ASSOCIAÇÃO EVANGÉLICA BENEFICENTE ESPÍRITO-SANTENSE, pessoa jurídica de direito privado de utilidade pública, inscrita no CNPJ sob o n.º 28.127.926/0003-23, com endereço na Rua Desembargador José Vicente, nº 110, Forte São João, Vitória/ES, CEP 29.017-090, que atua como gestora do Hospital Estadual de Urgência e Emergência, torna público a realização do processo de contratação Prestação de serviços gerenciados de segurança com características de Antivírus com XDR, do tipo Menor Preço.

1. DISPOSIÇÕES PRELIMINARES:

I. Data da Publicação**: 01/02/2024.**

II. Data de início do acolhimento das propostas: **às 10:00h do dia 01/02/2024.** (Horário de Brasília)

III. Data limite para o recebimento das propostas: **às 09:00h do dia 07/02/2024.** (Horário de Brasília)

IV. Abertura das propostas: **às 09:00h do dia 07/02/2024.** (Horário de Brasília)

V. Início da seção de disputa: **às 17:00h do dia 08/02/2024.** (Horário de Brasília)

VI. Endereço eletrônico para envio das propostas: **www.publinexo.com.br/privado/**

VII. O resultado da contratação será divulgado através do site: **https://www.evangelicovv.com.br/institutional/2478-briefings-heue**

VIII. **O envio da proposta para a prestação de serviços neste Termo de Referência importará no aceite total dos termos apresentados neste Termo de Referência e Minuta de Contrato em anexo.**

2. DO OBJETO DA CONTRATAÇÃO

O presente Termo de Referência tem por objeto a contratação de serviços gerenciados de segurança com características de Antivírus com XDR, contemplando os serviços de instalação, configuração, monitoramento e suporte técnico ilimitado/mês; para o Hospital Estadual de Urgência e Emergência.

SERVIÇOS E PRODUTOS	QTD LICENÇAS
Fornecimento de licenças de uso de solução corporativa de proteção de endpoints de próxima geração com ferramenta de detecção e resposta para estações de trabalho com gerência em nuvem.	320
Fornecimento de licenças de uso de solução corporativa de proteção de endpoints de próxima geração com ferramenta de detecção e resposta para servidores com gerência em nuvem.	15

2.1 ESPECIFICAÇÕES DA CONTRATAÇÃO

2.1.1 Todos os componentes que fazem parte da solução, de segurança para servidores, estações de trabalho deverão ser fornecidas por um único fabricante. Não serão aceitas composições de produtos de fabricantes diferentes;

2.1.2 A console de monitoração e configuração deverá ser feita através de uma central única, baseada em web e em nuvem, que deverá conter todas a fermentas para a monitoração e controle da proteção dos dispositivos;

2.1.3 A console de nuvem deve possuir o armazenamento de seus dados dentro do território nacional, garantindo conformidade e compliance com as leis locais como a LGPD, Instrução normativa 5 e NC-14 determinada pelo Banco Central;

2.1.4 A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional;

2.1.5 Deve possuir mecanismo de comunicação via API, para integração com outras soluções de segurança, como por exemplo SIEM;

2.1.6 Deve possuir capacidade de realizar a integração com soluções de firewalls para criar políticas automáticas em caso de ataques em massa nos computadores e servidores;

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

2.1.8 Deve permitir sincronização com o Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção.

2.1.9 Deve possuir a possibilidade de aplicar regras diferenciadas baseado em grupos ou usuários;

2.1.10 A instalação deve ser feita via cliente específico por download da gerência central ou também via email de configuração.

2.1.11 Deve a console ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando;

2.1.12 Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;

2.1.13 Deve permitir exclusões de escaneamento para um determinado websites, pastas, arquivos ou aplicações, tanto a nível geral quanto específico em uma determinada política.

2.1.14 A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs;

2.1.15 Atualização incremental, remota e em tempo-real, da vacina dos Antivírus e do mecanismo de verificação (Engine) dos clientes;

2.1.16 Permitir o agendamento da varredura contra vírus com a possibilidade de selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador;

2.1.17 Atualização automática das assinaturas de ameaças (malwares) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador;

2.1.18 Utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados.

2.1.19 As mensagens geradas pelo agente deverão estar no idioma em português ou permitir a sua edição.

2.1.20 Permitir a exportação dos relatórios gerenciais para os formatos CSV e PDF;

2.1.21 Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;

2.1.22 Possibilidade de exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão da engine, data da vacina, data da última verificação, eventos recentes e status;

2.1.23 Capacidade de geração de relatórios, estatísticos ou gráficos, tais como:

2.1.24 Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;

2.1.25 Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, bem como detalhes das varreduras e dos alertas nos computadores;

2.1.26 Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;

2.1.27 Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;

2.1.28 Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;

2.1.29 Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;

2.1.30 Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados.

2.1.31 Deverá possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada;

2.1.32 Deve fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um upload (exemplo Dropbox), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra malwares, procuradas palavras chaves ou informações confidenciais. Deve ser bloqueado o upload ou removida a informação confidencial antes do envio do arquivo;

2.1.33 As portas de comunicação deverão ser configuráveis. A comunicação deverá permitir QoS para controlar a largura de banda de rede.

2.1.34 A solução deverá permitir a seleção da versão do software de preferência, permitindo assim o teste da atualização sobre um grupo de PCs piloto antes de implantá-lo para toda a rede. Permitir ainda selecionar um grupo de computadores para aplicar a atualização para controlar a largura de banda de rede. A atualização da versão deverá ser transparente para os usuários finais.

2.1.35 O agente anti-vírus deverá proteger laptops, desktops e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, trojans, worms e spyware. No Windows o agente também deverá detectar PUA, adware, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso a web;

2.1.36 Deve possuir mecanismo contra a desinstalação do endpoint pelo usuário e cada dispositivo deverá ter uma senha única, não sendo autorizadas soluções com senha única válida para todos os dispositivos;

2.1.37 Deve prover no endpoint a solução de HIPS (Host Instrusion Prevention System) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deverá ser atualizado diariamente;

2.1.38 Deve prover proteção automática contra web sites infectados e maliciosos, assim como previnir o ataque de vulnerabilidades de browser via web exploits;

2.1.39 Deve permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalhao e redes sem fio, estando sempre atrelado ao usuário o controle e não ao dispositivo;

2.1.40 O controle de dispositivos deve ser ao nível de permissão, somente leitura ou bloqueio;

2.1.41 Os seguintes dispositivos deverão ser, no mínimo, gerenciados: HD (hard disks) externos, pendrives USB, storages removíveis seguras, CD, DVD, Blu-ray, floppy drives, interfaces de rede sem fio, modems, bluetooth, infra-vermelho, MTP (Media Transfer Protocol) tais como Blackberry, iPhone e Android smartphone e PTP (Picture Transfer Protocol) como câmeras digitais;

2.1.42 A ferramenta de administração centralizada deverá gerenciar todos os componentes da proteção para estações de trabalho e servidores e deverá ser projetada para a fácil administração, supervisão e elaboração de relatórios dos endpoint e servidores;

2.1.43 Deverá possuir interface gráfica web, com suporte a língua portuguesa (padrão brasileiro);

2.1.44 A Console de administração deve incluir um painel com um resumo visual em tempo real para verificação do status de segurança;

2.1.45 Deverá fornecer filtros pré-construídos que permitam visualizar e corrigir apenas os computadores que precisam de atenção;

2.1.46 Deverá exibir os PCs gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus, etc), e classificar os PCs em conformidade;

2.1.47 Uma vez que um problema seja identificado, deverá permitir corrigir os problemas remotamente, com no mínimo as opções abaixo:

2.1.48 Proteger o dispositivo com a opção de início de uma varredura;

2.1.49 Forçar uma atualização naquele momento;

2.1.50 Ver os detalhes dos eventos ocorridos;

2.1.51 Executar verificação completa do sistema;

2.1.52 Forçar o cumprimento de uma nova política de segurança;

2.1.53 Mover o computador para outro grupo;

2.1.54 Apagar o computador da lista;

2.1.55 Atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente;

2.1.56 Gravar um log de auditoria seguro, que monitore a atividade na console de gerenciamento para o cumprimento de regulamentações, auditorias de segurança, análise e solução de problemas forenses;

