

ANEXO I – TERMO DE REFERÊNCIA

1. DO OBJETO: Contratação de pessoa jurídica especializada para locação de solução de firewall e fornecimento de licenças de segurança para proteção de endpoints, incluindo serviços de suporte técnico, atualização, monitoramento e manutenção contínua, visando atender às demandas do **SENAR-AR/MS**.

2. DA FINALIDADE

2.1. MOTIVAÇÃO DA CONTRATAÇÃO: O Serviço Nacional de Aprendizagem Rural – Administração Regional de Mato Grosso do Sul (**SENAR-AR/MS**), entidade integrante do Sistema “S”, tem a missão institucional de promover a educação profissional e a difusão de tecnologias voltadas ao desenvolvimento do setor agropecuário, assegurando a qualidade, a inovação e a eficiência de suas atividades administrativas e pedagógicas.

2.2. Entre suas atribuições, compete ao **SENAR-AR/MS** manter infraestrutura tecnológica que dê suporte à gestão administrativa e educacional, garantindo a disponibilidade e a segurança das informações estratégicas sob sua responsabilidade. Para tanto, torna-se necessário assegurar níveis adequados de proteção às redes corporativas, às estações de trabalho, aos servidores de arquivos e aos dispositivos móveis utilizados em suas operações, de forma a racionalizar recursos, reduzir riscos cibernéticos e manter a integridade de seus serviços institucionais.

2.3. A crescente sofisticação dos ataques cibernéticos exige a adoção de soluções especializadas de segurança da informação que permitam prevenir, detectar e responder de maneira ágil e eficiente a incidentes de segurança. Nesse sentido, a contratação de empresa especializada, em caráter continuado, justifica-se para o fornecimento de serviços envolvendo hardware, software, appliances e respectivas assinaturas de atualização, bem como serviços de instalação, customização, treinamento e suporte técnico qualificado. Essa composição é indispensável para assegurar proteção integral contra ameaças avançadas e para promover a inspeção de tráfego em redes corporativas, garantindo maior resiliência e disponibilidade da infraestrutura tecnológica do **SENAR-AR/MS**.

2.4. A ausência de mecanismos modernos e padronizados de segurança em rede e de soluções antimalware de última geração representa significativa vulnerabilidade para a instituição, expondo seus sistemas e dados a riscos de indisponibilidade, perda ou vazamento de informações sensíveis, além de potenciais custos financeiros e danos à sua imagem institucional.

2.5. A presente contratação também encontra fundamento na **Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018)**, que impõe às instituições a adoção de medidas técnicas e administrativas aptas a resguardar a confidencialidade, a integridade e a disponibilidade das informações pessoais e sensíveis sob sua guarda.

2.6. Além disso, o cenário atual de cyber ameaças, constantemente monitorado por órgãos especializados, evidencia a necessidade de soluções tecnológicas que possibilitem uma defesa proativa e resiliente, alinhada às melhores práticas de governança digital e de segurança da informação.

2.7. Com a adoção da solução integrada de segurança, o **SENAR-AR/MS** contará com proteção eficaz da rede de computadores e maior segurança para estações de trabalho, servidores e dispositivos móveis, monitoramento e inspeção de tráfego em tempo real, suporte técnico qualificado e treinamento da equipe interna, promovendo transferência de conhecimento e maior autonomia institucional.

2.8. A continuidade das atividades finalísticas do **SENAR-AR/MS** depende da disponibilidade e da integridade de sua infraestrutura tecnológica, de modo que falhas ou indisponibilidades impactam diretamente a execução de programas de capacitação, projetos educacionais e ações administrativas.

2.9. A contratação também se ancora no **princípio da eficiência**, previsto no artigo 37 da Constituição Federal, e nas diretrizes do **Regulamento de Licitações e Contratos do SENAR (Resolução nº 30/2024/CD)**, assegurando racionalização de recursos, prevenção de desperdícios e garantia de maior robustez ao ambiente tecnológico institucional, resultando em benefícios concretos para a sociedade rural atendida pela entidade.

2.10. Assim, ao prover um ambiente seguro, monitorado e resiliente, esta contratação contribuirá diretamente para a continuidade das atividades administrativas e educacionais do **SENAR-AR/MS**, a proteção de dados sensíveis e críticos, a conformidade legal e regulatória, a mitigação de riscos cibernéticos e operacionais, além da modernização e do fortalecimento da infraestrutura tecnológica institucional.

2.11. O dimensionamento da solução foi realizado com base na análise da infraestrutura tecnológica atual do **SENAR-AR/MS** e nas necessidades de proteção de sua rede corporativa, contemplando tanto o cenário presente quanto a previsão de expansão das atividades educacionais e administrativas da instituição. O objetivo é assegurar a proteção integral dos ativos digitais críticos e o provisionamento para futuras demandas, em consonância com o crescimento do uso de sistemas e serviços digitais voltados à formação e capacitação no meio rural.

2.12. Firewall de Próxima Geração (NGFW)

a) Quantidade: 02 (duas) unidades.

b) Descrição: **01 appliance NGFW** instalado na sede do **SENAR-AR/MS**, destinado à segurança perimetral da rede corporativa, com recursos de inspeção avançada de tráfego, prevenção contra ameaças e proteção contínua contra ataques internos e externos. **01 appliance NGFW** instalado no Centro de Excelência em Bovinocultura de Corte SENAR MS (CEBC), com as mesmas finalidades, garantindo segurança descentralizada e redundância adequada.

c) Justificativa: o dimensionamento considera a necessidade de proteger redes distintas e descentralizadas, mantendo desempenho e segurança equivalentes nas duas unidades operacionais, ambas críticas para o funcionamento institucional.

2.13. Licenciamento de Endpoint Protection Platform (EPP)

a) Quantidade: 500 (quinhentas) licenças.

b) Descrição: licenças destinadas a estações de trabalho, servidores e dispositivos móveis do **SENAR-AR/MS**, CEBC e SENAR-ON, com funcionalidades de antivírus de nova geração, firewall de host, proteção contra ransomware, controle de dispositivos e prevenção contra exploração de vulnerabilidades.

c) Justificativa: quantidade definida com base no parque tecnológico atual, acrescida de margem de expansão para absorver novas demandas e garantir cobertura integral dos dispositivos institucionais. A quantidade prevê a necessidade de atendimento dos computadores do CEBC, **SENAR-AR/MS**, notebooks do SENAR ON e Inclusão Digital.

2.14. Acesso Seguro Zero Trust

a) Quantidade: 20 (vinte) licenças.

b) Descrição: solução de acesso remoto seguro e segmentado, permitindo controle granular de acesso conforme o modelo de Confiança Zero (Zero Trust).

c) Justificativa: dimensionada para contemplar os ativos mais críticos e sensíveis, garantindo proteção a usuários privilegiados, conexões externas e ambientes administrativos de maior risco.

2.15. Plataforma de Conscientização em Segurança da Informação

a) Quantidade: 50 (cinquenta) licenças.

b) Descrição: treinamento contínuo para usuários da rede, com metodologia adaptativa e foco em prevenção de incidentes causados por erro humano.

c) Justificativa: atender colaboradores e gestores do **SENAR-AR/MS**, promovendo cultura organizacional de segurança e capacitação continuada.

2.16. Justificativa do prazo de vigência e possibilidade de prorrogação

2.16.1. Os serviços contemplados, incluindo a locação de firewall com fornecimento de hardware e licenciamento completo, a disponibilização de plataforma de conscientização em segurança da informação e a solução de proteção de endpoints (EPP), possuem

características intrínsecas de continuidade operacional, exigindo monitoramento constante, atualizações frequentes, suporte técnico especializado e adaptação permanente frente às novas ameaças cibernéticas.

2.16.2. A descontinuidade ou substituição frequente dessas soluções pode acarretar riscos significativos à segurança da informação, à integridade dos dados institucionais e à disponibilidade dos serviços de rede, além de gerar custos adicionais relacionados à reimplantação, reconfiguração, treinamentos e possíveis indisponibilidades operacionais.

2.16.3. Adicionalmente, a possibilidade de prorrogação contratual proporciona maior eficiência administrativa e economicidade, ao evitar processos licitatórios recorrentes para serviços contínuos, bem como permite a amortização de custos relacionados à implantação inicial das soluções, especialmente no que se refere ao fornecimento de hardware, configuração e treinamento.

2.16.4. Destaca-se ainda que as soluções contratadas estão diretamente relacionadas à proteção do ambiente corporativo contra ameaças cibernéticas cada vez mais sofisticadas, exigindo evolução contínua por meio de atualizações de assinaturas, inteligência de ameaças, mecanismos de detecção e resposta, e ações de conscientização dos usuários.

2.16.5. Dessa forma, a previsão de prorrogação contratual está alinhada aos princípios da eficiência, economicidade e continuidade do serviço, ficando condicionada à verificação periódica de vantajosidade, conveniência e oportunidade por parte do **SENAR-AR/MS**, bem como ao interesse da contratada, conforme estabelecido no art. 33 do RLC.

3. DA DESCRIÇÃO DETALHADA DO OBJETO

3.1. O objeto necessário ao atendimento das demandas do **SENAR-AR/MS** segue detalhado:

ESPECIFICAÇÃO DO OBJETO							
LOTE	ITEM	DESCRIÇÃO	UNID. DE MEDIDA	QTDE ESTIMADA	VALOR MENSAL (12 MESES) (A)/12= Valor Mensal	PREÇO UNIT. MÁXIMO (ESTIMADO)	PREÇO TOTAL MÁXIMO (ESTIMADO) (A)
	01	LOCAÇÃO DE FIREWALL, COM FORNECIMENTO DE HARDWARE, LICENCIAMENTO COMPLETO, ATUALIZAÇÕES, INSTALAÇÃO, CONFIGURAÇÃO, TREINAMENTO E SUPORTE TÉCNICO QUALIFICADO, EM CARÁTER CONTINUADO, PARA PROTEÇÃO E INSPEÇÃO DE TRÁFEGO DE REDE. ID INTERNO: 28791	UN	02	R\$ 25.970,48	R\$ 155.822,91	R\$ 311.645,82
		SOLUÇÃO EPP (ENDPOINT PROTECTION), VISANDO À PROTEÇÃO PROATIVA CONTRA					

01	02	MALWARES, RANSOMWARES E AMEAÇAS PERSISTENTES AVANÇADAS (APTS) EM ESTAÇÕES DE TRABALHO, SERVIDORES DE REDE E DISPOSITIVOS MÓVEIS. O SERVIÇO DEVERÁ GARANTIR A PROTEÇÃO CONTÍNUA DE 500 DISPOSITIVOS, ASSEGURANDO A MITIGAÇÃO DE AMEAÇAS E A INTEGRIDADE DAS INFORMAÇÕES INSTITUCIONAIS DO SENAR-AR/MS. ACESSO SEGURO ZERO TRUST: 20 USUÁRIOS. ID INTERNO: 28813	Licenças de Uso	500	R\$ 12.160,41	R\$ 291,85	R\$ 145.925,00
	03	PLATAFORMA DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO, BASEADA EM APRENDIZAGEM AUTOMATIZADA E ADAPTATIVA, DESTINADA AO TREINAMENTO CONTÍNUO DE USUÁRIOS DA REDE CORPORATIVA DO SENAR-AR/MS. ID INTERNO: 28812	Licenças de Uso	50	R\$ 1.307,41	R\$ 313,78	R\$ 15.689,00

3.2. O valor total máximo estimado para a contratação é **R\$ 473.259,82** (quatrocentos e setenta e três mil, duzentos e cinquenta e nove reais e oitenta e dois centavos).

3.3. DETALHAMENTO DO OBJETO

3.3.1. Contratação de empresa especializada para locação de firewall, com fornecimento de hardware, licenciamento completo, atualizações, instalação, configuração, treinamento e suporte técnico qualificado, em caráter continuado, para proteção e inspeção de tráfego de rede;

3.3.1.1. Appliance de Firewall de Próxima Geração (Next Generation Firewall – NGFW), destinado a prover a segurança perimetral da rede corporativa, com recursos de inspeção avançada de tráfego, prevenção contra ameaças cibernéticas e mecanismos de proteção contínua contra-ataques internos e externos.

3.3.1.2. No que se refere a equipamentos e softwares, todos os produtos de hardware que compõem a solução deverão possuir homologação e certificação junto à **ANATEL**, em conformidade com a Lei nº 9.472/1997 e com a Resolução nº 715/2019 daquela Agência, assegurando a legalidade do uso e a regularidade técnica dos dispositivos de telecomunicações.

3.3.1.3. 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 2º da Resolução **ANATEL** n. 715, de 23 de outubro de 2019.

3.3.1.4. 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.

3.3.2. Requisitos de Capacidade e de Interfaces para solução de proteção de borda do Tipo I

3.3.2.1. Deve suportar, no mínimo, 5.3 Gbps de throughput com a funcionalidade de firewall habilitada;

3.3.2.2. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 3.3 Gbps ou superior;

3.3.2.3. Desempenho em modo de Inspeção (descriptografia 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;

3.3.2.4. Desempenho mínimo de 3.5 Gbps de IPS;

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

3.3.2.6. Suporte mínimo de 21.000 novas conexões por segundo;

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

3.3.2.8. Deve possuir uma fonte de alimentação com chaveamento automático de 100-240;

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

3.3.2.10. Deve possuir 04 interfaces 5 GbE padrão SFP+;

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

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

3.3.2.13. Deve possuir 1 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G;

3.3.2.14. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 30 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 500 usuários simultâneos;

3.3.2.15. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 250 usuários simultâneos;

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

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

3.3.3. Requisitos de Capacidade e de Interfaces para solução de proteção de borda do Tipo II

3.3.3.1. Deve suportar, no mínimo, 4.8 Gbps de throughput com a funcionalidade de firewall habilitada;

3.3.3.2. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de

3.3.3.3. Aplicação habilitados) mínimo de 2.8 Gbps ou superior;

3.3.3.4. Desempenho em modo de Inspeção (descriptorgrafia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 750 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;

3.3.3.5. Desempenho mínimo de 3.0 Gbps de IPS;

3.3.3.6. Suporte mínimo de 1.200.000 conexões simultâneas/concorrente no modo SPI;

3.3.3.7. Suporte mínimo de 20.000 novas conexões por segundo;

3.3.3.8. Deve permitir armazenamento interno de no mínimo 64 GB e suportar expansão de armazenamento de até 256 Gb;

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

3.3.3.10. Deve possuir 03 interfaces de 10GbE padrão SFP+;

3.3.3.11. Deve possuir 16 interfaces 1 GbE padrão RJ-45;

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

3.3.3.13. Deve possuir 1 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G;

3.3.3.14. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 30 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 500 usuários simultâneos;

3.3.3.15. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 250 usuários simultâneos;

3.3.3.16. Deve suportar 1.500 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos;

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

3.3.4. Requisitos de Firewall e SD-WAN para Solução de Proteção de Perímetro

3.3.4.1. 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;

3.3.4.2. 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;

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

- 3.3.4.4.** Deve possuir proteção anti-spoofing;
- 3.3.4.5.** Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;
- 3.3.4.6.** Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF;
- 3.3.4.7.** 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;
- 3.3.4.8.** A solução deverá possuir a tecnologia SD-WAN (Software Defined WAN), e que ela 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;
- 3.3.4.9.** 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 parâmetros simultâneos: Latência; Jitter; Perda de pacotes;
- 3.3.4.10.** 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;
- 3.3.4.11.** A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas;
- 3.3.4.12.** Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 3.3.4.13.** Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 3.3.4.14.** Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes;
- 3.3.4.15.** 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;
- 3.3.4.16.** Deve suportar DHCP relay;
- 3.3.4.17.** 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;
- 3.3.4.18.** 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;

3.3.4.19. Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) e de comunicadores instantâneos (Instant Messenger) incluindo, no mínimo: WhatsApp, Skype para usuários da rede, individualmente ou em grupo;

3.3.4.20. Deve ter suporte à proteção e identificação de hosts possivelmente infectados com “botnets”.

3.3.4.21. 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;

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

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

3.3.4.24. Detectar e bloquear a origem de portscans;

3.3.4.25. Deve permitir o bloqueio de ataques;

3.3.4.26. Deve permitir o bloqueio de exploits conhecidos;

3.3.4.27. O gateway Antivírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP e SMTP;

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

3.3.4.29. Implementar DSCP (Differentiated Services Code Points);

3.3.4.30. 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;

3.3.4.31. 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;

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

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

3.3.4.34. Possuir suporte a log via Syslog;

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

3.3.4.36. 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;

3.3.4.37. 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;

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

3.3.4.39. Deve permitir a funcionalidade de ARP bridging;

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

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

3.3.5. Requisitos de Acesso Seguro Zero Trust a aplicações privadas

3.3.5.1. A solução detalhada aqui deve fornecer acesso menos privilegiado a sites privados, servidores diversos, áreas de trabalho remotas, bancos de dados, clusters de Kubernetes e recursos e serviços de rede semelhantes. Ele também deve controlar o acesso a aplicativos baseados em navegador e infraestrutura de servidor usando proxy reverso com reconhecimento de identidade.

