e Gestor do Contrato |
| 2. | Avaliar se os serviços prestados estão atendendo as expectativas da contratação. | Fiscal e Gestor do Contrato |
| 3. | Garantir que o conhecimento seja repassado continuamente para a equipe de fiscalização técnica. | Fiscal e Gestor do Contrato |
| 4. | Executar atividades de validação do ambiente | Unidade de Tecnologia da |

| | | |
|---|---|---|
| | (verificação de Alta disponibilidade, atualização do equipamento, dentre outras.) | Informação da UG |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Iniciar novo processo de contratação, utilizando os artefatos de planejamento produzidos, com as atualizações baseadas na Infraestrutura e experiência adquirida no processo de gestão e fiscalização. | Autoridade Superior da UG |

| **Risco 02** | **Falta de pessoal técnico competente para fiscalização do contrato** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Deficiência na fiscalização do contrato com comprometimento na aferição dos níveis de serviço. | Alto |
| 2. | Baixa qualidade nas entregas dos serviços. | Alto |
| 3. | Não atendimento das expectativas da contratação. | Alto |
| 4. | Atrasos no pagamento, pagamento indevido e sem o devido desconto das glosas. | Alto |
| 5. | Inexecução parcial ou total do contrato. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Definir indicadores de fácil mensuração e que podem ser monitorados por meio da ferramenta de gestão de serviços de TIC. | Equipe de Planejamento da Contratação |
| 2. | Elaborar Plano de Fiscalização prevendo como deverá ser realizada a fiscalização do contrato, incluindo modelos de planilhas de aferição e listas de verificação. | Equipe de Planejamento da Contratação |
| 3. | Identificar se existem servidores com habilidades e competências em TIC adequadas e em quantidade suficiente para a atuação na fiscalização dos serviços contratados e mensuração sistemática dos indicadores e da qualidade dos serviços. | Equipe de Planejamento da Contratação |
| 4. | Promover o recrutamento de servidores públicos, de outras áreas ou outros órgãos, que possuam habilidades e competências em TIC adequadas para a aferição sistemática da qualidade das entregas dos serviços contratados. | Autoridade Superior da UG |
| 5. | Propor processo de seleção de servidores públicos, afim de alocar servidores que possuem competências técnicas adequadas para a aferição sistemática das entregas dos serviços contratados. | Autoridade Superior da UG |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Primar pela demanda de atividades críticas, que envolvam a disponibilidade do ambiente tecnológico | Fiscal e Gestor do Contrato |
| 2. | Propor processo seletivo simplificado para contratação de servidores temporários com habilidades e competências em TIC adequadas para a aferição sistemática da qualidade das entregas dos serviços contratados. | Autoridade Superior da UG |

| **Risco 03** | **Prestação de serviço por profissionais inexperientes ou sem conhecimento técnico adequado** |
|---|---|
| **Probabilidade** | Média |

| Id. | Dano | Impacto |
|---|---|---|
| 1. | Baixa qualidade nas entregas dos serviços. | Alto |
| 2. | Atraso na entrega dos serviços. | Médio |
| 3. | Indisponibilidade de serviços críticos. | Alto |
| 4. | Descumprimento dos requisitos contratuais. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Prever requisitos de qualificação técnica e experiência profissional de acordo com complexidade de cada tipo de serviço. | Equipe de Planejamento da Contratação |
| 2. | Realizar a fiscalização do cumprimento dos requisitos de qualificação técnica e experiência profissional exigidos. | Fiscal e Gestor do Contrato |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Notificar formalmente a Contratada quando os requisitos do contrato não forem descumpridos. | Fiscal e Gestor do Contrato |
| 2. | Aplicar glosas e penalidades previstas no instrumento convocatório, de forma a coibir a reincidência. | Fiscal e Gestor do Contrato |