2.1.57 Deverá permitir exportar o relatório de logs de auditoria nos formatos CSV e PDF;

2.1.58 Deve conter vários relatórios para análise e controle dos usuários e endpoints. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas para os endpoints;

2.1.59 Fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:

2.1.60 Nome do dispositivo;

2.1.61 Início da proteção;

2.1.62 Último usuário logado no dispositivo;

2.1.63 Último update;

2.1.64 Último escaneamento realizado;

2.1.65 Status de proteção do dispositivo;

2.1.66 Grupo a qual o dispositivo faz parte;

2.1.67 Permitir a execução manual de todos estes relatórios danos formatos CSV e PDF;

2.1.68 A console deve possuir métodos de verificação da saúde das configurações da console, possibilitando aos administradores descobrirem facilmente se existe alguma falha de configuração que pode facilitar a entrada de malwares e invasores no ambiente;

2.2 CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO

2.2.1 Características básicas do agente de proteção contra malwares:

2.2.2 Pré-execução do agente para verificar o comportamento malicioso e detectar malware desconhecido;

2.2.3 O agente deve buscar algum sinal de malware ativo e detectar malwares desconhecidos;

2.2.4 O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças;

2.2.5 O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;

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

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

2.2.8 Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

2.2.9 Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

2.2.10 Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

2.2.11 Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;

2.2.12 É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);

2.2.13 Suportar máquinas com arquitetura 32-bit e 64-bit, (Exceto para Windows 11 que não há opção de 32bits;

2.2.14 O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais, macOS 11 Big Sur, 12 Monterey, 13 Ventura, Microsoft Windows 7, 8.1, 10 e 11;

2.2.15 A solução deve ser compatível com a execução nativa em processadores Apple Silicon, não serão aceitas soluções que dependem de emulação via Rosetta2 da Apple.

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

2.2.17 Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;

2.3 FUNCIONALIDADE DE FIREWALL E DETECÇÃO E PROTEÇÃO DE INTRUSÃO (IDS\IPS) COM AS FUNCIONALIDADES:

2.3.1 Deverá possui atualização periódica de novas assinaturas de ataque;

2.3.2 Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

2.3.3 Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;

2.3.4 Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

2.3.5 Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

2.3.6 Deve possuir técnicas de proteção, que inclui:

2.3.7 Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

2.3.8 Algorítimo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;

2.39 Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

2.40 Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

2.41 Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

2.4 FUNCIONALIDADE DE ANTIVÍRUS E ANTISPYWARE:

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

2.4.2 Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

2.4.3 As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;

2.4.4 Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;

2.4.5 Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário;

2.4.6 Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;

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

2.4.8 A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

2.4.9 Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

2.4.10 Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

2.4.11 Antivírus de Web (verificação de sites e downloads contra vírus);

2.4.12 Controle de acesso a sites por categoria;

2.4.13 Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador web, de forma independente do navegador usado, ou seja, sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

2.4.14 O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;

2.4.15 Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;

2.4.16 Capacidade de verificar somente arquivos novos e alterados;

2.4.17 Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

2.5 FUNCIONALIDADE DE DETECÇÃO PRÓ-ATIVA DE RECONHECIMENTO DE NOVAS AMEAÇAS:

2.5.1 Funcionalidade de detecção de ameaças via técnicas de machine learning;

2.5.2 Funcionalidade de detecção de ameaças desconhecidas que estão em memória;

2.5.3 Capacidade de detecção, e bloqueio pró-ativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);

2.5.4 Capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória;

2.5.5 Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

2.6 FUNCIONALIDADE DE PROTEÇÃO CONTRA RANSOMWARES:

2.6.1 Para estações de trabalho, dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;

2.6.2 Para estações de trabalho, dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;

2.6.3 Para servidores, dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;

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

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

2.6.6 Deve ser realizada a *detecção e o bloqueio de, pelo menos, as seguintes* técnicas de *exploit*:

2.6.7 DEP (*Data Execution Prevention*);

2.6.8 *Address Space Layout Randomization* (ASLR);

2.6.9 *Bottom Up ASLR*;

2.6.10 *Null Page*;

2.6.11 *Anti-HeapSpraying*;

2.6.12 *Dynamic Heap Spray*;

2.6.13 *Import Address Table Filtering (IAF)*;

2.6.14 *VTable Hijacking*;

2.6.15 *Stack Pivot and Stack Exec*;

2.6.16 *SEHOP*;

2.6.17 *Stack*-based ROP (*Return-Oriented Programming*);

2.6.18 *Control-Flow Integrity (CFI)*;

2.6.19 *Syscall*;

2.6.20 *WOW64*;

2.6.21 *Load Library*;

2.6.22 *Shellcode*;

2.6.23 *VBScript God Mode*;

2.6.24 *Application Lockdown*;

2.6.25 *Process Protection*;

2.6.26 *Network Lockdown*.

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

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

2.6.29 A console de monitoração e configuração deverão ser feitas através de uma central única, baseada em web e em nuvem, que deverá conter todas a ferramentes para a monitoração e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware.

2.6.30 A console deverá apresentar *Dashboard* com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo ransomware nos endpoints.

2.7 SOLUÇÃO DE ENDPOINT DETECTION AND RESPONSE (EDR)

2.7.1 A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando

2.7.2 detecção e investigação nos endpoints com atividades suspeitas;

2.7.3 Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.

2.7.4 Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.

2.7.5 Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

2.7.6 Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;

2.7.7 Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

2.7.8 Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;

2.7.9 Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;

2.7.10 A solução de EDR deverá ser integrado ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

2.7.11 O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;

2.7.12 Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;

2.7.13 Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;

2.7.14 Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;

2.7.15 Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

2.7.16 Deve possibilizar o agendamento de consultas (queries);

2.7.17 Deve reter os dados no Data Lake por no mínimo 7 dias.

2.8 FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES E DISPOSITIVOS:

2.8.1 Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;

2.8.2 Atualiza automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada;

2.8.3 Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;

2.8.4 Oferecer proteção para chaves de registro e controle de processos;

2.8.5 Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo;

2.8.6 Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;

2.8.7 Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;

2.8.8 Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;

2.8.9 Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;

2.8.10 As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;

2.8.11 Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

2.8.12 A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;

2.8.13 Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

2.8.13.1 Permitir que todos os dispositivos do mesmo modelo;

2.8.13.2 Permitir que um único dispositivo com base em seu número de identificação único;

2.8.13.3 Permitir o acesso total;

2.8.13.4 Permitir acesso somente leitura;

2.8.14 Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

2.9 FUNCIONALIDADE DE PROTEÇÃO E PREVENÇÃO A PERDA DE DADOS

2.9.1 Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo**;**

2.9.2 Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

2.9.3 Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

2.9.4 Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

2.9.4.1 Números de cartões de crédito;

2.9.4.2 Números de contas bancárias;

2.9.4.3 Números de Passaportes;

2.9.4.4 Endereços;

2.9.4.5 Números de telefone;

2.9.4.6 Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, etc;

2.9.4.7 Lista de e-mails;

2.9.4.8 Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários, etc;

2.9.5 Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;

2.9.6 Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

2.9.7 Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

2.9.8 Permitir o controle de dados para no mínimo os seguintes meios:

2.9.8.1 Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);

2.9.8.2 Anexado no navegador (ao menos IE, Firefox e Chrome);

2.9.8.3 Anexado no cliente de mensagens instantâneas (ao menos Skype);

2.9.8.4 Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

2.10 CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA SERVIDORES

2.10.1 A solução deverá ser capaz de proteger servidores contra malwares, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores;

2.10.2 Deve realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos;

2.10.3 O agente host deve buscar algum sinal de malwares ativos e detectar malwares desconhecidos;

2.10.4 O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;

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

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

2.10.7 Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

2.10.8 Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

2.10.9 Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

2.10.10 Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;

2.10.11 É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);

2.10.12 O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais abaixo:

2.10.12.1 Versões sevidores tais como Windows Server 2008,2012,2016 e 2019

2.10.12.2 Versões desktop tais como Windows7, 8 e Windows 10

2.10.12.3 CentOS 7;

2.10.12.4 Debian 10;

2.10.12.5 Oracle Linux 7;

2.10.12.6 Oracle Linux 8;

2.10.12.7 Red Hat Enterprise 7;

2.10.12.8 Red Hat Enterprise 8;

2.10.12.9 Red Hat Enterprise 9;

2.10.12.10 SUSE Linux Enterprise Server 12;

2.10.12.11 SUSE Linux Enterprise Server 15;

2.10.12.12 Ubuntu 20.04 LTS;

2.10.12.13 Ubuntu 22.04 LTS;

2.10.13 Deve suportar o uso de servidores usados para atualização em cache para diminuir a largura de banda usada nas atualizações;