3.3.5.2. Para soluções que limitam o número de dispositivos associados a cada conta de usuário/acesso e controle de dispositivo, o licenciamento adicional (quando necessário) deve considerar pelo menos 10 dispositivos habilitados para cada usuário independente;

3.3.5.2.1. Além da cobertura de nuvem para pontos de presença globais, a plataforma deve considerar e incluir nativamente a possibilidade de uso híbrido que permita ao CLIENTE provisionar pontos de presença "privados" instalados em sua própria infraestrutura. Esses pontos de presença privados devem permitir uma integração transparente com os demais na nuvem, garantindo maior desempenho e menor latência para aplicações que demandam tal arquitetura.

3.3.5.3. Sistemas baseados em hardware ou software projetados para uso genérico ou código aberto ("código aberto") não serão aceitos. Os elementos oferecidos não podem ser personalizados;

3.3.5.4. O agente único a ser instalado nos dispositivos protegidos deve ser compatível com pelo menos os seguintes sistemas operacionais:

3.3.5.4.1. Windows 10 e 11; Fedora Linux 38 e 39; Ubuntu 22.04 LTS e 24.04 LTS; Oracle Linux 8, Oracle Linux 9; MacOS 14 Sonoma e MacOS 15 Sequoia; iOS 15 e superior; Android 12 e superior; ChromeOS, versão estável atual.

3.3.5.5. Toda a solução proposta deverá ser implementada com autenticação integrada de usuários e suportar aplicações de políticas granulares baseadas em nome de usuário, departamento e grupos, integradas à plataforma Microsoft EntraID do **SENAR-AR/MS**, utilizando o protocolo SAML 2.0 (Security Assertion Markup Language). O suporte para outros provedores de IdP, como (Okta, Google Cloud Services, OneLogin), também deve ser considerado, oferecendo alternativas ao EntraID existente, se necessário. Ele deve dar suporte a pelo menos um dos sugeridos como um complemento para o MS EntraID, e possibilidade de autenticação com LDAP.

3.3.5.6. A determinação do estado de integridade e confiança dos dispositivos deve ocorrer de forma permanente e automática, preservando e aplicando os conceitos de confiança zero. A determinação (ou cálculo) do estado de segurança do dispositivo deve permitir que o administrador da plataforma escolha diferentes condições de acesso, em políticas, com base nessa pontuação de status do dispositivo;

3.3.5.6.1. A ação do agente sobre o dispositivo deve ser automática de acordo com o monitoramento permanente, negando ou restabelecendo a conectividade sem a necessidade de intervenção do administrador da plataforma ou do usuário;

3.3.5.6.2. A conectividade dos dispositivos utilizados pelos usuários deve ocorrer de forma transparente, sem a obrigatoriedade de o usuário ativar ou desativar o agente instalado;

3.3.5.6.3. Quando encriptada a conectividade entre os dispositivos e a infraestrutura, a plataforma deve operar nativamente e disponibilizar os concentradores sob o conceito de VPNaaS (VPN as a service), sem necessidade de provisionamento específico de nós que dependam da infraestrutura do CLIENTE;

3.3.5.6.4. A solução deve ser capaz de fornecer visualização de log em tempo real para tarefas de investigação e auditoria;

3.3.5.6.5. A solução deverá fornecer acesso remoto às aplicações e recursos internos do CLIENTE, com segurança, validação de identidade, tunelamento criptografado, segregação de aplicações, verificação de postura e conexão direta com o menor privilégio. Esses acessos devem ser monitorados permanentemente e de acordo com as políticas granulares de admissão e acesso fornecidas pelo administrador da plataforma;

3.3.5.6.6. A solução deve habilitar a arquitetura Zero Trust Network Access (ZTNA), definindo políticas de acesso granulares para fornecer aos usuários, de acordo com seu contexto, acesso menos privilegiado a aplicativos ou recursos de forma a reduzir a superfície de ataque;

3.3.5.6.7. A solução deve ser oferecida na nuvem, conforme projetado no modelo SSE (Secure Service Edge). Somente os conectores que permitem a conectividade entre essa infraestrutura de nuvem e os datacenters do Cliente serão considerados permitidos na solução. O CLIENTE deve ser capaz de instalar quantos conectores sua infraestrutura de datacenter exigir, sem a

necessidade de licenciamento ou expansões complementares adquiridas fora do escopo deste processo.

3.3.5.7. O componente chamado conector deve permitir, mas não se limitar a:

3.3.5.7.1. Arquitetura de alta disponibilidade e realizar balanceamento de carga automaticamente, sem depender de nenhum componente de rede da infraestrutura do CLIENTE;

3.3.5.7.2. Não ter uma superfície de ataque exposta na Internet, sem endereços IP divulgados publicamente;

3.3.5.7.3. Todo o tunelamento com os conectores deve ser iniciado por eles (saída), destinado à nuvem do fabricante onde o serviço está concentrado. O túnel iniciado na nuvem para conectores não será aceito;

3.3.5.7.4. Permitir que o conector seja instalado de forma flexível a partir de qualquer ponto da rede do CLIENTE, como por meio de NAT (Network Address Translation) disponibilizado no perímetro de acesso à rede interna;

3.3.5.7.5. Não deve determinar um único ponto de conexão à rede do CLIENTE, sendo possível implementar múltiplos conectores em diferentes pontos de rede, datacenters ou nuvens privadas, proporcionando ao usuário acesso direto aos recursos com a menor latência possível e de forma dinâmica;

3.3.5.7.6. Permitir que o usuário se conecte a diferentes aplicativos simultaneamente usando conectores em diferentes pontos de rede. Essas conexões devem ser determinadas pelas políticas de acesso definidas pelo administrador;

3.3.5.7.7. Os conectores devem ser independentes, sem necessidade de conectividade interna total a todos os recursos privados, possibilitando o fornecimento de acesso a aplicativos ou recursos simultaneamente aos usuários em vários datacenters ou nuvem, mesmo que esses datacenters ou nuvem não tenham conectividade pré-estabelecida entre eles;

3.3.5.7.8. A solução deve autenticar o usuário no provedor de identidade (IdP), oferecendo políticas granulares, segmentação de aplicativos e posturas específicas. Deve fornecer acesso a aplicações Web, ou qualquer outra com protocolo TCP e UDP, como (SSH, RDP, SQL, aplicações cliente-servidor, compartilhamento de arquivos etc.) de forma transparente, sem a necessidade de alterar o cliente original da aplicação, criando tunelamento criptografado que conectará o usuário à aplicação e não à rede do CLIENTE.

3.3.5.8. A solução não deve operar como uma VPN tradicional que fornece endereçamento IP da rede local, mas sim conectar o usuário diretamente, após validação da política de identidade, postura e políticas de acesso, a recursos e aplicativos por meio de tunelamento criptografado específico;

3.3.5.8.1. Os usuários remotos não devem ter visibilidade de aplicativos não autorizados, o conceito de confiança zero deve ser preservado. Os recursos não autorizados não devem ser apenas inacessíveis, mas também invisíveis para os dispositivos que executam o acesso à rede;

3.3.5.9. O acesso aos aplicativos deve ser oferecido, no mínimo, por meio das seguintes opções:

3.3.5.9.1. Menu do aplicativo publicado no agente instalado no dispositivo;

3.3.5.9.2. Acesso direto e transparente após a conexão do dispositivo à nuvem de verificação de postura de segurança.

3.3.5.10. A definição de aplicativos, ou segmentos de aplicativos, deve ter a flexibilidade de oferecer suporte ao nome do host (FQDN), endereço IP ou domínio curinga;

3.3.5.10.1. A solução deve fazer com que cada solicitação de usuário flua por meio de políticas contextuais para autenticação e autorização consistentes, além de fornecer um ponto unificado de monitoramento e registro;

3.3.5.10.2. A solução deve usar túneis criptografados do tipo TLS/DTLS versões 1.2 ou 1.3, ou Wireguard;

3.3.5.10.3. A solução deve ser protegida contra-ataques "Man-in-the-middle" (MITM);

3.3.5.10.4. A plataforma deve oferecer suporte a vários provedores de identidade (IdP) e vários domínios na mesma instância e console de gerenciamento, oferecendo suporte à autenticação por meio do protocolo SAML 2.0. Dessa forma, deverá possibilitar o acesso seguro a outras diferentes unidades e terceiros aos recursos privados do CLIENTE, além de possibilitar a simplificação e modernização da conectividade e outras integrações futuras;

3.3.5.10.5. A solução deve permitir o acesso a quais recursos por meio de uma estrutura de política básica que leve em consideração quaisquer atributos de usuário fornecidos pelo IdP, incluindo os personalizados, e o estado contextual do dispositivo;

3.3.5.10.6. A solução deve trazer o monitoramento da atividade do usuário, dando às equipes de TI opções fáceis de monitoramento e gerenciamento de todas as atividades de forma granular, entendendo quais usuários, quando, quais aplicações e quais políticas autorizaram ou negaram o acesso, considerando o status da postura e a localização do usuário e de seu dispositivo;

3.3.5.10.7. A solução deve usar o console baseado na Web para criar e editar políticas. O portal de gerenciamento central deve trazer: Controle de acesso centralizado; Gestão de políticas; Configuração postural; Status da estrutura que suporta a solução e seus conectores; gerenciar a segmentação de acessos ou recursos;

3.3.5.10.8. Suporta a configuração de qualquer aplicação TCP ou UDP com tráfego originado pelo usuário de forma transparente, sem alterações ou customizações no cliente original;

3.3.5.10.9. Permitir o agrupamento de aplicações ou recursos para facilitar a criação de políticas (Ex: Aplicações Administrativas);

3.3.5.10.10. A solução deve suportar o gerenciamento de políticas de acesso via API;

3.3.5.10.11. A solução deve suportar diferentes tipos de validação de postura. O suporte para cada tipo pode variar dependendo da plataforma (Windows, Mac, Linux, iOS e Android), e é necessário que pelo menos 2 dos seguintes tipos por plataforma sejam suportados: Validação da presença de um Antivírus; Validação de certificado do cliente (chave privada e pública) assinada por uma CA específica; Validação de certificado confiável no dispositivo; Validação de qualquer processo em execução na máquina, incluindo validação da assinatura do fabricante; Validação de máquina no domínio; Validação de disco criptografado; Validação de Registro de Chaves no Windows; Validação da presença de um arquivo; Exigência de uma versão mínima do Sistema Operacional; Detectar alterações não autorizadas em dispositivos móveis, negando o acesso conforme estabelecido pelas políticas de acesso;

3.3.5.10.12. A solução deve ter mecanismos de proteção e políticas de postura granular para cada acesso à aplicação, preservando o conceito de zero trust, permitindo oferecer e impor maiores restrições a aplicações mais críticas, e menos restritas a aplicações consideradas menos críticas pelo administrador da plataforma. Ex.: para acessar o aplicativo "A" do **SENAR-AR/MS**, é necessário estar autenticado, fazer parte de um grupo pré-determinado de usuários, ter Antivírus ativo no dispositivo, ter o certificado do **SENAR-AR/MS** presente no dispositivo e fazer parte do domínio do AD. Para acessar o aplicativo "B" você só precisa ser autenticado.

3.3.5.10.13. A solução também deve oferecer na mesma plataforma, sem a necessidade de instalação de componentes adicionais, suporte ao usuário sem o uso de agentes para fornecer acesso a aplicativos privados por meio de navegadores da Web usando extensões totalmente suportadas pelo fabricante da solução. O seguinte navegador deve ser suportado, no mínimo: Google Chrome.

3.3.5.10.14. A solução deve permitir a integração ativa com soluções NGAV (Next-Gen Antivírus) para monitoramento de vetores de ataque em dispositivos, com ação concatenada revogando e restabelecendo a conectividade de acordo com a integração dinâmica dos dois componentes;

3.3.5.10.15. Esta integração ativa com soluções NGAV deve ser integrada com o agente da plataforma ZTNA, sem necessidade de licenciamento adicional;

3.3.5.10.16. Para este item de integração ativa com soluções NGAV, serão aceitas composições com produtos de diferentes fornecedores;

3.3.5.10.17. A solução deve ser capaz de detectar os seguintes ataques de estrutura MITRE ATT&CK, ou permitir a integração com soluções EDR, para alcançar:

a) T1046: Verificação de Serviço de Rede;

- b) T1565.001: Manipulação de dados;
- c) T1021: Serviços Remotos;
- d) T1210: Exploração de Serviços Remotos;
- e) T1110: Força Bruta;
- f) T1558: Roubar ou falsificar tíquetes Kerberos;
- g) T1087.002: Descoberta de Conta: Conta de Domínio;
- h) T1595: Varredura ativa;
- i) T1595.002: Verificação ativa: Verificação de vulnerabilidade;
- j) T1592: Coletar informações do host Victim;
- k) T1190: Explorar aplicativo voltado para o público;

3.3.6. Proteção Contra Ameaças da Web | DNS e Filtro de Navegação na Web

3.3.6.1. Proteção segura da camada DNS e navegação na Web em dispositivos minimamente para, mas não se limitando a, Windows e MacOS. A solução deve proteger os usuários contra sites maliciosos, ransomware ou ataques de phishing, filtrando domínios e URLs. A filtragem da Web e a proteção contra ameaças nos lados do cliente e do servidor para desempenho ideal devem ser a base dessa funcionalidade.