| **Risco 04** | **Não atendimento dos Níveis Mínimos de Serviços** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Não atendimento aos requisitos de negócio. | Alto |
| 2. | Ineficiência e não efetividade da contratação | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Prever sanções pelo descumprimento dos Níveis Mínimos de Serviços. | Equipe de Planejamento da Contratação |
| 2. | Estabelecer meios de monitoração e controle proativos da qualidade dos serviços. | Equipe de Planejamento da Contratação |
| 3. | Atuar proativamente e continuamente na aferição da qualidade dos serviços executados intervindo nos desvios de qualidade. | Fiscal e Gestor do Contrato |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Realizar as intervenções que forem necessárias para o reestabelecimento imediato do atendimento e dos serviços. | Fiscal e Gestor do Contrato |
| 2. | Notificar formalmente a Contratada quando cláusulas do contrato forem descumpridas ou violadas. | Fiscal e Gestor do Contrato |
| 3. | Aplicar glosas e penalidades previstas no instrumento convocatório, de forma a coibir a reincidência. | Unidade Administrativa e/ou Jurídica da UG |

| **Risco 05** | **Falha na estimativa de volume de serviços** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Não atendimento das expectativas da contratação. | Alto |
| 2. | Superdimensionamento ou subdimensionamento do contrato. | Alto |
| 3. | Contratação antieconômica e sobrepreço. | Alto |
| 4. | Rescisão contratual. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Realizar o levantamento criterioso do volume de serviços executados antes da contratação para estimar adequadamente o volume previsto. | Equipe de Planejamento da Contratação |

| | | |
|---|---|---|
| 2. | Elaboração minuciosa da memória de cálculo. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Solicitar aditivo de acréscimo ou supressão contratual. | Gestor do Contrato |
| 2. | Instituir nova equipe de planejamento da contratação e promover uma nova contratação para evitar o comprometimento da continuidade dos serviços sustentados pela STIC. | Autoridade Superior da UG |

| **Risco 06** | **Descumprimento de cláusulas contratuais pela Contratada** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Não entrega dos serviços. | Alto |
| 2. | Atraso na entrega dos serviços | Alto |
| 3. | Entrega com qualidade inferior à exigida | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Definição de níveis de serviços adequados | Equipe de Planejamento da Contratação |
| 2. | Acompanhamento e verificação de qualidade do serviço prestado | Fiscal e Gestor do Contrato |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Aplicação de glosas e, caso haja prejuízo maior previsto nos níveis mínimos de serviço, aplicação das sanções cabíveis, de forma a coibir a reincidência | Fiscal e Gestor do Contrato |

| **Risco 07** | **Indisponibilidade dos serviços de TI por não atendimento das demandas nos prazos definidos** | |
|---|---|---|
| **Probabilidade** | Média | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Paralisação dos serviços de infraestrutura de TI e indisponibilidade dos sistemas críticos | Alto |
| 2. | Comprometimento dos serviços prestados | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Prever sanções pelo descumprimento dos Níveis Mínimos de Serviços | Equipe de Planejamento da Contratação |
| 2. | Estabelecer meios de monitorar e controlar a qualidade dos serviços prestados | Equipe de Planejamento da Contratação |
| 3. | Atuar de forma proativa e contínua na aferição da qualidade dos serviços | Fiscal e Gestor do Contrato |
| 4. | Prover e implementar recursos e tecnologias de alta disponibilidade | Fiscal e Gestor do Contrato |
| **Id.** | **Ação de Contingênca** | **Responsável** |
| 1. | Aplicação de glosas e, caso haja prejuízo maior previsto nos níveis mínimos de serviço, aplicação das sanções cabíveis, de forma a coibir a reincidência | Unidade Administrativa e/ou Jurídica da UG |

## 16. DO PLANEJAMENTO

16.1. O Estudo Técnico Preliminar foi realizado por servidor que reúne as competências necessárias à complexa execução das etapas de Planejamento:

Campo Grande, assinado digitalmente.

**Equipe de Planejamento/Elaborado por:**

| **Nome: Luiz Fabiano Câmara** |
|---|
| Mat. 88990022 |
| Órgão: SSD/CTEC |
| Função: Analista de Tecnologia da Informação |

**Aprovado por:**

Márcia Bogena Cereser Tomasi
Superintendente de Saúde Digital