2.10.14 Deve possuir integração com as nuvens da Microsoft Azure e Amazon Web Services para identificar as informações dos servidores instanciados nas nuvens;

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

2.10.16 Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;

2.10.17 Deve possuir funcionalidades de tecnologias conhecidas como CWPP – Cloud Workload Protection Plataform, permitindo que seja possível trazer funcionalidades de próxima geração para cargas de trabalho em nuvem, bem como containers, e afins;

2.10.18 A solução deve no mínimo, utilizar o modelo de sensores para containers, garantindo visibilidade e proteção de, no mínimo, estes tipos de ataques:

2.10.18.1 Escalação de privilégios dentro de containers;

2.10.18.2 Programas utilizando técnicas de mineração de criptomoedas;

2.10.18.3 Detecção de atacantes tentando destruir evidências de ambientes comprometidos (IOC – Indicator of compromise);

2.10.18.4 Detecção de funções internas do kernel que estão sendo adulteradas em um host;

2.10.19 A solução deve também se integrar à tecnologias de CSPM – Cloud Security Posture Management, tendo como objetivo trazer funcionalidades de análises integradas de CWPP e CSPM a fim de melhorar a visibilidade e resposta à incidentes em ambientes de nuvem públicas,

2.11 FUNCIONALIDADE DE FIREWALL E DETECÇÃO E PROTEÇÃO DE INTRUSÃO (IDS\IPS) COM AS FUNCIONALIDADES:

2.11.1 Possuir proteção contra exploração de buffer overflow;

2.11.2 Deverá possui atualização periódica de novas assinaturas de ataque;

2.11.3 Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

2.11.4 Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;

2.11.5 Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

2.11.6 Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

2.11.7 Deve possuir técnicas de proteção, que inclui:

2.11.7.1 Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

2.11.7.2 Algoritmo correspondente **padrão** - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;

2.11.7.3 Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

2.11.7.4 Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

2.11.7.5 Verificação de ameaças web avançadas**:** bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

2.12 FUNCIONALIDADE DE ANTIVÍRUS E ANTISPYWARE:

2.12.1 Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.
2.12.2 Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.
2.12.3 As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;
2.12.4 Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;
2.12.5 Permitir a varredura das ameaças da maneira manual, agendada e em tempo real nos servidores;
2.12.6 Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;
2.12.7 Capacidade de detectar arquivos através da reputação dos mesmos;
2.12.8 Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;
2.12.9 A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;
2.12.10 Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;
2.12.11 Deverá detectar tráfego de rede para comandar e controlar os servidores;
2.12.12 Proteger arquivos de documento contra ataques do tipo ransomwares;
2.12.13 Proteger que o ataque de ransomware seja executado remotamente;
2.12.14 Permitir o envio de amostras de malwares para a nuvem de inteligência do fabricante;
2.12.15 Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;
2.12.16 Antivírus de Web (verificação de sites e downloads contra vírus);
2.12.17 Controle de acesso a sites por categoria;
2.12.18 Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.
2.12.19 O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;
2.12.20 Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;
2.12.21 Capacidade de verificar somente arquivos novos e alterados;

2.12.22 Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.
2.12.23 Capacidade de habilitar mensagens de desktop para a Proteção contra Ameaças;
2.12.24 Capacidade de adicionar exclusão de varredura para arquivos, pastas, processos, sites, aplicativos e tipos de explorações detectadas;

2.13 FUNCIONALIDADE DE PROTEÇÃO CONTRA RANSOMWARES:

2.13.1 Deve dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;
2.13.2 Deve dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;
2.13.3 Deve dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;

2.14 FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES E DISPOSITIVOS:

2.14.1 Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;
2.14.2 Atualiza automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada;
2.14.3 Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;
2.14.4 Oferecer proteção para chaves de registro e controle de processos;
2.14.5 Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo;
2.14.6 Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;
2.14.7 Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;
2.14.8 Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;
2.14.9 Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;
2.14.10 As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;
2.14.11 Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
2.14.12 A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;
2.14.13 Permitir a autorização de um dispositivo com no mínimo as seguintes opções:
2.14.13.1 Permitir que todos os dispositivos do mesmo modelo;
2.14.13.2 Permitir que um único dispositivo com base em seu número de identificação único;
2.14.13.3 Permitir o acesso total;

2.14.13.4 Permitir acesso somente leitura;

2.14.14 Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

2.15 FUNCIONALIDADE DE PROTEÇÃO E PREVENÇÃO A PERDA DE DADOS

2.15.1 Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;

2.15.2 Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

2.15.3 Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

2.15.4 Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

2.15.4.1 Números de cartões de crédito;

2.15.4.2 Números de contas bancárias;

2.15.4.3 Números de Passaportes;

2.15.4.4 Endereços;

2.15.4.5 Números de telefone;

2.15.4.6 Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, etc;

2.15.4.7 Lista de e-mails;

2.15.4.8 Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários, etc;

2.15.5 Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;

2.15.6 Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

2.15.7 Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

2.15.8 Permitir o controle de dados para no mínimo os seguintes meios:

2.15.8.1 Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);

2.15.8.2 Anexado no navegador (ao menos IE, Firefox e Chrome);

2.15.8.3 Anexado no cliente de mensagens instantâneas (ao menos Skype);

2.15.8.4 Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

2.16 SOLUÇÃO DE ENDPOINT DETECTION AND RESPONSE (EDR)

2.16.1 A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;

2.16.2 Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.

2.16.3 Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.

2.16.4 Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

2.16.4.1 Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;

2.16.4.2 Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

2.16.4.3 Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;

2.16.4.4 Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;

2.16.5 A solução de EDR deverá ser integrado ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

2.16.6 O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;

2.16.7 Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;

2.16.8 Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;

2.16.9 Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;

2.16.10 Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

2.16.10.1 Deve possibilizar o agendamento de consultas;

2.16.10.2 Deve reter os dados no Data Lake por no mínimo 7 dias.

2.17 SOLUÇÃO DE EXTENDED DETECTION AND RESPONSE (XDR)

2.17.1 Deve possuir Data Lake que armazene informações críticas de endpoints e servidores, mas também incorporando dados de outras soluções de segurança como firewalls, e-mail gateways, public cloud e mobile, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

2.17.2 Deve possuir recurso de pesquisa estruturada em banco de dados compatível com SQL, ou similar;

2.17.3 Deve disponibilizar recurso de pesquisa para comparar os indicadores de comprometimento de várias fontes de dados para identificar rapidamente um ataque suspeito;

2.17.4 Deve utilizar detecções de ATP e IPS do firewall para investigar endpoints suspeitos;

2.17.5 Deve disponibilizar pontos de aplicação que permitem a executar ações, como colocar em quarentena um endpoint comprometido, bloquear o tráfego de rede ou remover malware;

2.17.6 Deve possuir sensores que fornecem telemetria de diferentes aspectos da infraestrutura de TI, capazes de identificar dispositivos não gerenciados e desprotegidos em toda o ambiente da organização;

2.17.7 Deve possibilitar o agendamento de consultas (queries) cíclicas no Data Lake para identificação de IoCs em execuções antecipadas;

2.17.8 Deve permitir a integração via APIs com sistemas e fluxos de trabalhos já existentes;

2.17.9 Deve reter os dados no Data Lake por no mínimo 30 dias.

2.17.10 O XDR deve permitir integração com sistemas de terceiros, no mínimo, tecnologias como Office 365 e produtos de CSPM para visibilidade e correlação de eventos em ambientes de Cloud como Azure, AWS e Google Cloud;

2.17.11 A console do XDR deve correlacionar os dados recebidos e armazenados no DataLake e gerar evidências de ataques ou eventos suspeitos existentes dentro do ambiente;

2.17.12 Tais detecções e evidencias devem conter todos os detalhes do evento, bem como uma análise do próprio fabricante sobre a classificação de risco de tal evento;

2.17.13 Deve possibilitar também que investigações sejam realizadas a partir destes eventos, coletando dados e executando consultas dentro do Datalake ou nos próprios dispositivos a fim de coletar mais evidências para determinar a realidade do ataque presente na console;

2.17.14 Deve possuir console para gerenciamento de investigações, podendo adicionar de forma automática ou manual, diversos eventos e detecções encontradas na console;

2.17.15 A console de gerenciamento de investigações deve permitir atribuir analistas que acompanharão a investigação;

2.17.16 Será necessário também que exista uma trilha de auditoria para cada investigação, de tal forma que os administradores da console consigam auditar os detalhes da condução da investigação;

SLA PARA ATENDIMENTO

A CONTRATADA deverá cumprir prazos máximos para respostas aos acionamentos, de acordo com o nível de severidade de cada chamado, conforme detalhado seguir, onde as horas definidas são corridas a partir da abertura do chamado de atendimento (solicitação e incidente).