3.3.6.2. Proteção contra falsificação de DNS. A resolução de DNS deve ser protegida e executada por meio dos componentes da solução que permitem o uso, mas não se limitando a os seguintes componentes:

3.3.6.2.1. Resolução através do serviço de DNS central da plataforma (nuvem do fornecedor da solução);

3.3.6.2.2. Resolução através do conector instalado na infraestrutura da **CONTRATADA**;

3.3.6.2.3. Resolução pelo agente instalado no dispositivo.

3.3.6.3. Deve fornecer categorização de conteúdo para controle granular e proteção de locais da web acessados pelos usuários (URLs);

3.3.6.3.1. A categorização deve ser fornecida, permanentemente atualizada e gerenciada pelo provedor da solução;

3.3.6.3.2. Deve permitir o uso de curingas (*) nas políticas de acesso. Por exemplo: deve ser capaz de identificar e categorizar "portal.com.br" e "*.portal.com.br";

3.3.6.3.3. As políticas devem ser aplicáveis a diferentes perfis de acesso, considerando usuários, dispositivos, contexto de uso ou qualquer combinação dos itens acima mencionados;

3.3.6.3.4. Deve habilitar configurações de listas de bloqueio personalizadas e exceções (listas brancas/negras) que se sobreponham às categorizações oferecidas pela plataforma.

3.3.6.4. A solução SSE deve fornecer proteção pronta para uso contra ameaças conhecidas, incluindo botnets, domínios de phishing e domínios recém-registrados, com atualizações de inteligência de ameaças entrando em vigor em menos de um minuto.

3.3.6.5. A solução proposta deve incluir um plug-in do Chrome e oferecer suporte completo para Chromebooks, especificamente adaptado para atender às necessidades das instituições educacionais K-12. Ele também deve fornecer conformidade com os requisitos de segurança SLED (Estaduais, Locais e Educacionais) dos EUA para garantir proteção robusta para o setor educacional.

3.3.6.6. A solução SSE deve oferecer descriptografia de tráfego da Web e inspeção de URL maliciosa, estendendo os recursos de DPI-SSL ao endpoint. Ele também deve incluir filtragem de URL baseada em risco e filtragem de DNS para fornecer funcionalidade abrangente de Secure Web Gateway (SWG).

3.3.6.7. A solução proposta deve oferecer suporte à detecção de URL baseada em risco, que deve ser integrada aos recursos de filtragem de URL da solução proposta, com a capacidade de avaliar riscos mesmo em URLs permitidas.

3.3.5. Proteção de Aplicativos Públicos (SaaS) | Agente de Segurança de Acesso à Nuvem (CASB)

3.3.5.1. A plataforma deve fornecer controle de acesso e sobreposição de segurança para aplicativos SaaS. O CASB deve fornecer visibilidade não apenas sobre quais aplicativos SaaS os usuários estão acessando, mas também sobre o que os usuários estão fazendo no aplicativo SaaS. Deve permitir uma camada de segurança de confiança de dispositivo sem atrito para login único existente, eliminando riscos associados a ataques de phishing e controle de contas.

3.3.5.2. A solução deve incluir proteção para aplicativos de nuvem pública do tipo "SaaS" (Software as a Service) minimamente para, mas não se limitando a, dispositivos do tipo Windows ou MacOS.

3.3.5.3. Deve permitir o uso da plataforma em modo proxy, onde é permitido determinar pelo menos os seguintes modos de operação:

3.3.5.3.1. Lista de endereços IP permitidos: os acessos serão permitidos somente se forem originários de origens (endereços IP) previamente determinadas pelo administrador da plataforma;

3.3.5.3.2. Aplicações Federadas, onde a estratégia de acesso autentica o dispositivo para cada aplicação nesta condição de uso;

3.3.5.3.3. Baseado em proxy: Semelhante ao modo de operação da lista de permissões (endereços IP), onde o administrador pode configurar e associar o acesso a um site hospedado.

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

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

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

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

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

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

3.3.6.6. Autenticação via de tuneis IPsec via certificado digital para VPNs Site-to-Site e Client-to-Site;

3.3.6.7. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android; Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico;

3.3.6.8. 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;

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

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

3.3.6.11. 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;

3.3.6.12. 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;

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

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

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

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

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

3.3.7.2. 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;

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

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

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

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

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

3.3.7.8. Implementar interface CLI segura através do protocolo SSH;

3.3.7.9. Possuir Antivírus 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;

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

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

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

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

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

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

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

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

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

3.3.7.19. A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS;

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

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

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

3.3.7.22. 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;

3.3.8. Requisitos de Proteção Contra-ataques Avançados para solução de proteção de perímetro

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

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

3.3.8.3. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH; Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

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

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;

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

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

3.3.8.7. 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;

3.3.8.8. 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;

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

3.3.8.10. 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;

3.3.8.11. Conter ameaças avançadas de dia zero;

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

- 3.3.8.13.** Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;
- 3.3.8.14.** 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;
- 3.3.8.15.** Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado;
- 3.3.8.16.** Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado;
- 3.3.8.17.** Possuir Antivírus 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;
- 3.3.8.18.** Mitigar ameaças de dia zero de forma transparente para o usuário final;
- 3.3.8.19.** Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro;
- 3.3.8.20.** Implementar mecanismo de pesquisa por diferentes intervalos de tempo;
- 3.3.8.21.** Mitigar ameaças de dia zero via tráfego de internet;
- 3.3.8.22.** Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança;
- 3.3.8.23.** Mitigar ameaças de dia zero que possam burlar o sistema operacional emulado;
- 3.3.8.24.** A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo;
- 3.3.8.25.** Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso;
- 3.3.8.26.** Conter e mitigar exploits avançados;
- 3.3.8.27.** 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 Antivírus 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);
- 3.3.8.28.** Suporte a submissão manual de arquivos para análise através do serviço de Sandbox;
- 3.3.8.29.** 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;
- 3.3.8.30.** 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;

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

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

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

3.3.8.34. Inspeção profunda de memória em tempo real;

3.3.8.35. Inspeção profunda de pacotes livre de remontagem;

3.3.8.36. Descriptografia e inspeção TLS/SSL;

3.3.8.37. Inteligência e controle de aplicativos;

3.3.8.38. Recursos SD-WAN seguros;

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

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

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

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

3.3.9.4. Permitir a customização de página de bloqueio;

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

3.3.9.6. Deve permitir submissão de novos sites para categorização;

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

3.3.9.6.2. 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.

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

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

3.3.10. Requisitos de autenticação para solução de proteção de perímetro

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

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

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

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

3.3.10.5. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o login 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;

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

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

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

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

3.3.10.10. A solução deve possibilitar SSO via API;

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

3.3.11. Requisitos de Administração para solução de proteção de perímetro

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

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

- 3.3.11.3.** Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional;
- 3.3.11.4.** Possuir mecanismo para agendamento realização das cópias de segurança (backups) de configuração;
- 3.3.11.5.** Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP;
- 3.3.11.6.** A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante;
- 3.3.11.7.** Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões;
- 3.3.11.8.** Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real;
- 3.3.11.9.** Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados;
- 3.3.11.10.** Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de “ICMP Unreachable” para máquina de origem do tráfego, “TCP-Reset” para o cliente, “TCP-Reset” para o servidor ou para os dois lados da conexão;
- 3.3.11.11.** Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas;
- 3.3.11.12.** Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento;
- 3.3.11.13.** Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF;
- 3.3.11.14.** Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP IPV4 e IPV6;
- 3.3.11.15.** Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização;

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

3.3.11.17. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreamento das configurações aplicadas no produto;

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

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

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

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

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

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

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

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

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

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

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

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

3.3.12. Requisitos do Software de Gerenciamento e Relatórios para Solução de Proteção de Perímetro

3.3.12.1. 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:

- 3.3.12.1.1.** Os firewalls devem possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de toda a solução;
- 3.3.12.1.2.** Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções;
- 3.3.12.1.3.** 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;
- 3.3.12.1.4.** Caso seja entregue em appliance virtual dever ser compatível com VMware ESXi ou Hyper-V;
- 3.3.12.1.5.** Caso seja entregue em appliance físico, o equipamento deve possuir fonte de chaveamento automático (100-240 VAC), com formato compatível para instalação em rack;
- 3.3.12.1.6.** Deve suportar organizar os dispositivos administrados em grupos;
- 3.3.12.1.7.** Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;
- 3.3.12.1.8.** Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;
- 3.3.12.1.9.** Deve permitir a centralização da administração de regras e políticas dos firewalls configurados de forma individual e em cluster;
- 3.3.12.2.** O gerenciamento deve permitir/possuir:
 - 3.3.12.2.1.** Criação e administração de políticas de firewall e controle de aplicação;
 - 3.3.12.2.2.** A solução deve permitir acesso concorrente de administradores;
 - 3.3.12.2.3.** Deve permitir o provisionamento de configuração por "Zero-Touch";
 - 3.3.12.2.4.** Deve permitir a integração com LDAP ou Radius;
 - 3.3.12.2.5.** A solução de gerenciamento deverá ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL;
 - 3.3.12.2.6.** 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;
 - 3.3.12.2.7.** A solução deve possuir tela situacional com os 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;
 - 3.3.12.2.8.** Deverá permitir atualizar o sistema operacional de múltiplos equipamentos gerenciados de uma única vez;
 - 3.3.12.2.9.** A solução deve possuir Dashboard com sumário de alertas e informação de status de licença;

- 3.3.12.2.10.** A solução deverá permitir seu gerenciamento por Web GUI utilizando protocolo HTTPS sem a necessidade de uso de cliente ou console do tipo aplicativo;
- 3.3.12.2.11.** Deve manter um canal de comunicação segura, com encriptação baseada HTTPS, entre todos os componentes que fazem parte da solução de firewall;
- 3.3.12.2.12.** A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão no console de gerência local do firewall sem a necessidade de o administrador utilizar endereço IP do dispositivo, URL ou FQDN;
- 3.3.12.2.13.** 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;
- 3.3.12.2.14.** Os modelos de configuração ou “templates” devem suportar configurações de interfaces físicas ou virtuais;
- 3.3.12.2.15.** 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;
- 3.3.12.2.16.** Deverá permitir visualizar a diferença nas mudanças antes que a configurações sejam implantadas;
- 3.3.12.2.17.** 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;
- 3.3.12.2.18.** 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;
- 3.3.12.2.19.** 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;
- 3.3.12.2.20.** 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;
- 3.3.12.2.21.** 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;

3.3.12.2.22. 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;

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

3.3.12.2.24. Deverá suportar logs do tipo Netflow, IPFIX ou Syslog, para a gerar Reports;

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

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

3.3.12.2.27. 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;

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

3.3.12.2.29. 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;

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

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

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

3.3.12.2.33. A solução deve permitir visualização de eventos correlacionados que possam ser investigados por: Lista de eventos correlacionados com opção de navegação "drilldown"; ou Modo gráfico; ou Lista de logs;

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

3.3.13. ITEM 2 - Solução EPP (Endpoint Protection), visando a proteção proativa contra malwares, ransomwares e ameaças persistentes avançadas (APTs) em estações de trabalho, servidores de rede e dispositivos móveis.

3.3.14. Requisitos Técnicos para Solução para Proteção de Endpoints

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

3.3.14.1.1. 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;

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

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

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

3.3.14.2. A solução proposta deve fornecer tecnologias de proteção da próxima geração, sendo no mínimo:

3.3.14.2.1. Proteção contra ameaças sem arquivos (Fileless);

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

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

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

3.3.14.2.5. 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;

3.3.14.2.6. 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;

3.3.14.2.7. 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;

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

3.3.14.2.9. 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;

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

3.3.14.3.1. Controles de aplicativos;

3.3.14.3.2. Controle web e dispositivos;

3.3.14.3.3. HIPS e Firewall;

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

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

3.3.14.3.6. 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;

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

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

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

3.3.14.4.1. Bloqueio de aplicativos com base em sua categorização;

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

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

3.3.14.4.4. 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;

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

3.3.14.4.6. 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;

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

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

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

3.3.14.4.11. 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;

3.3.14.4.12. 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;

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

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

3.3.14.4.15. 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;

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

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

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

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

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

3.3.14.4.21. 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;

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

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

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

3.3.14.4.25. 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;

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

3.3.14.4.27. 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;

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

- 3.3.14.4.28.** A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais;
- 3.3.14.4.29.** A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;
- 3.3.14.4.30.** 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;
- 3.3.14.4.31.** 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;
- 3.3.14.4.32.** 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;
- 3.3.14.4.33.** O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração;
- 3.3.14.4.34.** O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões;
- 3.3.14.4.35.** A solução proposta deve suportar o controle de scripts executados em PowerShell.
- 3.3.14.4.36.** A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados;
- 3.3.14.4.37.** A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo;
- 3.3.14.4.38.** A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem;
- 3.3.14.4.39.** A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor;
- 3.3.14.4.40.** 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;
- 3.3.14.4.41.** A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint;
- 3.3.14.5.** A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
- 3.3.14.5.1.** Filtro de anexos;
- 3.3.14.5.2.** Verificação de mensagens de e-mail ao receber, ler e enviar;
- 3.3.14.5.3.** A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo;

- 3.3.14.5.4.** A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;
- 3.3.14.5.5.** 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.);
- 3.3.14.5.6.** A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registro do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware;
- 3.3.14.5.7.** 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;
- 3.3.14.5.8.** A solução proposta deve incluir suporte ao protocolo IPv6;
- 3.3.14.5.9.** A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente;
- 3.3.14.5.10.** A solução proposta deve incorporar a tecnologia de autoproteção de aplicação;
- 3.3.14.5.11.** Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo;
- 3.3.14.5.12.** Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários;
- 3.3.14.5.13.** A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar;
- 3.3.14.5.14.** 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;
- 3.3.14.5.15.** A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística;
- 3.3.14.5.16.** A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail;
- 3.3.14.5.17.** A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária;
- 3.3.14.5.18.** A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows;

- 3.3.14.5.19.** 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;
- 3.3.14.5.20.** 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;
- 3.3.14.5.21.** A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft;
- 3.3.14.5.22.** A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização;
- 3.3.14.5.23.** 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.
- 3.3.14.5.24.** A solução proposta deve suportar endereços IPv6;
- 3.3.14.5.25.** A solução proposta deve suportar verificação em duas etapas (autenticação);
- 3.3.14.5.26.** A solução proposta deve prever a instalação, atualização e remoção centralizada de software anti-malware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento;
- 3.3.14.5.27.** A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração;
- 3.3.14.5.28.** 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;
- 3.3.14.5.29.** A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes;
- 3.3.14.5.30.** A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware;
- 3.3.14.5.31.** A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas;
- 3.3.14.5.32.** A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas;
- 3.3.14.5.33.** A solução proposta deve permitir a gestão de um componente que controle o trabalho com dispositivos de E/S externos;
- 3.3.14.5.34.** A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet;

- 3.3.14.5.35.** A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em Microsoft Hyper-V;
- 3.3.14.5.36.** A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes;
- 3.3.14.5.37.** A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS;
- 3.3.14.5.38.** 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;
- 3.3.14.5.39.** A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração;
- 3.3.14.5.40.** A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos;
- 3.3.14.5.41.** A solução proposta deve ter a capacidade de excluir atualizações baixadas;
- 3.3.14.5.42.** A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados;
- 3.3.14.5.43.** A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma inglês e português;
- 3.3.14.5.44.** A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints;
- 3.3.14.5.45.** 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;
- 3.3.14.5.46.** Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou;
- 3.3.14.5.47.** 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;
- 3.3.14.5.48.** 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;
- 3.3.14.5.49.** A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor;
- 3.3.14.5.50.** A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
- 3.3.14.5.50.1.** Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível;

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

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

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

3.3.15. Do Módulo de Proteção de Endpoint

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

3.3.15.1.1. Windows 10; Windows 11;

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

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

3.3.15.2. Sistemas operacionais Linux de 64 bits:

3.3.15.2.1. CentOS 6.7 e posterior; CentOS 7.2 e posterior; CentOS Stream 8; CentOS Stream 9; Debian GNU/Linux 11.0 e posterior; Debian GNU/Linux 12.0 e posterior; Ubuntu 20.04 LTS; Ubuntu 22.04 LTS; Sistemas operacionais Arm de 64 bits; Ubuntu 22.04 LTS;

3.3.15.3. Sistemas operacionais MAC OS:

3.3.15.3.1. MacOS 12 – 15;

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

3.3.15.4.1. Microsoft Hyper-V Server 2019 e superiores;

3.3.16. Do Módulo de Gerenciamento Avançado

3.3.16.1. A solução proposta deve suportar arquitetura cloud-native e on-premise;

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

3.3.16.2.1. Amazon Web Services e Microsoft Azure;

3.3.16.2.2. 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;

3.3.16.2.3. 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;

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

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

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

3.3.16.2.7. 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;

3.3.16.2.8. 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;

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

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

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

3.3.16.2.12. 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 um único/múltiplos dispositivos com base nas seguintes regras de ativação: Status do dispositivo; Tag; Diretório ativo; Proprietários de dispositivos; Hardware;

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

3.3.16.3.1. E-mail; Registro de sistema; SMS;

3.3.16.3.2. 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;

3.3.16.3.3. 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;

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

3.3.16.3.5. Bluetooth; Dispositivos móveis; Modems externos; CD/DVD; Câmeras e scanners; MTPs; E a transferência de dados para dispositivos móveis;

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

3.3.16.3.7. 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;

3.3.16.4. 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:

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

3.3.16.4.2. Estruturas de grupos do Active Directory;

3.3.16.4.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador.