Estado do Ambiente	Tipo	Tipo de Chamado	Tempo para primeiro Atendimento	Tempo para solução de contorno ou definitiva
Parado	Crítico	Incidente	30 minutos corridos	2 horas corridas
Intermitente	Alerta	Incidente	1 hora corrida	4 horas corridas
Operando	Ações preventivas, criação e alteração de novas regras e pequenos ajustes de configuração (de baixo impacto)	Solicitação	4 horas úteis	12 horas úteis
Informacional	Esclarecimento de dúvidas, consultas técnicas, criação de relatórios e análise de vulnerabilidades	Solicitação	4 horas úteis	24 horas úteis

ABERTURA DE CHAMADOS

Deverá ser possível a abertura de chamado técnico (Solicitações de Atendimento) via ferramenta WEB, telefone (fixo ou celular), e-mail. O registro via ferramenta WEB será à principal forma de abertura de chamados (Solicitações de Atendimento) e de relacionamento técnico entre o CONTRATANTE e a CONTRATADA.

A empresa CONTRATADA deverá disponibilizar funcionalidade de internet para registro de chamados (Solicitações de Atendimento), devendo esta ferramenta ser capaz de gerenciar todo o ciclo de atendimento, desde a solicitação até o encerramento do atendimento. Alternativamente, a empresa atenderá a Solicitações de Atendimento através de e-mail, devendo a CONTRATADA gerenciar a troca de e-mails de forma a permitir o acompanhamento de todo o ciclo de atendimento.

A CONTRATADA deverá responsabilizar-se e permitir o registro de todos os fatos e dados a partir do recebimento das Solicitações de Atendimento nesta ferramenta WEB, de maneira a evidenciar as variáveis para atendimento e posterior faturamento dos serviços.

OS SERVIÇOS DE SUPORTE ESPECIALIZADO SOLUÇÃO DE ANTIVÍRUS NO MÍNIMO, AS SEGUINTES ATIVIDADES:

Execução de serviços de suporte, disponível durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

A CONTRATADA deverá manter em regime de sobreaviso, em regime de 24x7, profissionais especializados nas atividades inerentes ao serviço de suporte especializado. Nas situações de sobreaviso, a CONTRATADA deverá disponibilizar aos técnicos contratados os mecanismos tecnológicos (tais como telefones celulares, telefones fixos, e-mails ou outros), que permitam o acionamento nos casos de necessidade, sem ônus adicional para a CONTRATANTE.

Os serviços de suporte especializado serão executados preferencialmente de forma remota a partir das dependências da CONTRATADA, onde os técnicos ficarão alocados, exceto quando a presença do técnico nas dependências da CONTRATANTE for indispensável.

3. DA VIGÊNCIA DO CONTRATO

O prazo de vigência do contrato será por 60 (sessenta), a contar da data de assinatura do instrumento contratual.

4. CRITÉRIO DE JULGAMENTO

Menor Preço.

4.1 TETO ORÇAMENTÁRIO

O valor do Teto Orçamentário será de R$ 6.000,00 (seis mil reais) mensal.

5. DA PARTICIPAÇÃO

As empresas que desejarem participar do Termo de Referência deverão, obrigatoriamente, cadastrar-se gratuitamente na plataforma eletrônica denominada PUBLInexo, através do link a seguir: **www.publinexo.com.br/privado/**.

5.1 Do Credenciamento na Plataforma

5.1.1 O registro no site, o credenciamento dos representantes que atuarão em nome da proponente e a senha de acesso, deverá ser obtido antes do prazo limite do recebimento das propostas. O cadastro e o acesso à plataforma são gratuitos.

5.1.2 Para participação do Termo de Referência na plataforma PUBLInexo, a proponente deverá utilizar a chave de acesso e senha fornecida através de cadastro no site: www.publinexo.com.br/privado/.

5.1.3 A proponente responderá integralmente por todos os atos praticados no Termo de Referência, por seus representantes devidamente credenciados, assim como pela utilização da senha de acesso ao sistema, ainda que indevidamente, inclusive por pessoa não credenciada como sua representante.

5.2 Da Proposta

5.2.1 A Proposta de preço deverá ser apresentada por meio eletrônico no endereço www.publinexo.com.br/privado/, em idioma nacional, com a identificação da empresa, sem emendas, rasuras ou entrelinhas, devidamente datada, e na qual constará obrigatoriamente:

I. Nome;
II. Razão ou Denominação Social;

III. Endereço completo do proponente;
IV. Identificação do signatário da proposta, sua função e cargo na empresa no campo Observações no ato do registro das propostas;
V. CNPJ e Inscrição Estadual da empresa;

5.2.2 Junto com a proposta de preço, o interessado deverá apresentar os documentos alusivos à sua habilitação, nos termos do item 8 deste Termo de Referência, sob pena de eliminação do certame.

5.2.3 Caso haja discrepâncias entre o descritivo na plataforma e no Termo de Referência, prevalecerá sempre o descritivo do Termo de Referência;

5.2.4 Deverá constar Preços UNITÁRIOS, de forma clara e induvidosa, expresso em moeda nacional, apurada na data de apresentação da proposta, sem inclusão de encargo financeiro ou previsão inflacionária;

I. Nesses preços deverão ser computadas todas as despesas, impostos e outros que envolvam o Fornecimento objeto deste Termo de Referência;
II. Todos os preços da Proposta deverão ser apresentados na moeda corrente nacional (Real), utilizando-se até quatro casas decimais para os centavos, precedidos da vírgula que segue a unidade, desprezando-se as frações remanescentes.

5.2.5 O Responsável pelo certame, solicitará ao arrematante do lote, que encaminhe exclusivamente por meio do sistema e/ou e-mail, em até 02 (dois) dias úteis após o encerramento da disputa, a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Termo de Referência e já apresentados.

5.2.6 Após a negociação do preço, o Responsável pelo certame iniciará a fase de aceitação e julgamento da proposta.

5.2.7 Na hipótese de a proposta vencedora não ser aceitável ou a participante não atender às exigências para habilitação, o Responsável pelo certame examinará a proposta subsequente e assim sucessivamente na ordem de classificação, até a apuração de uma proposta que atenda ao Termo de Referência.

5.3 Do Procedimento

5.3.1 O Ato Convocatório será processado e julgado com observância dos seguintes procedimentos:

I. No dia e horário indicado neste ato Convocatório será aberta a sessão do Termo de Referência, com a abertura automática das propostas e sua divulgação, pelo sistema, na forma de grade ordenatória;

II. A análise das propostas visará ao atendimento das condições estabelecidas neste Ato Convocatório e seus anexos, sendo desclassificadas as propostas:

a) cujo objeto não atenda as especificações, prazos e condições fixados no Ato Convocatório; e
b) que apresentem preço baseado exclusivamente em proposta das demais proponentes.

III. No tocante aos preços, as propostas serão verificadas quanto à exatidão das operações aritméticas que conduziram ao valor total orçado, procedendo-se às correções no caso de eventuais erros, tomando-se como corretos os preços unitários. As correções efetuadas serão consideradas para apuração do valor da proposta.

IV. As propostas não desclassificadas serão selecionadas para a etapa de lances.

V. Será iniciada a etapa de lances, com a participação de todas as proponentes detentoras de propostas classificadas.

VI. Os lances deverão ser formulados exclusivamente por meio eletrônico e em valores distintos e decrescentes, inferiores à proposta de menor preço, observada a redução mínima entre os lances de acordo com o critério do responsável pelo presente processo (decréscimo), aplicável inclusive em relação ao primeiro colocado.

VII. A etapa de lances será considerada encerrada após o prazo determinado pelo responsável pelo presente processo e após a execução do tempo randômico. O Responsável não terá controle sobre o tempo randômico, ou seja, o sistema se encerará automaticamente e aleatoriamente sem a intervenção humana.

VIII. A aceitabilidade será aferida a partir dos preços de mercado vigentes na data da apresentação das propostas, apurados mediante pesquisa realizada pelo departamento de compras da instituição.

5.4 Da Desconexão do Sistema Eletrônico

5.4.1 À proponente caberá acompanhar as operações no sistema eletrônico, durante a sessão, respondendo pelo ônus decorrente de sua desconexão ou da inobservância de quaisquer mensagens emitidas pelo sistema.

5.4.2 No caso de desconexão do responsável pelo presente processo, no decorrer da etapa de lances, se o sistema eletrônico permanecer acessível aos proponentes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

5.5.3 Quando a desconexão do responsável pelo presente processo persistir por tempo superior a dez minutos, a sessão na forma eletrônica será suspensa e reiniciada somente após comunicação aos participantes, no endereço eletrônico utilizado para divulgação.

6. CRITÉRIO ELIMINATÓRIO

I. Envio da proposta fora do prazo estabelecido nas disposições preliminares do presente termo ou em desacordo com o objeto da contratação.

II. Ausência do envio de qualquer dos documentos obrigatórios descritos no item 8.

7. CRITÉRIO DE DESEMPATE

Melhor oferta com vistas a redução de preço.

8. DA HABILITAÇÃO OBRIGATÓRIA

Para habilitação, exigir-se-á dos interessados, exclusivamente, documentação relativa a:

8.1. Habilitação Jurídica:

I. Prova de inscrição no Cadastro Nacional de Pessoa Jurídica – CNPJ do Ministério da Fazenda;

II. Registro comercial, no caso de empresa individual;

III. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades empresariais ou cooperativas e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores e alterações ou da consolidação respectiva, sendo que deles deverá constar, entre os objetivos sociais, a execução de atividades da mesma natureza ou compatível com o objeto deste Termo de Referência;

IV. Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de eleição da diretoria em exercício;

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

8.2. Qualificação Técnica:

I. Alvará de funcionamento e demais alvarás obrigatórios em relação ao ramo de atividade desenvolvida. (Exemplos: Alvará de vigilância sanitária e corpo de bombeiro);

II. Certificado de responsabilidade e regularidade técnica, se houver imposição legal para a atividade desenvolvida;

III. CNAE - Classificação Nacional de Atividades Econômicas, compatível com o objeto da contratação para qual será contratada.

IV. Atestado de capacidade técnica atual na área de prestação dos serviços/fornecimento de produtos, conforme anexo I;

8.3. Regularidade fiscal e trabalhista

I. Prova de regularidade para com a Fazenda Federal, Estadual e Municipal do domicílio ou sede da contratada, ou outra equivalente, na forma da lei;

II. Certidão Negativa de Débitos Trabalhistas (CNDT), expedida gratuitamente e eletronicamente junto à justiça trabalhista (TST);

III. Prova de regularidade perante a Seguridade Social, mediante a apresentação dos seguintes documentos:
III.I CRF – Certificado de Regularidade do FGTS, emitido pela Caixa Econômica Federal;

IV. É requisito para habilitação da empresa capital social compatível com o número de empregados, observando-se parâmetros estabelecido no Art. 4º-B da Lei 13.429, de 31 de março de 2017;

8.4 Os documentos devem ser enviados juntamente com a proposta, sob pena de eliminação.

8.5 A qualificação exigida deverá ser mantida vigente durante toda vigência do contrato a ser firmado com a empresa

ganhadora.

8.6 Se a empresa estiver desobrigada da apresentação de quaisquer documentos solicitados deverá comprovar esta condição por meio de certificado expedido por órgão competente ou legislação em vigor.

8.7 Caso necessário, o responsável pelo presente processo, poderá solicitar visita técnica à empresa que apresentar melhor proposta e documentação obrigatória de acordo com o Termo de Referência, cabendo ao setor de qualidade do hospital realizar a visita técnica no prazo máximo de 5 dias úteis posterior a data da solicitação de visita requerida, apresentando o resultado da avaliação em até 2 dias úteis após a visita técnica.

9. DOS ESCLARECIMENTOS, IMPUGNAÇÕES E RECURSOS:

9.1 Será permitido esclarecimento de dúvidas até o terceiro dia útil após a publicação do Termo de Referência, somente através do e-mail: **compras.tr@heue.aebes.org.br**. Na solicitação de esclarecimentos, a empresa deverá apresentar sua razão social, número de CNPJ, identificar o nº do Termo de Referência e objeto da contratação, devendo o questionamento ser redigido de forma clara e objetiva.

9.2 A empresa que solicitar esclarecimentos, deverá informar os contatos para retorno, telefone e e-mails.

9.3 As solicitações de esclarecimentos que não atenderem os requisitos dos itens anteriores, não serão respondidos.

9.4 Serão recebidas as impugnações enviadas até às 17h do quinto dia útil anterior à data limite para o recebimento das propostas.

9.5 Não serão conhecidas às impugnações e os recursos apresentados fora do prazo estabelecido neste Termo de Referência.

9.6 As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame. No entanto, caso o responsável pelo processo julgue pelo acolhimento de eventual impugnação contra o ato convocatório, poderá ser definida e publicada nova data para o envio de propostas.

9.7 Encerrado o processo na plataforma **www.publinexo.com.br/privado/** o resultado será publicado no site **https://www.evangelicovv.com.br/institutional/2478-briefings-heue**, qualquer participante do referido Termo de Referência poderá recorrer do resultado, interpondo o recurso com as razões de pedido e seus fundamentos, até às 17h do terceiro dia útil, após a data de publicação, de forma motivada e com o registro de suas razões.

9.8 A falta de interposição do recurso contendo suas razões de pedido e seus fundamentos por parte dos participantes, na forma e prazo estabelecidos nos itens anteriores, importará decadência desse direito, ficando o responsável pelo presente processo autorizado a homologar o objeto ao participante declarado vencedor.

9.9 Os recursos deverão ser endereçados ao endereço de e-mail **compras.tr@heue.aebes.org.br** e dirigidos ao responsável pelo presente processo. O e-mail deverá conter razão social, número do cartão CNPJ, identificar o nº do Termo de Referência e objeto da contratação e as alegações. Caberá ao responsável pelo presente processo receber, examinar e decidir os recursos impetrados contra suas decisões, no prazo de 06 (seis) dias úteis do recebimento do recurso.

9.10 O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

9.11 Decididos os recursos e constatada a regularidade dos atos praticados, o responsável competente adjudicará o objeto e homologará o processo de contratação.

10. DISPOSIÇÕES FINAIS

10.1 O presente Termo de Referência não importa necessariamente em contratação, podendo a AEBES revogá-la, no todo ou em parte, por razões de interesse público, derivadas de fato supervenientes comprovados ou anulá-la por ilegalidade, de ofício ou por provocação, mediante ato escrito e fundamentado, disponibilizado no sistema para conhecimento dos interessados. A ASSOCIAÇÃO EVANGÉLICA BENEFICENTE ESPÍRITO SANTENSE – AEBES poderá, ainda, prorrogar, a qualquer tempo, os prazos para recebimento das propostas e divulgação do resultado, bem como corrigir possíveis erros materiais no documento publicado, mediante errata.

10.2 O foro designado para julgamento de quaisquer questões judiciais resultantes deste Termo de Referência será a Comarca de Vitória – ES.

10.3 Aquele que deixar de entregar ou de apresentar documentação exigida no Termo de Referência, apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal e que, convocado dentro do prazo de validade de sua proposta, não assinar o contrato, ficará sujeito a reparação dos danos causados ao Hospital.

10.4 É vedada a participação no mesmo Termo de Referência de pessoas jurídicas que sejam controladoras, controladas, coligadas ou integrantes de um mesmo grupo econômico.

(IMPRESSÃO EM PAPEL TIMBRADO DA EMPRESA)

(ANEXO I)

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos, para fins de prova, aptidão de desempenho e atestado de execução, que a empresa [**nome da empresa prestadora de serviços/fornecimento de produtos, em negrito**], inscrita no CNPJ sob o nº 00.000.000/0000-00, estabelecida na Rua ....., nº....., bairro ....., na cidade de ....., Estado de ....., prestou serviços à [**nome da empresa contratante, em negrito**], CNPJ nº 00.000.000/0001-00, de [**descrição dos serviços prestados/fornecimento de produtos, especificando o prazo de execução**].