3.3.16.5. 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;

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

Verificação manual; Verificação no acesso; Verificação por demanda; Verificação de arquivos compactados; Verificação de arquivos individuais, pastas e unidades; Bloqueio e verificação de scripts; Proteção contra alteração de registros; Proteção contra estouro de buffer; Verificação em segundo plano/inativa; Verificação de unidade removível na conexão com o sistema;

3.3.16.5.2. 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;

3.3.16.5.3. 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;

3.3.16.5.4. 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;

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

3.3.16.5.6. 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;

3.3.16.5.7. A solução proposta deve suportar Windows Failover Cluster;

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

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

3.3.16.5.10. 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;

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

3.3.16.5.12. 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;

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

- 3.3.16.5.14.** A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB;
- 3.3.16.5.15.** A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB;
- 3.3.16.5.16.** A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes;
- 3.3.16.5.17.** A solução proposta deverá possuir controles para download de DLL e drivers;
- 3.3.16.5.18.** 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 específico de prevenção de intrusão;
- 3.3.16.5.19.** 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;
- 3.3.16.5.20.** 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);
- 3.3.16.5.20.** A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server;
- 3.3.16.5.21.** 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;
- 3.3.16.5.22.** 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;
- 3.3.16.5.23.** 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;
- 3.3.16.5.24.** 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;
- 3.3.16.5.25.** A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração;
- 3.3.16.5.26.** A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários;

3.3.16.5.27. 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;

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

3.3.16.5.29. 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;

3.3.16.5.30. 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;

3.3.16.5.31. 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.;

3.3.16.5.32. 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 definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis;

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

3.3.16.5.34. 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;

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

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

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

3.3.16.5.38. 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;

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

3.3.16.5.40. 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;

3.3.16.5.41. 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;

3.3.16.4. A solução proposta deverá suportar os seguintes servidores de banco de dados: Windows; Microsoft SQL Server; Microsoft Banco de dados SQL do Azure; MySQL Standard e Enterprise; MariaDB; PostgreSQL;

3.3.16.4.1. Linux: MySQL; MariaDB; PostgreSQL;

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

3.3.16.5.1. Servidor Microsoft Hyper-V 2012 de 64 bits e superiores;

3.3.17. Do Módulo de Gerenciamento Simplificado

3.3.17.1. A solução proposta deve suportar arquitetura cloud;

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

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

3.3.17.4. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque;

3.3.17.5. 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;

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

3.3.17.7. A solução proposta deve incluir informações do endpoint:

3.3.17.7.1. IP público de internet;

3.3.17.7.2. IP interno do dispositivo;

3.3.17.7.3. Versão do agente de proteção;

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

3.3.17.7.5. Informações do sistema operacional;

3.3.18. Do Módulo de Gerenciamento de Dispositivos Móveis

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

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

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

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

3.3.18.3.1. iOS 10 e superiores ou iPadOS 13 e superiores;

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

3.3.18.3.3. A solução proposta deve suportar dispositivos iOS supervisionados;

3.3.18.3.4. 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;

3.3.18.3.5. 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;

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

3.3.18.3.7. 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);

3.3.18.3.8. 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;

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

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

3.3.18.3.11. A solução proposta deve ter recursos de containerização para dispositivos Android;

3.3.18.3.12. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android: Dados em contêineres; Contas de e-mail corporativo; Configurações para conexão à rede Wi-Fi corporativa e VPN; Nome do ponto de acesso (APN); Perfil do Android for Work; Recipiente KNOX; Chave do gerenciador de licença KNOX;

3.3.18.3.13. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS: Todos os perfis de configuração instalados; Todos os perfis de provisionamento; O perfil iOS MDM;

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

3.3.18.3.15. 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;

3.3.18.3.16. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa.

3.3.18.4. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:

3.3.18.4.1. Critérios de verificação do dispositivo;

3.3.18.4.2. 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;

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

3.3.18.4.4. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo: Cartões de memória e outras unidades removíveis; Câmera do dispositivo; Conexões Wi-Fi; Conexões Bluetooth; Porta de conexão infravermelha; Ativação do ponto de acesso Wi-Fi; Conexão de área de trabalho remota; Sincronização de área de trabalho;

3.3.18.4.5. Definir configurações da caixa de correio do Exchange; Configurar caixa de e-mail em dispositivos iOS MDM; Configure contêineres Samsung KNOX; Definir as configurações do perfil do Android for Work; Configurar e-mail/calendário/contatos; Defina as configurações de restrição de conteúdo de mídia; Definir configurações de proxy no dispositivo móvel; Configurar certificados e SCEP;

3.3.18.4.6. 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;

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

3.3.18.5.1. Huawei App Gallery e Apple App Store;

3.3.18.5.2. Portal de inscrição móvel KNOX;

3.3.18.5.3. Pacotes de instalação pré-configurados independentes;

3.3.18.5.4. 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;

- 3.3.18.5.5.** A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente;
- 3.3.18.5.6.** A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros: VMware AirWatch 9.3 ou posterior; MobileIron 10.0 ou posterior; IBM MaaS360 10.68 ou posterior; Microsoft Intune 1908 ou posterior; SOTI MobiControl 14.1.4 (1693) ou posterior;
- 3.3.18.5.7.** A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo;
- 3.3.18.5.8.** A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de: Galeria de aplicativos Huawei; Loja de aplicativos da Apple;
- 3.3.18.5.9.** A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo;
- 3.3.18.5.10.** A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo;
- 3.3.18.5.11.** 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;
- 3.3.18.5.12.** A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena;
- 3.3.18.5.13.** 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;
- 3.3.18.5.14.** 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;
- 3.3.18.5.15.** A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores;
- 3.3.18.5.16.** A solução proposta deve fornecer funcionalidade Antirroubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente;
- 3.3.18.5.17.** A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel;
- 3.3.18.5.18.** A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis;
- 3.3.18.5.19.** A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel;
- 3.3.18.5.20.** A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido;

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

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

3.3.19. Do Módulo de EDR

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

3.3.19.2. 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;

3.3.19.3. 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;

3.3.19.4. Deve apresentar informações detalhadas contendo: Processo; Arquivos; Chaves de registro; Conexões de rede; SHA256 e MD5;

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

3.3.19.6. Deve apresentar informações detalhadas contendo: Usuário que executou a ação; Informações acesso privilegiado.

3.3.20. ITEM 3 - Plataforma de conscientização em segurança da informação, baseada em aprendizagem automatizada e adaptativa, destinada ao treinamento contínuo de usuários da rede corporativa do SENAR-AR/MS. Quantidade: 50 (cinquenta) licenças.

3.3.20.1. Compatibilidade com sistemas operacionais de desktop: Windows e MacOs;

3.3.20.2. Compatibilidade com sistemas operacionais de dispositivos mobiles: iOS e Android;

3.3.20.3. Suporte a browsers: Google Chrome;

3.3.20.4. A plataforma de treinamento deverá conter base de conhecimento com as principais dúvidas, dicas e guias de recomendações para o administrador da plataforma;

3.3.20.5. A plataforma deverá conter vídeos de demonstração de uso da solução;

3.3.20.6. A plataforma deverá conter uma base com possíveis mensagens/banner de alertas e segurança para compartilhamento dentro do programa de conscientização;

3.3.20.7. Durante a validade da licença, as atualizações da plataforma devem ser entregues sem ônus adicional;

3.3.20.8. Atualizações devem ser disponibilizadas para:

3.3.20.8.1. Atualização de conteúdo dos treinamentos.

3.3.20.9. Adição de novos conteúdos;

3.3.20.10. Novas funcionalidades para facilitar administração;

3.3.20.11. Novas funcionalidades para facilitar interação dos usuários;

3.3.20.12. Melhorias gerais do sistema e correção de bugs;

3.3.20.13. As atualizações na plataforma devem ser realizadas sem causar indisponibilidade ou afetar as funcionalidades;

3.3.20.14. O usuário deverá informar possíveis Phishing recebido, para isso a plataforma deve disponibilizar de funcionalidade ou plug-in para envio de notificação aos administradores;

3.3.20.15. O plano de atualização da plataforma deve:

3.3.20.15.1. Ser apresentado ao administrador da plataforma dias antes da sua execução;

3.3.20.15.2. Possibilitar ao administrador sugerir melhorias e votar estas melhorias durante a fase de discussão destas;

3.3.20.15.3. A interface da plataforma de treinamento, as notificações por e-mail e todo material de treinamento deverá ser disponibilizado minimamente no idioma português;

3.3.20.16. A plataforma deverá gerar automaticamente os seguintes relatórios de acompanhamento ao Administrador:

3.3.20.16.1. Relatório resumo com informações sobre o progresso dos usuários;

3.3.20.16.2. Deve ser enviado no mínimo semanalmente;

3.3.20.16.3. Conter análise dos usuários por categoria de desempenho;

3.3.20.16.4. Conter link para relatório completo do treinamento;

3.3.20.16.5. Conter links com recomendações para alteração das categorias de treinamento baseado no desempenho do usuário.

3.3.20.17. Relatório geral detalhado da empresa:

3.3.20.17.1. Deve conter lista de administradores da plataforma;

3.3.20.17.2. O número de usuários (número geral e por status de treinamento);

3.3.20.17.3. Informações sobre uso de licenças;

3.3.20.17.4. Informações sobre categorias de desempenho;

3.3.20.17.5. Lista completa de usuários, especificando o grupo de treinamento pertencente;

3.3.20.17.6. A data em que o usuário consentiu em participar dos treinamentos;

3.3.20.17.7. As datas de conclusão planejadas e calculadas;

3.3.20.17.8. O número de unidades de treinamento com datas expiradas;

3.3.20.17.9. O número de testes não iniciados;

3.3.20.17.10. O número de testes a serem repetidos;

3.3.20.17.11. O número de certificados recebidos;

3.3.20.17.1. Exportar o relatório em formato XLSX;

3.3.20.17.2. Conter informações detalhadas sobre todos os alunos que estão em treinamento ou com treinamento suspenso;

3.3.20.17.2. Relatório sobre treinamento por grupo e individualizado.

3.3.20.17.3. Histórico de treinamento do usuário;

3.3.20.17.4. O usuário deverá receber e-mails semanais com relatórios de desempenho e de treinamento;

3.3.20.17.5. Requisitos para estatísticas de campanhas simuladas de phishing.

3.3.20.18. A plataforma de treinamento deve auxiliar na realização dos seguintes objetivos em uma organização:

3.3.20.18.1. Reduzir o risco de incidentes quando os funcionários usam recursos de TI, trocam dados pela Internet e trocam dados inadequadamente usando dispositivos móveis;

3.3.20.18.2. Minimizar os custos trabalhistas de gerenciamento de treinamento para funcionários.

3.3.20.19. A plataforma de treinamento deve resolver as seguintes tarefas:

3.3.20.19.1. Definir metas de treinamento e atribuir um programa de treinamento aos usuários;

3.3.20.19.2. Fornecer aos usuários os materiais de treinamento relevantes para o programa de treinamento;

3.3.20.19.3. Fornecer informações sobre o programa de treinamento na forma de relatório e diagramas;

3.3.20.20. A plataforma deve incluir os seguintes elementos:

3.3.20.20.1. Materiais de treinamento (conteúdo);

3.3.20.20.2. Simulador de ataque de phishing;

3.3.20.20.3. O acesso à plataforma de treinamento deve ser feito via internet, utilizando protocolos HTTPS e HTTP;

3.3.20.20.4. O administrador da plataforma de treinamento deve ser capaz de gerenciar o processo de treinamento de todos os usuários;

3.3.20.21. A plataforma deve executar automaticamente as seguintes etapas:

3.3.20.21.1. Criar horários de aula para grupos e cada usuário, com base no nível de destino selecionado do grupo;

3.3.20.21.2. Enviar notificações por e-mail automaticamente aos usuários;

3.3.20.21.3. Criar e ajustar um cronograma de treinamento individual para cada funcionário;

3.3.20.21.4. Atribuir todos os materiais de treinamento ao usuário;

3.3.20.21.5. Acompanhar o progresso do treinamento de cada usuário;

3.3.20.21.6. Fornecer relatórios de desempenho semanais aos usuários;

3.3.20.21.7. Enviar e-mails aos usuários com recomendações personalizadas, para que possam concluir o curso no prazo e com sucesso;

3.3.20.21.8. Enviar e-mails ao administrador com relatórios semanais, incluindo recomendações sobre como motivar um usuário para a comunicação fora da plataforma de treinamento.

3.3.20.21.9. A plataforma deve ser capaz de se integrar com o Microsoft Active Directory e com outros sistemas via OpenAPI para sincronizar listas de usuários.

3.3.20.22. O programa de treinamento da plataforma deve incluir, no mínimo, os seguintes tópicos:

3.3.20.22.1. Senhas e contas; Segurança de E-mail; Navegação na Web; Redes sociais e serviços de mensageria; Segurança do PC: Dispositivos móveis; Informação Confidencial; LGPD; Segurança de cartões de banco; PCI DSS; Infraestrutura industrial;

3.3.20.22.2. O programa de treinamento deve incluir lições com temas atuais que possam desenvolver as habilidades dos usuários nas seguintes áreas de segurança cibernética: Phishing; Links maliciosos; Ransomware; Arquivos perigosos; Aplicações maliciosas; Engenharia social.

3.3.21. Requisitos para o programa de treinamento

3.3.21.1. Cada tópico deve ser dividido em vários níveis dedicados à prática de um grupo específico de habilidades no campo da segurança cibernética.

3.3.21.2. Cada nível do programa deve corresponder a ameaças com vários graus de gravidade, desde ataques básicos e em larga escala até proteção contra-ataques complexos e direcionados.

3.3.21.3. Cada tópico deve incluir aulas (exercícios), material para reforço (e-mail), teste de conhecimento e simulação de um ataque de phishing.

3.3.21.4. Para concluir um tópico com sucesso, o usuário deve fazer o teste de conhecimento relacionado.

3.3.21.5. A transição para o próximo nível deve ser possível depois que todos os tópicos anteriores no nível apropriado foram realizados e o teste de conhecimento relacionado aprovado com sucesso.

3.3.22. Requisitos para materiais de treinamento:

3.3.22.1. A estrutura de aulas (incluindo exercícios) para cada tópico deve ser a mesma em todos os tópicos e deve seguir a sequência lógica abaixo:

3.3.22.1.1. Um conjunto de ações a serem realizadas;

3.3.22.1.2. Porque um usuário deve realizar essas ações;

3.3.22.1.3. As consequências potenciais de ações incorretas;

3.3.22.1.4. Os sinais de perigo que um usuário deve identificar;

3.3.22.1.5. As ações que um usuário deve realizar ao detectar sinais de perigo; o que fazer se as dúvidas permanecerem.

3.3.22.2. Os seguintes tipos de materiais de treinamento devem ser apresentados:

3.3.22.2.1. Aulas, incluindo parte teórica e exercícios práticos com feedback;

3.3.22.2.2. Testes de conhecimento;

3.3.22.2.3. Simulações de ataque de phishing;

3.3.22.2.4. Exercícios de reforço.

3.3.22.3. As aulas devem incluir:

3.3.22.3.1. Slides a serem estudados;

3.3.22.4. Devem conter:

3.3.22.4.1. Informações textuais e gráficas;

3.3.22.4.2. Botões para avançar e retornar aos slides;

3.3.22.4.3. Questões para autoavaliação;

3.3.22.4.4. Os exercícios de reforço devem consistir em coleção de conselhos ou recomendações para exercícios anteriores, bem como exemplos reais de consequências do não cumprimento das regras de segurança cibernética;

3.3.22.4.5. O teste deve consistir em questões às quais o usuário deve dar uma resposta ou múltipla escolha de opções;

3.3.22.4.6. Os resultados do teste devem indicar a aprovação ou não;

3.3.22.4.7. Deve ser possível definir um valor mínimo de acertos para êxito no teste;

3.3.22.4.8. Quando o teste for concluído, o usuário poderá dar feedback para cada questão, independentemente de ter respondido corretamente;

3.3.22.4.9. Os ataques simulados de phishing devem permitir que a reação do usuário à ameaça cibernética seja verificada;

3.3.22.4.10. Os materiais de treinamento devem ser adaptados para usuários que suas contas pessoais em um navegador de dispositivo móvel.

3.3.23. Requisitos para funcionalidade de simulação de ataques phishing

3.3.23.1. A plataforma de treinamento deve abranger duas opções de atribuição de ataques simulados de phishing:

3.3.23.1.1. Integrado ao caminho de aprendizagem automatizado para dominar especificamente o conjunto de habilidades criadas nas lições anteriores da unidade.

3.3.23.1.2. Possibilidade de criar uma companhia de phishing separada para um grupo específico de usuário não relacionados a nenhuma atividade de treinamento;

3.3.23.1.3. Um ataque de phishing simulado deve ser semelhante a uma mensagem real na forma de um texto com layout, imagens (opcional) e um link. Quando clicado, o link deve redirecionar o usuário para uma página simulada especial;

3.3.23.1.4. A página simulada para qual o usuário foi redirecionado no ataque simulado de phishing deve conter uma explicação sobre o motivo pelo qual o usuário foi parar naquele site,

uma descrição do e-mail que o usuário receber, bem como recomendações sobre o reconhecimento de e-mails de phishing.

3.3.23.1.5. A plataforma deve conter pelo menos trinta modelos de phishing diferentes que são enviados aos usuários durante o treinamento;

3.3.23.1.6. A campanha deve possibilitar ser agendada ou ser enviada imediatamente;

3.3.23.1.7. Quando configurada separada do programa de aprendizagem, a campanha de phishing deverá incluir vários modelos para o grupo de pessoas para envio aleatório de um determinado modelo para cada funcionário.

3.3.23.1.8. O usuário deverá ser considerado como aprovado no ataque de phishing simulado se ele (a) não clicar no link do e-mail e não for direcionado para a página simulada.

3.3.23.1.9. A conta pessoal deve ser uma página da web acessível ao usuário através de um link exclusivo que o usuário recebe por meio de notificações por e-mail;

3.3.23.1.10. O histórico de treinamento deve incluir uma lista de todas as tarefas concluídas e seus respectivos resultados;

3.3.23.1.12. O usuário deverá ser capaz de retornar ao material preenchido anteriormente para repetir o treinamento;

3.3.23.1.13. Na conta pessoal do usuário, deverá haver informações sobre andamento e estatísticas sobre os materiais abordados;

3.3.23.2. As estatísticas de treinamento devem ser visíveis para o usuário:

3.3.23.2.1. Informações sobre o nível sobre a habilidade alvo do usuário;

3.3.23.2.2. Porcentagem de habilidade adquiridas até o momento do número total de habilidades para um determinado nível alvo.

3.3.24. DOS REQUISITOS PARA CERTIFICADOS

3.3.24.1. O usuário deve receber um certificado após a conclusão bem-sucedida de cada tópico realizado;

3.3.24.2. O tópico deve ser considerado concluído com êxito quando o usuário tiver concluído com êxito o teste e for aprovado na simulação de ataque de phishing;

3.3.24.3. O certificado deve ser apresentado em formato eletrônico na interface do usuário e estar disponível para download;

3.3.24.4. O administrador deve ter a possibilidade de escolher como representar o nome do funcionário e outros campos personalizados no certificado.

3.4. JUSTIFICATIVA DO LOTE ÚNICO

3.4.1. A contratação em lote único é tecnicamente necessária devido à interdependência operacional e funcional entre os três componentes que compõem a estratégia de segurança da informação da instituição: a proteção perimetral (firewall), a proteção de endpoint (EPP/EDR) e

a plataforma de conscientização em segurança. Esses elementos são projetados para funcionar como **camadas complementares de defesa**, devendo operar de forma integrada, coordenada e com compartilhamento contínuo de telemetria e políticas.

3.4.2. A contratação fragmentada, com fornecedores distintos, comprometeria diretamente a eficácia da segurança institucional por gerar riscos de incompatibilidade, falhas de comunicação entre sistemas e ausência de correlação completa dos eventos de ameaça. A arquitetura moderna de segurança — alinhada à ISO/IEC 27001, ao NIST Cybersecurity Framework (Identify–Protect–Detect–Respond–Recover) e aos princípios Zero Trust — exige **visibilidade unificada de ameaças, resposta orquestrada e padronização de políticas em toda a superfície de ataque**, o que só é possível quando todos os componentes pertencem a uma mesma solução ou, no mínimo, são geridos de ponta a ponta pela mesma empresa responsável.

3.4.3. Do ponto de vista técnico, o firewall de próxima geração precisa correlacionar eventos de rede com eventos de endpoint (EPP/EDR), consumindo telemetria, alertas, indicadores de comprometimento (IOCs) e informações de postura dos dispositivos para identificar, bloquear e responder a ameaças em tempo real. Quando cada componente é contratado separadamente, há risco concreto de:

- a) incompatibilidade entre consoles, agentes, APIs e motores de detecção;
- b) falhas de integração entre firewall e EPP/EDR, prejudicando a análise de ameaças multi-vetoriais;
- c) ausência de correlação automática entre eventos de rede e de endpoint, diminuindo a capacidade de detectar ataques laterais;
- d) atrasos na resposta a incidentes, já que fornecedores diferentes não compartilham telemetria nativa;
- e) lacunas na aplicação uniforme de políticas de segurança;
- f) aumento do risco operacional, inclusive pela possibilidade de um ataque passar despercebido em uma das camadas.

3.4.4. Além disso, a plataforma de conscientização em segurança da informação depende diretamente do EPP/EDR para operar adequadamente. A maioria das plataformas de treinamento adaptativo utiliza a telemetria do próprio endpoint para ajustar os níveis de risco, produzir campanhas de phishing alinhadas ao comportamento do usuário, registrar indicadores de exposição e correlacionar vulnerabilidades comportamentais com incidentes reais. Ou seja, **a plataforma de ensino deve obrigatoriamente pertencer ao mesmo ecossistema do EPP**, pois precisa acessar a mesma base de dados, console de gestão, indicadores de risco e relatórios integrados.

3.4.5. Quando firewall, EPP/EDR e plataforma de conscientização operam sob um único fornecedor ou integrador, obtêm-se benefícios essenciais:

- a) compatibilidade plena entre as camadas de segurança;
- b) visibilidade unificada em console único;
- c) aplicação coerente de políticas institucionais;
- d) respostas automatizadas e coordenadas (ex.: isolar dispositivo, bloquear tráfego, elevar nível de risco do usuário);
- e) suporte técnico único, padronizado e com menor tempo de resposta; eliminação de conflitos entre versões, motores de detecção e agentes; redução de custos indiretos relacionados a múltiplas integrações, contratos e equipes.

3.4.6. A fragmentação em lotes distintos, portanto, acarretaria não só riscos técnicos, mas também risco de não conformidade com diretrizes de segurança adotadas mundialmente, além de elevar custos administrativos e operacionais. A segurança moderna exige abordagem integrada end-to-end, e não a soma de soluções isoladas.

3.4.7. Assim, a contratação em lote único não apenas é justificada tecnicamente, como é condição essencial para garantir a efetividade, coerência, correlação inteligente, tempo de resposta reduzido e a continuidade da política de segurança da informação do **SENAR-AR/MS**, preservando a integridade, a confidencialidade e a disponibilidade das informações institucionais.

3.5. Nos preços propostos deverão estar inclusos todos os custos diretos e indiretos para a perfeita execução do objeto, encargos da legislação social, trabalhista, previdenciária e responsabilidade civil, por quaisquer danos causados a terceiro ou dispêndios resultantes de taxas, regulamentos e impostos municipais, estaduais e federais, enfim, tudo o que for necessário para execução total e completa do objeto, sem que lhe caiba, em qualquer caso, direto regressivo em relação ao **SENAR-AR/MS** nem qualquer outro pagamento adicional.

4. DA FORMA DE EXECUÇÃO DO OBJETO

4.1. A execução do objeto, após assinatura do contrato e início de sua vigência, ocorrerá em conformidade com as características e quantidades indicadas neste instrumento, atendendo as necessidades do **SENAR-AR/MS**.

4.2. Os serviços serão executados em até 30 (trinta) dias corridos, na sede da Administração do **SENAR-AR/MS**, localizada na Rua Marcino dos Santos, n.º 401, Bairro Chácara Cachoeira II, Campo Grande/MS, CEP: 79040-902, de segunda a sexta-feira, das 08h às 12h e das 13h às 17h.

4.3. O objeto entregue e recebido será considerado definitivamente aceito na forma e/ou condições acordadas neste instrumento após 03 (três) dias úteis, acaso não recusado.

4.3.1. Transcorrido o prazo supra, não caberá ao **SENAR-AR/MS** quaisquer questionamentos por falta de conferência quando do recebimento do objeto.

4.4. A instalação, configuração, integração e ativação da plataforma de segurança, incluindo os appliances NGFW, do software de proteção de endpoints (EPP), das licenças de Acesso Seguro Zero Trust, da plataforma de conscientização, bem como a realização dos treinamentos técnicos e operacionais, deverão ser executadas em conjunto com as equipes técnicas do **SENAR-AR/MS**, garantindo a plena transferência de conhecimento e a validação do ambiente de produção.

4.5. As atividades presenciais relacionadas à instalação, configuração, customização e treinamentos deverão ser realizadas, preferencialmente, em horário comercial (08h às 17h, de segunda a sexta-feira), ressalvadas situações excepcionais que demandem atuação fora desse período, desde que previamente acordadas com o fiscal do contrato.

4.6. CONDIÇÕES DA PRESTAÇÃO DO SERVIÇO

4.6.1. A **CONTRATADA** deverá disponibilizar todos os recursos necessários à implantação da solução de segurança da informação, abrangendo o fornecimento de appliances de firewall de próxima geração (NGFW), licenciamento de software de proteção de endpoints (EPP), licenciamento de Acesso Seguro Zero Trust, plataforma de conscientização em segurança, serviços de instalação, configuração, integração, customização, treinamento e suporte técnico especializado, de forma a assegurar a plena operacionalização da solução no ambiente tecnológico do **SENAR-AR/MS**.

4.6.2. O fornecimento das licenças de uso das soluções deverá ser realizado em sua versão mais atual, contemplando todas as atualizações, correções de segurança e melhorias tecnológicas disponibilizadas pelos fabricantes, sem ônus adicional ao **SENAR-AR/MS**, durante toda a vigência contratual.

4.6.3. A **CONTRATADA** deverá disponibilizar acesso à base de conhecimento técnico do fabricante, incluindo documentação oficial, manuais, guias de instalação, relatórios técnicos, downloads de atualizações e patches de segurança. A documentação poderá ser entregue em meio eletrônico, devendo estar redigida em português ou inglês, garantindo clareza e acessibilidade para a equipe técnica responsável pela fiscalização contratual.

4.6.4. Os serviços de suporte técnico especializado (remoto e on-site) deverão ser prestados em regime 24x7x365, por meio de múltiplos canais (telefone, e-mail e plataforma web), em conformidade com os Acordos de Nível de Serviço (SLA) definidos neste instrumento. O atendimento remoto e presencial, sempre que necessário ao pleno funcionamento da solução. Esse suporte incluirá manutenção preventiva, corretiva e adaptativa, de forma a assegurar a continuidade da operação e a disponibilidade permanente dos serviços contratados.

4.6.4.1. O atendimento presencial deverá ser realizado sempre que as intervenções remotas se mostrarem insuficientes ou inadequadas para a resolução da demanda, garantindo a continuidade operacional e a adequada prestação dos serviços. Os serviços de suporte técnico presenciais deverão ser realizados na sede administrativa do **SENAR-AR/MS**, no **CEBC** ou em outro endereço indicado pelo **SENAR-AR/MS**.

4.6.5. Todo o suporte técnico deverá ser executado por profissionais qualificados e certificados pelos fabricantes das soluções, integrantes do quadro funcional da **CONTRATADA**, sendo indispensável a apresentação de documentação comprobatória atualizada da certificação e do vínculo empregatício. A substituição de técnicos credenciados somente poderá ocorrer mediante apresentação prévia de documentação comprobatória equivalente, devendo a **CONTRATADA** comunicar formalmente ao **SENAR-AR/MS** a alteração, acompanhada de cronograma atualizado de atendimentos programados.