Registramos, ainda, que as prestações dos serviços acima referidos apresentaram bom desempenho operacional, tendo a empresa cumprido fielmente com suas obrigações, nada constando que a desabone técnica e comercialmente, até a presente data.

[cidade], em XX de XXXX de 202X.

_____

Assinatura do responsável legal

[Razão social da empresa]

CNPJ nº xx.xxx.xxx/xxxx-xx

[endereço da empresa, caso não possua papel timbrado]

MINUTA DE CONTRATO

(ANEXO II)

CT: 0xx/202x

CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE ENTRE SI FAZEM A ASSOCIAÇÃO EVANGÉLICA BENEFICENTE ESPÍRITO SANTENSE E (RAZÃO SOCIAL DA CONTRATADA).

CONTRATANTE: ASSOCIAÇÃO EVANGÉLICA BENEFICENTE ESPÍRITO SANTENSE – AEBES, (QUALIFICAÇÃO COMPLETA DO HEUE E REPRESENTANTE LEGAL).

CONTRATADA: (RAZÃO SOCIAL, QUALIFICAÇÃO DA EMPRESA, RESPONSÁVEL LEGAL, QUALIFICAÇÃO DO RESPONSÁVEL), ajustam o presente contrato de prestação de serviços, de acordo com as cláusulas seguintes:

CLÁUSULA PRIMEIRA – DO OBJETO CONTRATUAL

1.1 O presente Termo de Referência tem por objeto a contratação de serviços gerenciados de segurança com características de Antivírus com XDR, contemplando os serviços de instalação, configuração, monitoramento e suporte técnico ilimitado/mês; para o Hospital Estadual de Urgência e Emergência.

SERVIÇOS E PRODUTOS	QTD LICENÇAS
Fornecimento de licenças de uso de solução corporativa de proteção de endpoints de próxima geração com ferramenta de detecção e resposta para estações de trabalho com gerência em nuvem.	320
Fornecimento de licenças de uso de solução corporativa de proteção de endpoints de próxima geração com ferramenta de detecção e resposta para servidores com gerência em nuvem.	15

1.2 Os serviços, objeto deste instrumento, serão realizados pela CONTRATADA, tendo por executores, profissionais plena e legalmente aptos, capacitados e habilitados.

1.3 A CONTRATADA declara para todos os fins de direito estar devidamente habilitada, consoante a legislação regulamentar, para a prestação do serviço ora contratada.

CLÁUSULA SEGUNDA – DAS OBRIGAÇÕES DA CONTRATADA

2.1 A CONTRATADA deverá:

2.1.1 Todos os componentes que fazem parte da solução, de segurança para servidores, estações de trabalho deverão ser fornecidas por um único fabricante. Não serão aceitas composições de produtos de fabricantes diferentes;

2.1.2 A console de monitoração e configuração deverá ser feita através de uma central única, baseada em web e em nuvem, que deverá conter todas a fermentas para a monitoração e controle da proteção dos dispositivos;

2.1.3 A console de nuvem deve possuir o armazenamento de seus dados dentro do território nacional, garantindo conformidade e compliance com as leis locais como a LGPD, Instrução normativa 5 e NC-14 determinada pelo Banco Central;

2.1.4 A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional;

2.1.5 Deve possuir mecanismo de comunicação via API, para integração com outras soluções de segurança, como por exemplo SIEM;

2.1.6 Deve possuir capacidade de realizar a integração com soluções de firewalls para criar políticas automáticas em caso de ataques em massa nos computadores e servidores;

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

2.1.8 Deve permitir sincronização com o Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção.

2.1.9 Deve possuir a possibilidade de aplicar regras diferenciadas baseado em grupos ou usuários;

2.1.10 A instalação deve ser feita via cliente específico por download da gerência central ou também via email de configuração.

2.1.11 Deve a console ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando;

2.1.12 Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;

2.1.13 Deve permitir exclusões de escaneamento para um determinado websites, pastas, arquivos ou aplicações, tanto a nível geral quanto específico em uma determinada política.

2.1.14 A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs;

2.1.15 Atualização incremental, remota e em tempo-real, da vacina dos Antivírus e do mecanismo de verificação (Engine) dos clientes;

2.1.16 Permitir o agendamento da varredura contra vírus com a possibilidade de selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador;

2.1.17 Atualização automática das assinaturas de ameaças (malwares) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador;

2.1.18 Utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados.

2.1.19 As mensagens geradas pelo agente deverão estar no idioma em português ou permitir a sua edição.

2.1.20 Permitir a exportação dos relatórios gerenciais para os formatos CSV e PDF;

2.1.21 Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;

2.1.22 Possibilidade de exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão da engine, data da vacina, data da última verificação, eventos recentes e status;

2.1.23 Capacidade de geração de relatórios, estatísticos ou gráficos, tais como:

2.1.24 Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;

2.1.25 Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, bem como detalhes das varreduras e dos alertas nos computadores;

2.1.26 Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;

2.1.27 Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;

2.1.28 Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;

2.1.29 Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;

2.1.30 Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados.

2.1.31 Deverá possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada;

2.1.32 Deve fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um upload (exemplo Dropbox), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra malwares, procuradas palavras chaves ou informações confidenciais. Deve ser bloqueado o upload ou removida a informação confidencial antes do envio do arquivo;

2.1.33 As portas de comunicação deverão ser configuráveis. A comunicação deverá permitir QoS para controlar a largura de banda de rede.

2.1.34 A solução deverá permitir a seleção da versão do software de preferência, permitindo assim o teste da atualização sobre um grupo de PCs piloto antes de implantá-lo para toda a rede. Permitir ainda selecionar um grupo de computadores para aplicar a atualização para controlar a largura de banda de rede. A atualização da versão deverá ser transparente para os usuários finais.

2.1.35 O agente anti-vírus deverá proteger laptops, desktops e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, trojans, worms e spyware. No Windows o agente também deverá detectar PUA, adware, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso a web;

2.1.36 Deve possuir mecanismo contra a desinstalação do endpoint pelo usuário e cada dispositivo deverá ter uma senha única, não sendo autorizadas soluções com senha única válida para todos os dispositivos;

2.1.37 Deve prover no endpoint a solução de HIPS (Host Instrusion Prevention System) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deverá ser atualizado diariamente;

2.1.38 Deve prover proteção automática contra web sites infectados e maliciosos, assim como previnir o ataque de vulnerabilidades de browser via web exploits;

2.1.39 Deve permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalhao e redes sem fio, estando sempre atrelado ao usuário o controle e não ao dispositivo;

2.1.40 O controle de dispositivos deve ser ao nível de permissão, somente leitura ou bloqueio;

2.1.41 Os seguintes dispositivos deverão ser, no mínimo, gerenciados: HD (hard disks) externos, pendrives USB, storages removíveis seguras, CD, DVD, Blu-ray, floppy drives, interfaces de rede sem fio, modems, bluetooth, infra-vermelho, MTP (Media Transfer Protocol) tais como Blackberry, iPhone e Android smartphone e PTP (Picture Transfer Protocol) como câmeras digitais;

2.1.42 A ferramenta de administração centralizada deverá gerenciar todos os componentes da proteção para estações de trabalho e servidores e deverá ser projetada para a fácil administração, supervisão e elaboração de relatórios dos endpoint e servidores;

2.1.43 Deverá possuir interface gráfica web, com suporte a língua portuguesa (padrão brasileiro);

2.1.44 A Console de administração deve incluir um painel com um resumo visual em tempo real para verificação do status de segurança;

2.1.45 Deverá fornecer filtros pré-construídos que permitam visualizar e corrigir apenas os computadores que precisam de atenção;

2.1.46 Deverá exibir os PCs gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus, etc), e classificar os PCs em conformidade;

2.1.47 Uma vez que um problema seja identificado, deverá permitir corrigir os problemas remotamente, com no mínimo as opções abaixo:

2.1.48 Proteger o dispositivo com a opção de início de uma varredura;

2.1.49 Forçar uma atualização naquele momento;

2.1.50 Ver os detalhes dos eventos ocorridos;

2.1.51 Executar verificação completa do sistema;

2.1.52 Forçar o cumprimento de uma nova política de segurança;

2.1.53 Mover o computador para outro grupo;

2.1.54 Apagar o computador da lista;

2.1.55 Atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente;

2.1.56 Gravar um log de auditoria seguro, que monitore a atividade na console de gerenciamento para o cumprimento de regulamentações, auditorias de segurança, análise e solução de problemas forenses;

2.1.57 Deverá permitir exportar o relatório de logs de auditoria nos formatos CSV e PDF;

2.1.58 Deve conter vários relatórios para análise e controle dos usuários e endpoints. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas para os endpoints;

2.1.59 Fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:

2.1.60 Nome do dispositivo;

2.1.61 Início da proteção;

2.1.62 Último usuário logado no dispositivo;

2.1.63 Último update;

2.1.64 Último escaneamento realizado;

2.1.65 Status de proteção do dispositivo;

2.1.66 Grupo a qual o dispositivo faz parte;

2.1.67 Permitir a execução manual de todos estes relatórios danos formatos CSV e PDF;

2.1.68 A console deve possuir métodos de verificação da saúde das configurações da console, possibilitando aos administradores descobrirem facilmente se existe alguma falha de configuração que pode facilitar a entrada de malwares e invasores no ambiente;

2.2 CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO

2.2.1 Características básicas do agente de proteção contra malwares:

2.2.2 Pré-execução do agente para verificar o comportamento malicioso e detectar malware desconhecido;

2.2.3 O agente deve buscar algum sinal de malware ativo e detectar malwares desconhecidos;

2.2.4 O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças;

2.2.5 O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;

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

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

2.2.8 Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

2.2.9 Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

2.2.10 Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

2.2.11 Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;

2.2.12 É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);

2.2.13 Suportar máquinas com arquitetura 32-bit e 64-bit, (Exceto para Windows 11 que não há opção de 32bits;

2.2.14 O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais, macOS 11 Big Sur, 12 Monterey, 13 Ventura, Microsoft Windows 7, 8.1, 10 e 11;

2.2.15 A solução deve ser compatível com a execução nativa em processadores Apple Silicon, não serão aceitas soluções que dependem de emulação via Rosetta2 da Apple.

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

2.2.17 Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;

2.3 FUNCIONALIDADE DE FIREWALL E DETECÇÃO E PROTEÇÃO DE INTRUSÃO (IDS\IPS) COM AS FUNCIONALIDADES:

2.3.1 Deverá possui atualização periódica de novas assinaturas de ataque;

2.3.2 Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

2.3.3 Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;

2.3.4 Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

2.3.5 Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

2.3.6 Deve possuir técnicas de proteção, que inclui:

2.3.7 Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

2.3.8 Algorítimo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;

2.39 Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

2.40 Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

2.41 Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

2.4 FUNCIONALIDADE DE ANTIVÍRUS E ANTISPYWARE:

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

2.4.2 Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

2.4.3 As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;

2.4.4 Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;

2.4.5 Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário;

2.4.6 Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;

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

2.4.8 A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

2.4.9 Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

2.4.10 Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;
2.4.11 Antivírus de Web (verificação de sites e downloads contra vírus);
2.4.12 Controle de acesso a sites por categoria;
2.4.13 Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador web, de forma independente do navegador usado, ou seja, sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.
2.4.14 O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;
2.4.15 Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;
2.4.16 Capacidade de verificar somente arquivos novos e alterados;
2.4.17 Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

2.5 FUNCIONALIDADE DE DETECÇÃO PRÓ-ATIVA DE RECONHECIMENTO DE NOVAS AMEAÇAS:

2.5.1 Funcionalidade de detecção de ameaças via técnicas de machine learning;
2.5.2 Funcionalidade de detecção de ameaças desconhecidas que estão em memória;
2.5.3 Capacidade de detecção, e bloqueio pró-ativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);
2.5.4 Capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória;
2.5.5 Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

2.6 FUNCIONALIDADE DE PROTEÇÃO CONTRA RANSOMWARES:

2.6.1 Para estações de trabalho, dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;
2.6.2 Para estações de trabalho, dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;
2.6.3 Para servidores, dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;
2.6.4 A solução deverá previnir ameaças e interromper que eles sejam executados em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas.
2.6.5 Deve possuir uma tecnologia anti-exploit baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de malware, protegendo os endpoints de ameaças desconhecidas e vulnerabilidades *zero-day*.

2.6.6 Deve ser realizada a detecção e o bloqueio de, pelo menos, as seguintes técnicas de exploit:

2.6.7 DEP (*Data Execution Prevention*);

2.6.8 *Address Space Layout Randomization* (ASLR);

2.6.9 *Bottom Up ASLR*;

2.6.10 *Null Page*;

2.6.11 *Anti-HeapSpraying*;

2.6.12 *Dynamic Heap Spray*;

2.6.13 *Import Address Table Filtering (IAF)*;

2.6.14 *VTable Hijacking*;

2.6.15 *Stack Pivot and Stack Exec*;

2.6.16 *SEHOP*;

2.6.17 *Stack*-based ROP (*Return-Oriented Programming*);

2.6.18 *Control-Flow Integrity (CFI)*;

2.6.19 *Syscall*;

2.6.20 *WOW64*;

2.6.21 *Load Library*;

2.6.22 *Shellcode*;

2.6.23 *VBScript God Mode*;

2.6.24 *Application Lockdown*;

2.6.25 *Process Protection*;

2.6.26 *Network Lockdown*.

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

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

2.6.29 A console de monitoração e configuração deverão ser feitas através de uma central única, baseada em web e em nuvem, que deverá conter todas a ferramentes para a monitoração e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware.

2.6.30 A console deverá apresentar *Dashboard* com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo ransomware nos endpoints.

2.7 SOLUÇÃO DE ENDPOINT DETECTION AND RESPONSE (EDR)

2.7.1 A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando

2.7.2 detecção e investigação nos endpoints com atividades suspeitas;

2.7.3 Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.

2.7.4 Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.

2.7.5 Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

2.7.6 Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;

2.7.7 Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

2.7.8 Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;

2.7.9 Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;

2.7.10 A solução de EDR deverá ser integrado ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

2.7.11 O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;

2.7.12 Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;

2.7.13 Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;

2.7.14 Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;

2.7.15 Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

2.7.16 Deve possibilizar o agendamento de consultas (queries);

2.7.17 Deve reter os dados no Data Lake por no mínimo 7 dias.

2.8 FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES E DISPOSITIVOS:

2.8.1 Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;

2.8.2 Atualiza automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada;

2.8.3 Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;

2.8.4 Oferecer proteção para chaves de registro e controle de processos;

2.8.5 Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo;

2.8.6 Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;

2.8.7 Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;

2.8.8 Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;

2.8.9 Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;

2.8.10 As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;

2.8.11 Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

2.8.12 A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;

2.8.13 Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

2.8.13.1 Permitir que todos os dispositivos do mesmo modelo;

2.8.13.2 Permitir que um único dispositivo com base em seu número de identificação único;

2.8.13.3 Permitir o acesso total;

2.8.13.4 Permitir acesso somente leitura;

2.8.14 Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

2.9 FUNCIONALIDADE DE PROTEÇÃO E PREVENÇÃO A PERDA DE DADOS

2.9.1 Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo**;**

2.9.2 Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

2.9.3 Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

2.9.4 Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

2.9.4.1 Números de cartões de crédito;

2.9.4.2 Números de contas bancárias;

2.9.4.3 Números de Passaportes;

2.9.4.4 Endereços;

2.9.4.5 Números de telefone;

2.9.4.6 Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, etc;

2.9.4.7 Lista de e-mails;
2.9.4.8 Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários, etc;
2.9.5 Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;
2.9.6 Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.
2.9.7 Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;
2.9.8 Permitir o controle de dados para no mínimo os seguintes meios:
2.9.8.1 Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);
2.9.8.2 Anexado no navegador (ao menos IE, Firefox e Chrome);
2.9.8.3 Anexado no cliente de mensagens instantâneas (ao menos Skype);
2.9.8.4 Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