4.6.6. Durante toda a vigência contratual, a **CONTRATADA** deverá manter a solução em operação contínua, segura e atualizada, garantindo a substituição, sem custo adicional ao **SENAR-AR/MS**, de qualquer componente (software, licença ou módulo) que apresente falhas, incompatibilidades ou se torne obsoleto, de forma a não comprometer a proteção da rede corporativa do **SENAR-AR/MS**, suas estações de trabalho, servidores e dispositivos móveis.

4.7. DA IMPLEMENTAÇÃO DA SOLUÇÃO

4.7.1. Para a correta implantação da solução contratada, deverá ser fornecido um Serviço Especializado de Instalação, Configuração e Customização, compreendendo todas as etapas necessárias à plena operacionalização dos appliances NGFW, do software de proteção de endpoints (EPP), das licenças de Acesso Seguro Zero Trust, da plataforma de conscientização.

4.7.2. Entende-se por serviço especializado de instalação, configuração e customização a parametrização lógica e física da solução, em conformidade com o ambiente tecnológico do **SENAR-AR/MS**, abrangendo:

4.7.2.1. A integração da solução à rede corporativa existente;

4.7.2.2. A definição de políticas de segurança, perfis de usuários e fluxos de resposta a incidentes;

4.7.2.3. A adequação da plataforma às necessidades específicas do **SENAR-AR/MS**, contemplando regras de acesso, relatórios de conformidade e procedimentos de auditoria;

4.7.2.4. A implementação de mecanismos de redundância e alta disponibilidade, quando aplicável.

4.7.2.5. Esse serviço, correspondente ao Projeto Executivo, tem como objetivo a configuração personalizada da solução, com base nas características previamente definidas pelo **SENAR-AR/MS**. Compete à **CONTRATADA** a responsabilidade pelo planejamento, execução e documentação de todas as etapas de instalação e customização, observando-se as melhores

práticas de mercado, a legislação aplicável (notadamente a LGPD) e os requisitos estabelecidos pelo RLC do SENAR.

4.7.3. Para a execução do serviço especializado de implementação, a **CONTRATADA** deverá entregar ao **SENAR-AR/MS**, para análise e validação, um **Plano de Implementação da Solução**, contemplando, no mínimo:

4.7.3.1. Descrição das etapas de instalação, parametrização e integração da solução de EPP, NGFW, Acesso Seguro Zero Trust e plataforma de conscientização;

4.7.3.2. Cronograma detalhado de execução, com prazos e marcos de entrega;

4.7.3.3. Procedimentos de testes de segurança, desempenho e validação funcional em ambiente de produção controlado;

4.7.3.4. Plano de contingência e reversão em caso de falhas na implementação;

4.7.3.5. Especificação de perfis de usuários, regras de segurança, fluxos de resposta a incidentes e relatórios de acompanhamento.

4.8. MODELO DE DOCUMENTAÇÃO TÉCNICA A SER ENTREGUE AO FINAL DE CADA ETAPA

4.8.1. O Projeto Executivo deverá consolidar o detalhamento da arquitetura implantada, a documentação das parametrizações realizadas, os resultados dos testes efetuados e os procedimentos de integração, migração e entrega definitiva da solução ao ambiente tecnológico do **SENAR-AR/MS**.

4.8.2. O cumprimento das obrigações de instalação, configuração e customização será acompanhado e fiscalizado pelo fiscal do contrato designados pelo **SENAR-AR/MS**, devendo a **CONTRATADA** atender integralmente às determinações quanto à conformidade da solução implementada.

4.9. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL DA EQUIPE

4.9.1. A **CONTRATADA** deverá prover suporte técnico especializado para a solução ofertada através de equipe técnica especializada e devidamente capacitada;

4.9.2. A equipe deverá ser composta por profissionais com as seguintes especialidades:

4.9.2.1. No mínimo **02 (dois) profissionais**, devidamente qualificados, 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 <i>Administrator</i> , <i>Professional</i> 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).
---	--

4.9.2.2. No mínimo, **02 (dois) profissionais**, devidamente qualificados, contemplando 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 técnico ou manutenção nas soluções do fabricante da solução de proteção e segurança para endpoints	- Certificado de conclusão de capacitação fornecido pelo fabricante da solução de proteção e segurança para endpoints, com o nível de certificação <i>Administrator</i> , <i>Professional</i> 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).

4.9.2.3. No mínimo **01 (um) profissional**, devidamente qualificado, 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 NOC.	- 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).

4.9.2.4. No mínimo **01 (um) profissional**, devidamente qualificado, 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 (v3 ou superior) e Certificação ISO/IEC 20000.	- Certificado de conclusão ITIL (v3 ou superior), fornecido por instituto credenciado, dentro do período de validade; - 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).

4.9.2.5. Na assinatura do contrato deverá ser apresentada a comprovação de que os profissionais fazem parte do quadro funcional da **CONTRATADA**.

4.9.2.5.1. A comprovação dar-se-á mediante um dos seguintes documentos:

- a) Contrato Social, no caso de sócio proprietário.
- b) Carteira de Trabalho e Previdência Social (CTPS);
- c) Contrato de Prestação de Serviços, no caso de profissional autônomo.

4.10. DAS CONDIÇÕES DE EXECUÇÃO DO SERVIÇO E METODOLOGIA DE TRABALHO

4.10.1. A **CONTRATADA** deverá designar profissionais com formação e experiência compatíveis com as atividades a serem desempenhadas, em conformidade com a complexidade e o volume de serviços exigidos pela presente contratação, assegurando a observância das qualificações técnicas necessárias ao bom desempenho das funções.

4.10.2. Todas as atividades deverão ser executadas em conformidade com o ambiente tecnológico do **SENAR-AR/MS**, observando-se a compatibilidade de perfis profissionais, os requisitos de segurança da informação e as metodologias de trabalho previamente acordadas com a área técnica do **SENAR-AR/MS**.

4.10.3. Os serviços poderão ser realizados de forma remota ou, quando necessário, presencialmente nas dependências do **SENAR-AR/MS**, cabendo à **CONTRATADA** garantir todos os meios necessários para a plena execução das atividades, sob acompanhamento do Fiscal do Contrato, designados na forma do RLC do SENAR.

4.10.4. Quando houver necessidade de execução dos serviços no ambiente físico do **SENAR-AR/MS**, os profissionais da **CONTRATADA** deverão cumprir os procedimentos internos estabelecidos pela instituição, sendo a assiduidade e a execução supervisionadas pela Administração e registradas pela própria **CONTRATADA**.

4.10.5. É vedado à **CONTRATADA** subcontratar, subempreitar, ceder ou transferir, total ou parcialmente, o objeto desta contratação, ressalvadas as hipóteses expressamente autorizadas pelo **SENAR-AR/MS**, em conformidade com o disposto no RLC-SENAR.

4.10.6. A **CONTRATADA** será integralmente responsável pela instalação, configuração, customização e ativação da solução contratada, assegurando sua plena operacionalização no ambiente tecnológico do **SENAR-AR/MS**.

4.10.7. Todos os recursos, ferramentas, licenças, appliances e serviços necessários à implementação e ao funcionamento da solução correrão por conta da **CONTRATADA**, devendo ser fornecidos sem qualquer ônus adicional ao **SENAR-AR/MS** além do valor global contratado.

4.10.8. A **CONTRATADA** deverá garantir que a instalação, integração e parametrização da solução observem as boas práticas de governança de TIC, os requisitos de segurança da informação e cibersegurança e os padrões técnicos previamente validados pela equipe técnica do **SENAR-AR/MS**, em conformidade com a LGPD (Lei nº 13.709/2018) e com os normativos internos aplicáveis.

4.11. CONDIÇÕES DE GARANTIA E SUPORTE TÉCNICO:

4.11.1. A presente contratação exige a implementação de condições rigorosas de garantia de funcionamento e suporte técnico especializado, fundamentadas na necessidade de manter a solução de segurança da informação em operação contínua, estável e segura durante toda a vigência do contrato.

4.11.2. A **CONTRATADA** é responsável pela entrega integral do objeto, pela manutenção da qualidade e pelo atendimento contínuo às condições pactuadas, bem como na Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), que estabelece a obrigatoriedade de adoção de medidas técnicas e administrativas adequadas à proteção de dados pessoais e sensíveis sob custódia da instituição.

4.12. Justificativa da necessidade de suporte especializado

4.12.1. A solução contratada compreende o fornecimento de appliances de firewall de próxima geração (NGFW), licenciamento de software de Proteção de Endpoints (EPP), licenciamento de Acesso Seguro Zero Trust e plataforma de conscientização em segurança da informação. Tais recursos são destinados a proteger a rede corporativa, servidores, estações de trabalho e dispositivos móveis do **SENAR-AR/MS**, que compõem a base tecnológica de apoio às suas atividades educacionais e administrativas.

4.12.2. A interrupção, falha ou mau funcionamento dessa solução pode gerar impactos críticos, tais como:

4.12.2.1. Indisponibilidade de sistemas e plataformas essenciais ao funcionamento institucional;

4.12.2.2. Vazamento, perda ou acesso indevido a dados sensíveis de alunos, instrutores e colaboradores, em afronta à lgpd;

4.12.2.3. Riscos de ataques cibernéticos em larga escala, comprometendo a continuidade das atividades de capacitação e gestão do **SENAR-AR/MS**;

4.12.2.4. Prejuízos financeiros, contratuais e reputacionais à entidade.

4.12.3. Diante da criticidade, mostra-se imprescindível que os serviços de suporte técnico não se restrinjam ao horário comercial. A **CONTRATADA** deverá garantir atendimento ininterrupto, em regime 24 horas por dia, 7 dias por semana (24x7x365), por múltiplos canais (plataforma web, telefone e e-mail), assegurando agilidade e efetividade na resposta a incidentes ou falhas.

4.12.3.1. Na assinatura do contrato a **CONTRATADA** que possua sede fora do município de Campo Grande/MS deverá apresentar declaração formal de compromisso, na qual se comprometa a estabelecer equipe de suporte técnico dedicada e permanentemente disponível na localidade indicada pelo **SENAR-AR/MS**, no prazo máximo de 15 (quinze) dias. Tal equipe deverá estar plenamente apta a atender, de forma tempestiva e satisfatória, às condições operacionais e aos Acordos de Nível de Serviço (SLA) definidos neste instrumento.

4.12.4. Além disso, caberá à **CONTRATADA** assegurar que todo o suporte técnico seja executado por profissionais qualificados e certificados pelos fabricantes das soluções fornecidas, garantindo que os atendimentos realizados, sejam remotos ou presenciais, observem as melhores práticas internacionais de cibersegurança e a conformidade regulatória aplicável.

4.12.5. Durante toda a vigência contratual, o suporte técnico especializado deverá compreender, no mínimo:

4.12.5.1. Abertura, acompanhamento e tratamento de chamados em regime ininterrupto (24x7x365), por múltiplos canais (plataforma de suporte técnico via web, telefone e e-mail), assegurando agilidade e rastreabilidade no atendimento;

4.12.5.2. Atendimento remoto imediato, com escalonamento para suporte presencial sempre que a complexidade ou criticidade da ocorrência demandar intervenção local;

4.12.5.2. Execução de correções, parametrizações e ajustes de configuração, garantindo a manutenção plena da operação da solução e a recuperação da normalidade em prazos compatíveis com os Acordos de Nível de Serviço (SLA);

4.12.5.3. Disponibilização, orientação e aplicação de atualizações de software (major, minor, patches, fixes, releases e versões corretivas), sem ônus adicional ao **SENAR-AR/MS**, assegurando que todos os componentes permaneçam atualizados frente às ameaças emergentes;

4.12.5.4. Suporte proativo, incluindo análise preventiva de vulnerabilidades, recomendações técnicas de mitigação de riscos e orientações de melhoria contínua para fortalecimento da segurança da rede corporativa, servidores, estações de trabalho e dispositivos móveis;

4.12.5.5. Manutenção da solução em conformidade com as melhores práticas de governança de TIC e segurança cibernética, observando padrões internacionais (ISO/IEC 27001, NIST

Cybersecurity Framework, OWASP) e os requisitos legais aplicáveis, notadamente a LGPD (Lei nº 13.709/2018).

4.12.6. Compete à **CONTRATADA** assegurar a operação estável, contínua e segura da solução contratada, devendo:

4.12.6.1. Disponibilizar equipe técnica qualificada e certificada para execução dos serviços de suporte, devidamente vinculada ao quadro funcional da empresa;

4.12.6.2. Realizar atendimentos presenciais, quando necessário, nas dependências indicadas pelo **SENAR-AR/MS**, observando os prazos estabelecidos nos Acordos de Nível de Serviço (SLA);

4.12.6.2. Observar integralmente os procedimentos internos, políticas institucionais e normas de segurança da informação definidos pelo **SENAR-AR/MS**, bem como aqueles que vierem a ser instituídos durante a vigência contratual;

4.12.6.3. Fornecer, sempre que solicitado, documentação técnica atualizada, incluindo manuais, guias de operação, procedimentos de troubleshooting e materiais de capacitação, preferencialmente em meio digital e em idioma português (Brasil);

4.12.6.4. Assumir, às suas expensas, todas as medidas necessárias para assegurar a plena operacionalidade da solução durante o contrato, incluindo substituição de componentes, atualização de software, correção de falhas e manutenção contínua.

4.13. SUPORTE TÉCNICO DO FABRICANTE

4.13.1. Além do suporte da **CONTRATADA**, a solução deverá contar com suporte técnico direto do fabricante, a ser acionado sempre que necessário, com as seguintes características mínimas:

4.13.1.1. Sistema de abertura e acompanhamento de chamados em regime 24x7, com registro e rastreabilidade;

4.13.1.2. Atendimento telefônico em português no mínimo em regime 8x5, com escalonamento para 24x7 em situações críticas, assegurando comunicação efetiva com os técnicos do **SENAR-AR/MS**;

4.13.1.3. Acesso integral à base de conhecimento, repositórios técnicos e documentação oficial do fabricante, sem restrições de consulta ou download;

4.13.1.4. Direito a todas as atualizações de software disponibilizadas pelo fabricante durante a vigência contratual (major, minor, patches e correções de segurança), sem custos adicionais ao **SENAR-AR/MS**.

4.14. MONITORAMENTO, SLA E ACOMPANHAMENTO

4.14.1. A **CONTRATADA** deverá observar prazos de atendimento e resolução proporcionais à criticidade dos incidentes, mediante escalonamento definido em Acordo de Nível de Serviço

(SLA) a ser aprovado pelo **SENAR-AR/MS**, garantindo prioridade absoluta para incidentes de alta gravidade.

4.14.2. O cumprimento dessas obrigações será acompanhado e fiscalizado pelo Fiscal Titular e/ou substituto do Contrato designados pelo **SENAR-AR/MS**. Compete-lhes atestar a conformidade da execução contratual e adotar as medidas administrativas previstas no regulamento em caso de descumprimento.

4.15. NÚCLEO DE OPERAÇÕES E CONTROLE (NOC)

4.15.1. A **CONTRATADA** deverá manter estrutura de Núcleo de Operações e Controle (NOC) dedicada ao monitoramento preventivo e corretivo da solução contratada, garantindo o diagnóstico de falhas, a tomada de decisões de intervenção e a prestação de assistência técnica contínua, a fim de assegurar a disponibilidade operacional e a segurança da informação.

4.15.2. O NOC deverá operar em regime mínimo de 8x5 (oito horas por dia, cinco dias por semana), com escalonamento obrigatório para regime 24x7 em situações críticas, durante toda a vigência contratual.

4.15.3. A estrutura deverá contar com, no mínimo, um profissional de cada perfil descrito no subitem “4.9. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL DA EQUIPE”, alocados remotamente, devidamente certificados nas soluções ofertadas, responsáveis pelo pronto atendimento às solicitações de suporte de primeiro e segundo nível, originadas do ambiente monitorado e/ou dos usuários técnicos do **SENAR-AR/MS**.

4.15.4. Compete à **CONTRATADA**:

4.17.4.1. Implantar, monitorar e administrar os serviços de monitoração da solução implementada;

4.15.4.2. Assegurar a coleta e análise de dados, a configuração de alertas e a emissão de relatórios periódicos de status e incidentes;

4.15.4.3. Disponibilizar dashboards e ferramentas de visualização que permitam acompanhamento em tempo real do desempenho da solução e dos indicadores de segurança; Prover todos os recursos, ferramentas e insumos necessários à manutenção do núcleo, sem ônus adicional ao **SENAR-AR/MS**.

4.15.4.4. A exigência de instalação e manutenção do NOC fundamenta-se na criticidade da solução contratada, que envolve a proteção de dados sensíveis, estratégicos e de alto valor para o **SENAR-AR/MS**, e na necessidade de resposta tempestiva a incidentes que possam comprometer a continuidade de suas atividades educacionais, administrativas e de capacitação rural.

4.15.4.5. O modelo de NOC está incluído no escopo do serviço de suporte técnico especializado, devendo seus custos estarem integralmente previstos na proposta financeira da licitante vencedora.

4.15.5. A **CONTRATADA** deverá elaborar e entregar **relatórios mensais** contendo, no mínimo: Registro de incidentes e falhas ocorridas, com classificação por criticidade e respectiva solução adotada;

4.15.5.1. Indicadores de desempenho e disponibilidade da solução monitorada;

4.15.5.2. Medidas preventivas implementadas e recomendações para mitigação de riscos;

4.15.5.3. Histórico consolidado de chamados e tempos de resposta/resolução;

4.15.5.4. Conformidade com os Acordos de Nível de Serviço (SLA) pactuados;

4.15.5.5. O cumprimento dessas obrigações será acompanhado pelo Fiscal Titular e/ou substituto do Contrato, designados pelo **SENAR-AR/MS**, cabendo à Administração adotar as medidas previstas em caso de descumprimento contratual.

4.16. ACORDOS DE NÍVEL DE SERVIÇO (SLA) SOBRE O ITEM 1

4.16.1. A execução dos serviços de Suporte Técnico Especializado, Manutenção e Apoio deverá observar os Acordos de Nível de Serviço (SLA) estabelecidos neste instrumento, que constituem cláusulas essenciais do contrato.

4.16.1.1. O SLA representa o instrumento pelo qual se definem os prazos, as condições de atendimento e os parâmetros mínimos de qualidade da prestação dos serviços, permitindo aferir objetivamente o desempenho da **CONTRATADA** e assegurar a conformidade com as exigências institucionais.

4.16.2. A adoção de SLA justifica-se pela alta criticidade da solução contratada, que abrange o fornecimento de appliances de firewall de próxima geração (NGFW).

4.16.2.1. Esses componentes formam a camada essencial de proteção da infraestrutura tecnológica do **SENAR-AR/MS**, incluindo sua rede corporativa, estações de trabalho, servidores de arquivos e dispositivos móveis, que dão suporte direto às atividades educacionais, administrativas e de capacitação rural desempenhadas pela instituição.

4.16.3. A indisponibilidade ou mau funcionamento da solução pode acarretar consequências graves, tais como:

4.16.3.1. Interrupção das atividades finalísticas do **SENAR-AR/MS**, com impacto direto nos programas de capacitação rural e na execução de sua missão institucional;

4.16.3.2. Exposição a ataques cibernéticos sofisticados, com risco de comprometimento da integridade e da disponibilidade de dados sensíveis;

4.16.3.3. Vazamento ou perda de informações estratégicas e pessoais, em afronta à Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) e aos princípios de confidencialidade e responsabilidade institucional;

4.16.3.4. Prejuízos financeiros e reputacionais, decorrentes de indisponibilidade dos serviços, da necessidade de remediação emergencial ou de eventual responsabilização civil por falhas de proteção da informação.

4.16.4. Diante desse cenário, mostra-se imprescindível que a **CONTRATADA** assegure suporte técnico em regime contínuo (24x7x365) para incidentes críticos, bem como prazos de resposta e de resolução proporcionais à gravidade das ocorrências, de forma a mitigar riscos e garantir a rápida recuperação da normalidade operacional.

4.16.5. O atendimento deverá ocorrer por múltiplos canais (plataforma web, telefone e e-mail), todos com registro, rastreabilidade e protocolo eletrônico de cada chamado, permitindo ao **SENAR-AR/MS** acompanhar a execução e avaliar a conformidade do serviço prestado.

4.16.6. Além do atendimento a incidentes, o SLA deverá abranger:

4.16.6.1. Atualizações de software e patches de segurança, sempre incluídos no contrato e sem ônus adicional à instituição;

4.16.6.2. Execução de manutenções preventivas, corretivas e adaptativas, com comunicação prévia e mínima indisponibilidade;

4.16.6.3. Emissão de relatórios periódicos de desempenho, contendo indicadores de disponibilidade, tempos médios de resposta e de resolução, incidentes registrados, medidas preventivas implementadas e recomendações técnicas;

4.16.6.4. Auditoria contratual, possibilitando ao **SENAR-AR/MS** verificar o cumprimento dos soóparâmetros acordados e adotar medidas corretivas quando necessário.

4.16.7. A obrigatoriedade de SLA nesta contratação ancora-se nos princípios da eficiência, economicidade, continuidade e segurança institucional, previstos no RLC-SENAR, assegurando, não apenas previsibilidade na prestação dos serviços, mas também estabelecendo mecanismos de responsabilização e penalização em caso de descumprimento, criando garantias objetivas de desempenho e confiabilidade da solução de segurança cibernética.

4.16.8. Em síntese, os Acordos de Nível de Serviço a serem pactuados constituem um instrumento indispensável de governança e fiscalização, assegurando que a contratação de segurança cibernética do **SENAR-AR/MS** resulte na efetiva proteção de seus ativos digitais, no fortalecimento de sua resiliência organizacional e na plena conformidade com a LGPD e com os normativos internos aplicáveis.

4.17. CONDIÇÕES GERAIS

4.17.1. Todas as atividades de suporte e manutenção deverão ser prestadas por profissionais devidamente qualificados e certificados nas tecnologias contratadas, garantindo não apenas a correta execução das atividades, mas também a aderência às melhores práticas internacionais de segurança cibernética (ISO/IEC 27001, NIST Cybersecurity Framework, OWASP Top 10).

4.17.2. Qualquer intervenção que implique interrupção da solução, ainda que parcial, deverá ser previamente acordada com o **SENAR-AR/MS** e executada preferencialmente fora do horário regular de expediente, incluindo finais de semana ou períodos de menor utilização, de modo a evitar impactos às atividades administrativas e educacionais da entidade. Essas atividades não poderão gerar custos adicionais ao **SENAR-AR/MS**.

4.17.3. É vedada a desativação ou suspensão de softwares, serviços digitais ou componentes críticos da solução sem prévia anuência formal do **SENAR-AR/MS**. Toda alteração que envolva descontinuidade, substituição de módulos ou retirada de funcionalidades deverá estar documentada e formalmente autorizada pelo **SENAR-AR/MS**.

4.17.4. O não cumprimento dos SLA acarretará a aplicação de glosas financeiras proporcionais à gravidade e à recorrência do descumprimento, multas percentuais progressivas e, nos casos de inexecução parcial ou total, sanções administrativas.

4.17.5. A solução deverá manter disponibilidade global mínima de 99% ao mês, excluídos apenas períodos de manutenção programada previamente autorizados pelo **SENAR-AR/MS**. A aferição dessa disponibilidade será feita por meio de relatórios técnicos e sistemas de monitoramento, constituindo critério objetivo de aferição contratual.

4.18. RELATÓRIOS DE ATIVIDADES TÉCNICAS

4.18.1. Mensalmente, a **CONTRATADA** deverá entregar ao **SENAR-AR/MS** um Relatório de Atividades Técnicas, contendo, no mínimo:

4.18.1.1. Identificação e classificação de cada chamado (urgente, alto impacto, médio, baixo);

4.18.1.2. Data/hora de abertura, encaminhamento e conclusão de cada atendimento;

4.18.1.3. Descrição da ocorrência, impacto identificado e ambiente afetado;

4.18.1.4. Procedimentos técnicos adotados, tempo de resposta e de solução;

4.18.1.5. Cumprimento ou descumprimento dos SLA, com justificativas formais e evidências técnicas sempre que aplicável.

4.18.1.6. Registro das manutenções preventivas realizadas e recomendações de melhorias.

4.18.2. Além do relatório mensal, o **SENAR-AR/MS** poderá solicitar relatórios adicionais a qualquer tempo, em formato digital, analítico ou sintético, destinados a auditoria, fiscalização e acompanhamento estratégico da execução contratual.

4.18.3. Relatórios consolidados deverão incluir análise preditiva e de tendências, permitindo identificar recorrência de falhas, riscos emergentes e oportunidades de melhoria na segurança do ambiente corporativo.

4.19. ATUALIZAÇÕES E EVOLUÇÃO TECNOLÓGICA

4.19.1. Durante toda a vigência do contrato, deverão estar disponíveis ao **SENAR-AR/MS**, sem custo adicional, todas as atualizações e versões da solução (major, minor, patches, fixes e releases) disponibilizadas pelo fabricante.

4.19.2. Tais atualizações deverão abranger não apenas correções de vulnerabilidades e falhas, mas também:

4.19.2.1. Melhorias de desempenho;

4.19.2.2. Novos recursos e funcionalidades;

4.19.2.3. Ajustes de conformidade com a LGPD (lei nº 13.709/2018) e demais normas aplicáveis;

4.19.2.3. Alinhamento às tendências de mercado e às práticas de segurança em constante evolução.

4.19.3. A **CONTRATADA** deverá documentar cada atualização aplicada, informando impactos, testes realizados, data de implementação e eventuais ajustes de configuração, de modo a assegurar rastreabilidade e auditoria completa.

4.20. ACORDOS DE NÍVEIS DE SERVIÇO (SLA) E PENALIDADES

4.20.2. Os chamados técnicos deverão observar os seguintes prazos de resposta e solução:

Nível / Indicador	Nível de Severidade	Descrição da ocorrência	Prazo máx. de resposta	Prazo máx. de solução	Penalidade de SLA por descumprimento
N01	Manutenção Preventiva	Atividades programadas para verificação da solução, aplicação de atualizações e melhorias, previamente agendadas com o SENAR-AR/MS	Na data agendada	Dentro da janela acordada	0,1% de decréscimo no valor total da Nota Fiscal para o mês de referência para cada unidade percentual abaixo do SLA Aceitável.
N02	Urgente – alto impacto	Indisponibilidade total ou parcial da solução que comprometa serviços críticos ou paralise atividades essenciais do SENAR-AR/MS	Até 2 horas	Até 6 horas	0,5% de decréscimo no valor total da Nota Fiscal para cada unidade percentual abaixo do SLA Aceitável.
N03	Alto impacto	Indisponibilidade parcial ou degradação grave de desempenho, sem paralisação total, que prejudique de forma relevante a operação	Até 4 horas	Até 12 horas	0,5% de decréscimo no valor total da Nota Fiscal para cada unidade percentual abaixo do SLA Aceitável.
N04	Médio impacto	Erros recorrentes ou problemas relevantes que impactem a operação, com possibilidade de contorno ou alternativa de	Até 8 horas	Até 24 horas	0,1% de decréscimo no valor total da Nota Fiscal para o mês de referência para cada unidade percentual abaixo do SLA Aceitável

		execução			
N05	Baixo impacto	Ocorrências eventuais que não afetem a continuidade dos serviços, como falhas isoladas de usuário ou ajustes simples	Até 24 horas	Até 48 horas	Notificação formal à contratada. A reincidência ou de recorrência de descumprimentos poderá ensejar a reclassificação da ocorrência para níveis de maior severidade, sujeitando-se às penalidades previstas.

4.20.3. EXEMPLO DE APLICAÇÃO DA PENALIDADE

4.20.3.1. Exemplo de Cálculo de Penalidade – Nível N02

Cenário:

- I. Prazo máximo de solução (SLA): 6 horas
- II. Tempo real de solução: 8 horas
- III. Tempo excedido: 2 horas

Calcular o percentual de descumprimento = $2/6 \times 100 = 33,33\%$

4.20.4. APLICAÇÃO DA PENALIDADE

Regra: 0,5% de decréscimo no valor da Nota Fiscal para cada 1% abaixo do SLA

$33,33 \times 0,5\% = 16,67\%$ sobre o valor da Nota Fiscal

4.21. FISCALIZAÇÃO E SANÇÕES

4.21.1. O cumprimento das obrigações de SLA será acompanhado pelo Fiscal do Contrato designados pelo **SENAR-AR/MS**.

4.21.2. Compete à fiscalização contratual:

4.21.2.1. Monitorar continuamente os indicadores de desempenho definidos;

4.21.2.2. Aplicar glosas financeiras e multas progressivas conforme tabela estabelecida;

4.21.2.3. Considerar como inexecução parcial o não atendimento reiterado das condições estabelecidas;

4.21.2.4. Caracterizar como inexecução total o descumprimento continuado que comprometa a execução integral do objeto;

4.21.2.5. Adotar providências administrativas adicionais, inclusive rescisão contratual, sem prejuízo das demais sanções previstas no regulamento.

4.22. O **SENAR-AR/MS** poderá recusar o serviço prestado de forma insatisfatória, ou que apresente defeitos ou até mesmo seja considerado imprestável, devendo a **CONTRATADA** promover a correção às suas expensas, bem como, poderá cancelar o Contrato ou documento equivalente, no todo ou em parte, de acordo com sua conveniência.

4.23. A aprovação do objeto pela inspeção ou a sua dispensa, não diminui e nem altera a plena e total garantia e não exclui a responsabilidade civil da **CONTRATADA** por vícios de quantidade ou qualidade na execução do objeto, bem como no material empregado ou disparidade com as especificações técnicas exigidas neste instrumento ou atribuídas a **CONTRATADA**, cabendo-lhe sanar quaisquer irregularidades verificadas durante sua utilização, garantindo-se ao **SENAR-AR/MS** as faculdades previstas no artigo 18, da Lei nº 8.078/90 (Código de Defesa do Consumidor – CDC).

4.24. Serão garantidas ao **SENAR-AR/MS** todas as garantias legais relacionadas à prestação dos serviços sem prejuízo àquelas fornecidas pelos fabricantes quanto a eventuais defeitos e vícios dos equipamentos.

4.25. Na execução do objeto deverão ser observadas, de modo geral, as Especificações, Posturas, Normas Técnicas, Leis e Regulamentos vigentes em todo o território nacional, bem como será necessário possuir e/ou observar, independente de exigência expressa neste instrumento ou seus anexos, as licenças, alvarás e/ou certificados necessários à fabricação, comercialização, distribuição, fornecimento e/ou prestação de serviços relacionados a qualquer dos materiais envolvidos na execução do objeto contratado, incluindo, mas não se limitando, as expedidas pelos órgãos fiscalizadores, agências de regulação, institutos de metrologia, órgãos de controle ambiental.

5. DO PRAZO DE VIGÊNCIA E DO PAGAMENTO

5.1. O presente instrumento vigorará pelo período de 12 (doze) meses, contados a partir da data de xx de xxxxxx de 202x, podendo ser prorrogado até o limite de 10 (dez) anos, nos termos do art. 33 do RLC do SENAR, desde que verificadas as hipóteses de conveniência e oportunidade por parte do **SENAR-AR/MS** cumuladas ao interesse da **CONTRATADA**.

5.2. O pagamento, decorrente da execução do objeto será efetuado mensalmente, por meio de crédito em conta bancária de natureza jurídica após a apresentação da nota fiscal e recebimento do objeto, em até 25 (vinte e cinco) dias, respeitando o Cronograma de Pagamentos do **SENAR-AR/MS**, onde:

a) Os pagamentos serão efetuados nos dias 15 e 30 de cada mês, mediante crédito em conta bancária de sua titularidade, sendo programados para o primeiro dia útil subsequente caso recaiam sobre feriado, final de semana ou data em que não haja expediente no **SENAR-AR/MS**.

b) As notas fiscais recebidas e aceitas entre os dias 21 e o dia 05 do mês seguinte terão seus pagamentos executados no dia 15 mais próximo.

c) As notas fiscais recebidas e aceitas entre os dias 06 e 20 de cada mês terão seus pagamentos executados no dia 30 mais próximo.

5.2.1. A liquidação financeira ficará condicionada à entrega e aceitação do objeto, bem como o envio da respectiva nota fiscal para o e-mail notafiscal@senarms.org.br.

5.2.2. Os documentos fiscais encaminhados em data que não houver expediente no **SENAR-AR/MS**, serão considerados como recebidos no primeiro dia útil subsequente.

5.2.3. As notas fiscais deverão ser encaminhadas para o e-mail notafiscal@senarms.org.br no ato de sua emissão, a fim de evitar transtornos caso seja necessário o seu cancelamento.

5.2.4. Não produzirão efeitos, notas fiscais endereçadas a e-mail que não seja aquele previsto no **subitem 5.2.3**, nem documentos fiscais cujo envio não tenha sido autorizado pelo **SENAR-AR/MS**.

5.3. A nota fiscal, para liquidação e pagamento da despesa deverá estar obrigatoriamente atestada pelo **SENAR-AR/MS**, acompanhada do relatório dos serviços executados no período faturado, de acordo com o item 4.18, ficando a **CONTRATADA** obrigada a comprovar a regularidade fiscal para com a Fazenda Federal e Previdência Social (INSS), Fazenda Estadual ou Municipal (aquela que for pertinente ao seu ramo de atividade e compatível com o objeto deste instrumento), o Fundo de Garantia por Tempo de Serviço (FGTS) e Justiça do Trabalho (CNDT – TST).

5.3.1. Caso a execução do objeto seja realizada através de nota fiscal da Matriz ou Filial cujo CNPJ seja diferente do constante na Proposta apresentada, esta deverá estar acompanhada das mesmas certidões mencionadas no item anterior.

5.3.1.1. Somente poderá ocorrer a situação acima, caso não ocorra à alteração de Alíquota de ICMS ou qualquer outro custo que possa ser creditado ao **SENAR-AR/MS**.

5.4. Deverá constar na nota fiscal emitida: o objeto, o período faturado, as quantidades, o valor unitário, o valor total, o número da conta bancária de natureza jurídica, agência e banco a ser efetuado o pagamento, o número do Contrato.

5.5. Valores constantes da Nota Fiscal deverão refletir fidedignamente o objeto contratado pelo **SENAR-AR/MS**.

5.6. As notas fiscais não aprovadas pelo **SENAR-AR/MS** serão devolvidas à **CONTRATADA**, para as devidas correções, acompanhadas dos motivos de sua rejeição, renovando-se o prazo para pagamento estabelecido no **subitem 5.2** deste Instrumento, a partir da sua reapresentação, sem qualquer tipo de correção de seu valor.

5.7. A inadimplência da **CONTRATADA**, com referência aos encargos pertinentes à execução do objeto não transfere a responsabilidade por seu pagamento ao **SENAR-AR/MS**, nem pode onerar o objeto contratado.

6. DA FISCALIZAÇÃO

6.1. O **SENAR-AR/MS** fiscalizará a execução do objeto pela **CONTRATADA** por meio de colaborador designado formalmente e que verificará o cumprimento das especificações solicitadas, no todo ou em parte, no sentido de corresponderem ao desejado ou especificado.

6.2. A fiscalização pelo **SENAR-AR/MS** não desobriga a **CONTRATADA** de sua responsabilidade quanto à perfeita execução do objeto deste Instrumento.

6.3. A ausência de comunicação por parte do **SENAR-AR/MS**, referente a irregularidades ou falhas, não exime a **CONTRATADA** das responsabilidades determinadas no contrato ou documento equivalente.

6.4. A fiscalização se reserva ao direito de impugnar a execução do objeto pela **CONTRATADA**, quando não realizada a contento, ficando a **CONTRATADA** obrigada a refazê-los, sem quaisquer ônus para o **SENAR-AR/MS**.

6.5. O fiscal deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto no contrato ou documento equivalente.

7. DAS OBRIGAÇÕES DA CONTRATADA

7.1. Constituem obrigações da **CONTRATADA**, além das demais previstas neste documento ou dele decorrentes:

7.1.1. Designar um responsável para exercer a fiscalização deste instrumento junto ao **SENAR-AR/MS** adotando as providências necessárias para a boa execução do objeto.

7.1.2. Manter, durante a vigência deste instrumento, todas as condições de habilitação válidas, apresentando sempre que exigido, os comprovantes de regularidade fiscal, bem como quaisquer outras determinações legais que sejam próprias de seu ramo de atividade mesmo que não inseridas neste instrumento ou instrumentos a ele vinculados.

7.1.3. Cumprir todas as leis e posturas federais, estaduais e municipais pertinentes e responsabilizar-se por todos os prejuízos decorrentes de infrações a que houver dado causa.

7.1.4. Assumir, com exclusividade, todos os impostos e taxas que forem devidos em decorrência da execução do objeto, bem como as contribuições devidas à Previdência Social, encargos trabalhistas e quaisquer outras despesas que se fizerem necessárias.

7.1.5. Responsabilizar-se pelo ônus resultante de quaisquer ações, demandas, custos e despesas decorrentes de danos causados por culpa ou dolo de seus empregados, prepostos e/ou contratados, bem como se obrigar por quaisquer responsabilidades decorrentes de ações judiciais que lhe venham a ser atribuídas por força de lei, relacionadas com o cumprimento deste instrumento.

7.1.6. Praticar rigorosamente os preços estabelecidos na sua Proposta de Preços para a execução do objeto.

7.1.7. Não subcontratar ou transferir em hipótese alguma os direitos advindos deste instrumento a terceiros, seja a que título for.

7.1.8. Não permitir a utilização de qualquer trabalho de menor de 16 (dezesseis) anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre.

7.1.9. Comunicar ao responsável indicado pelo **SENAR-AR/MS** sobre qualquer anormalidade constatada e prestar os esclarecimentos solicitados.

7.1.10. Encaminhar as notas fiscais para pagamento juntamente com as certidões de regularidade fiscal e outros documentos que se fizerem necessários.

7.1.11. Comunicar imediatamente ao **SENAR-AR/MS** qualquer alteração em seus dados cadastrais.

7.1.12. Prestar todos os esclarecimentos que forem solicitados pela fiscalização, cujas reclamações se obrigam prontamente a atender, corrigindo imediatamente as deficiências apontadas, sejam elas relativas à execução do objeto ou burocráticas, bem como dará ciência ao **SENAR-AR/MS**, prontamente e por escrito, de qualquer anormalidade verificada na execução do objeto.

7.1.13. Responder, civil e penalmente, por quaisquer danos materiais ou pessoais ocasionados, ao **SENAR-AR/MS** e/ou a terceiros, por seus empregados e/ou prepostos, dolosa ou culposamente, quando da execução do objeto.

8. DA VISTORIA

8.1. As empresas interessadas poderão realizar vistoria prévia nas instalações do **SENAR-AR/MS**, onde será implantada e operacionalizada a solução integrada de segurança cibernética, mediante prévio agendamento junto à área de Tecnologia da Informação do **SENAR-AR/MS**.

8.1.1. A vistoria deverá ser agendada por meio do telefone **(67) 3320-9748** ou do e-mail tinfra@senarms.org.br, direcionado à área de Tecnologia da Informação do **SENAR-AR/MS**, em dias úteis, no horário das 9h às 11h e das 14h às 16h30, condicionada à disponibilidade previamente estabelecida em sua agenda.

8.1.2. Para a vistoria a empresa interessada deverá estar devidamente identificada, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

8.1.2. A vistoria será acompanhada por funcionário do **SENAR-AR/MS**. Ao final da visita será emitido atestado de vistoria prévia (**Modelo Anexo VII**), que servirá como comprovação de participação.

8.2. A vistoria técnica, embora facultativa, é fortemente recomendada em razão da complexidade do ambiente tecnológico a ser protegido, tendo por finalidade permitir que as licitantes conheçam, de forma prévia e adequada, a infraestrutura existente, incluindo servidores, estações de trabalho, ativos de conectividade, sistemas administrativos e educacionais e os mecanismos de integração já utilizados, de modo a subsidiar a elaboração de propostas tecnicamente compatíveis com as condições atuais do **SENAR-AR/MS**, bem como a avaliação in loco dos aspectos operacionais que possam impactar na configuração, parametrização, implantação, suporte, manutenção e desempenho da solução de segurança da informação, contribuindo para maior precisão na formação de preços e na previsão dos recursos necessários.

8.3. A empresa interessada que **optar por realizar a vistoria** deverá apresentar a Declaração de Vistoria (**Modelo Anexo VII**), declarando que vistoriou, por intermédio de seu Representante Legal, os locais e instalações da prestação dos serviços, tendo então pleno conhecimento das condições e eventuais dificuldades para a execução dos mesmos, bem como de todas as informações necessárias à formulação da sua proposta de preços. **Não serão aceitas alegações posteriores quanto ao desconhecimento da situação.**

8.4. Caso a empresa interessada **opte por não realizar a vistoria**, deverá apresentar a Declaração de Dispensa de Vistoria (**Modelo Anexo VIII**), em substituição a Declaração de Vistoria, devidamente assinada por seu responsável legal, em conformidade com o instrumento convocatório, sob as penalidades da Lei, assumindo que:

- a)** Compreende integralmente o escopo e as exigências da contratação;
- b)** Não poderá alegar, em momento posterior, desconhecimento de informações técnicas ou de condições locais como justificativa para descumprimento contratual;
- c)** Assume integralmente os ônus decorrentes de eventual insuficiência de análise prévia.

8.5. Realizada ou não a vistoria, a Administração do **SENAR-AR/MS** não aceitará alegações posteriores baseadas em desconhecimento das condições locais, da infraestrutura tecnológica existente ou das especificidades do ambiente institucional.

9. DOS REQUISITOS MÍNIMOS DA EMPRESA – QUALIFICAÇÃO TÉCNICA

9.1. As empresas interessadas deverão comprovar aptidão para prestação de serviço com características semelhantes ao objeto deste instrumento, por meio de apresentação de Atestado de Capacidade Técnica, expedido por pessoa jurídica de direito público ou privado,

em seu nome que comprove a execução, de forma satisfatória, de desempenho de atividades compatíveis e/ou similares de:

- a)** Serviços de implantação de solução de segurança da informação tipo appliances NGFW (Next Generation Firewall) em ambiente de alta disponibilidade (High-availability clusters), conforme previsto no item “Especificação do Objeto”;
- b)** Serviços de operação de solução de segurança da informação tipo appliances NGFW (Next Generation Firewall) em ambiente de alta disponibilidade (High-availability clusters) pelo período mínimo de 12 (doze) meses, conforme previsto no item “Tipos de Serviços de Suporte Técnico e Manutenção”;
- c)** Fornecimento de solução de segurança da informação tipo appliances NGFW (Next Generation Firewall), de linha Enterprise, em ambiente de alta disponibilidade (High-availability clusters), com capacidade mínima cada um de 2.6 Gbps de performance de firewall, 1.7 Gbps de desempenho de IPS (Intrusion Prevention System), 1.6 Gbps de desempenho em modo Threat Prevention (Proteção Anti Malware, IPS e Controle de Aplicação habilitados), 400 Mbps de desempenho em modo de inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS), 900.000 conexões simultâneas/concorrentes no modo SPI e 10.000 novas conexões por segundo, conforme previsto no item “Requisitos Mínimos de Desempenho”;
- d)** Implantação de solução de segurança da informação tipo Endpoint com recursos EDR (Endpoint Detection and Response) para proteção de estações de trabalho, servidores e dispositivos móveis, com no mínimo 200 (duzentos) endpoints, conforme previsto no item “Requisitos Técnicos para Solução para Proteção de Endpoints”;
- e)** Operação de solução de segurança da informação, com no mínimo 200 (duzentos) endpoints com recursos EDR (Endpoint Detection and Response) para proteção de estações de trabalho, servidores e dispositivos móveis, pelo período mínimo de 12 (doze) meses, conforme previsto no item “Requisitos Técnicos para Solução para Proteção de Endpoints, Módulo de Gerenciamento Avançado e Módulo de EDR”;
- f)** Prestação de serviços de treinamento para solução de segurança da informação endpoint, com no mínimo os seguintes tópicos: visão geral da solução; console central, agentes e endpoint; criação de regras, políticas e relatórios; utilização das melhores práticas.

9.1.1. O documento deverá ser fornecido em papel timbrado de cliente da proponente, no qual expressamente constará o detalhamento e o período da prestação dos serviços anteriormente realizada, data de emissão do atestado, assinatura e identificação do signatário (nome, cargo e função que exerce junto à empresa emitente).

9.1.2. Para fins de comprovar a atuação em trabalhos similares da forma como determinado no item **9.1**, o atestado poderá ser acompanhado de outros documentos pertinentes.

9.2. A **CONTRATADA** deverá apresentar carta de credenciamento emitida pelo fabricante, assinada por representante legal no Brasil, atestando que a **CONTRATADA** é empresa autorizada e credenciada para comercializar, instalar e dar suporte aos produtos ofertados.

9.3. As empresas interessadas deverão possuir regularidade fiscal para com a Fazenda Federal e Previdência Social (INSS), Fazenda Estadual ou Municipal (aquela que for pertinente ao seu ramo de atividade e compatível com o objeto deste instrumento), o Fundo de Garantia por Tempo de Serviço (FGTS) e Justiça do Trabalho (CNDT – TST).