2.10 CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA SERVIDORES

2.10.1 A solução deverá ser capaz de proteger servidores contra malwares, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores;
2.10.2 Deve realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos;
2.10.3 O agente host deve buscar algum sinal de malwares ativos e detectar malwares desconhecidos;
2.10.4 O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;
2.10.5 A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;
2.10.6 Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;
2.10.7 Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;
2.10.8 Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);
2.10.9 Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;
2.10.10 Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;
2.10.11 É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);
2.10.12 O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais abaixo:
2.10.12.1 Versões sevidores tais como Windows Server 2008,2012,2016 e 2019
2.10.12.2 Versões desktop tais como Windows7, 8 e Windows 10
2.10.12.3 CentOS 7;
2.10.12.4 Debian 10;
2.10.12.5 Oracle Linux 7;
2.10.12.6 Oracle Linux 8;
2.10.12.7 Red Hat Enterprise 7;
2.10.12.8 Red Hat Enterprise 8;
2.10.12.9 Red Hat Enterprise 9;
2.10.12.10 SUSE Linux Enterprise Server 12;

2.10.12.11 SUSE Linux Enterprise Server 15;
2.10.12.12 Ubuntu 20.04 LTS;
2.10.12.13 Ubuntu 22.04 LTS;

2.10.13 Deve suportar o uso de servidores usados para atualização em cache para diminuir a largura de banda usada nas atualizações;
2.10.14 Deve possuir integração com as nuvens da Microsoft Azure e Amazon Web Services para identificar as informações dos servidores instanciados nas nuvens;
2.10.15 Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;
2.10.16 Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;
2.10.17 Deve possuir funcionalidades de tecnologias conhecidas como CWPP – Cloud Workload Protection Plataform, permitindo que seja possível trazer funcionalidades de próxima geração para cargas de trabalho em nuvem, bem como containers, e afins;
2.10.18 A solução deve no mínimo, utilizar o modelo de sensores para containers, garantindo visibilidade e proteção de, no mínimo, estes tipos de ataques:
2.10.18.1 Escalação de privilégios dentro de containers;
2.10.18.2 Programas utilizando técnicas de mineração de criptomoedas;
2.10.18.3 Detecção de atacantes tentando destruir evidências de ambientes comprometidos (IOC – Indicator of compromise);
2.10.18.4 Detecção de funções internas do kernel que estão sendo adulteradas em um host;
2.10.19 A solução deve também se integrar à tecnologias de CSPM – Cloud Security Posture Management, tendo como objetivo trazer funcionalidades de análises integradas de CWPP e CSPM a fim de melhorar a visibilidade e resposta à incidentes em ambientes de nuvem públicas,

2.11 FUNCIONALIDADE DE FIREWALL E DETECÇÃO E PROTEÇÃO DE INTRUSÃO (IDS\IPS) COM AS FUNCIONALIDADES:

2.11.1 Possuir proteção contra exploração de buffer overflow;
2.11.2 Deverá possui atualização periódica de novas assinaturas de ataque;
2.11.3 Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.
2.11.4 Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;
2.11.5 Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.
2.11.6 Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.
2.11.7 Deve possuir técnicas de proteção, que inclui:
2.11.7.1 Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;
2.11.7.2 Algoritmo correspondente **padrão** - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;

2.11.7.3 Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

2.11.7.4 Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

2.11.7.5 Verificação de ameaças web avançadas**:** bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

2.12 FUNCIONALIDADE DE ANTIVÍRUS E ANTISPYWARE:

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

2.12.3 Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

2.12.4 As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;

2.12.5 Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;

2.12.6 Permitir a varredura das ameaças da maneira manual, agendada e em tempo real nos servidores;

2.12.7 Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;

2.12.8 Capacidade de detectar arquivos através da reputação dos mesmos;

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

2.12.10 A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

2.12.11 Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

2.12.12 Deverá detectar tráfego de rede para comandar e controlar os servidores;

2.12.13 Proteger arquivos de documento contra ataques do tipo ransomwares;

2.12.14 Proteger que o ataque de ransomware seja executado remotamente;

2.12.15 Permitir o envio de amostras de malwares para a nuvem de inteligência do fabricante;

2.12.16 Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

2.12.17 Antivírus de Web (verificação de sites e downloads contra vírus);

2.12.18 Controle de acesso a sites por categoria;

2.12.19 Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

2.12.20 O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;

2.12.21 Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;
2.12.22 Capacidade de verificar somente arquivos novos e alterados;
2.12.23 Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.
2.12.24 Capacidade de habilitar mensagens de desktop para a Proteção contra Ameaças;
2.12.25 Capacidade de adicionar exclusão de varredura para arquivos, pastas, processos, sites, aplicativos e tipos de explorações detectadas;

2.13 FUNCIONALIDADE DE PROTEÇÃO CONTRA RANSOMWARES:

2.13.1 Deve dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;
2.13.2 Deve dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;
2.13.3 Deve dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;

2.14 FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES E DISPOSITIVOS:

2.14.1 Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;
2.14.2 Atualiza automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada;
2.14.3 Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;
2.14.4 Oferecer proteção para chaves de registro e controle de processos;
2.14.5 Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo;
2.14.6 Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;
2.14.7 Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;
2.14.8 Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;
2.14.9 Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;
2.14.10 As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;
2.14.11 Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
2.14.12 A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;

2.14.13 Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

2.14.13.1 Permitir que todos os dispositivos do mesmo modelo;

2.14.13.2 Permitir que um único dispositivo com base em seu número de identificação único;

2.14.13.3 Permitir o acesso total;

2.14.13.4 Permitir acesso somente leitura;

2.14.14 Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

2.15 FUNCIONALIDADE DE PROTEÇÃO E PREVENÇÃO A PERDA DE DADOS

2.15.1 Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;

2.15.2 Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

2.15.3 Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

2.15.4 Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

2.15.4.1 Números de cartões de crédito;

2.15.4.2 Números de contas bancárias;

2.15.4.3 Números de Passaportes;

2.15.4.4 Endereços;

2.15.4.5 Números de telefone;

2.15.4.6 Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, etc;

2.15.4.7 Lista de e-mails;

2.15.4.8 Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários, etc;

2.15.5 Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;

2.15.6 Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

2.15.7 Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

2.15.8 Permitir o controle de dados para no mínimo os seguintes meios:

2.15.8.1 Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);

2.15.8.2 Anexado no navegador (ao menos IE, Firefox e Chrome);

2.15.8.3 Anexado no cliente de mensagens instantâneas (ao menos Skype);

2.15.8.4 Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

2.16 SOLUÇÃO DE ENDPOINT DETECTION AND RESPONSE (EDR)

2.16.1 A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;

2.16.2 Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.

2.16.3 Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.

2.16.4 Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

2.16.4.1 Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;

2.16.4.2 Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

2.16.4.3 Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;

2.16.4.4 Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;

2.16.5 A solução de EDR deverá ser integrado ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

2.16.6 O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;

2.16.7 Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;

2.16.8 Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;

2.16.9 Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;

2.16.10 Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

2.16.10.1 Deve possibilizar o agendamento de consultas;

2.16.10.2 Deve reter os dados no Data Lake por no mínimo 7 dias.

2.17SOLUÇÃO DE EXTENDED DETECTION AND RESPONSE (XDR)

2.17.1 Deve possuir Data Lake que armazene informações críticas de endpoints e servidores, mas também incorporando dados de outras soluções de segurança como firewalls, e-mail gateways, public cloud e mobile, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

2.17.2 Deve possuir recurso de pesquisa estruturada em banco de dados compatível com SQL, ou similar;

2.17.3 Deve disponibilizar recurso de pesquisa para comparar os indicadores de comprometimento de várias fontes de dados para identificar rapidamente um ataque suspeito;

2.17.4 Deve utilizar detecções de ATP e IPS do firewall para investigar endpoints suspeitos;

2.17.5 Deve disponibilizar pontos de aplicação que permitem a executar ações, como colocar em quarentena um endpoint comprometido, bloquear o tráfego de rede ou remover malware;

2.17.6 Deve possuir sensores que fornecem telemetria de diferentes aspectos da infraestrutura de TI, capazes de identificar dispositivos não gerenciados e desprotegidos em toda o ambiente da organização;

2.17.7 Deve possibilitar o agendamento de consultas (queries) cíclicas no Data Lake para identificação de IoCs em execuções antecipadas;

2.17.8 Deve permitir a integração via APIs com sistemas e fluxos de trabalhos já existentes;

2.17.9 Deve reter os dados no Data Lake por no mínimo 30 dias.

2.17.10 O XDR deve permitir integração com sistemas de terceiros, no mínimo, tecnologias como Office 365 e produtos de CSPM para visibilidade e correlação de eventos em ambientes de Cloud como Azure, AWS e Google Cloud;

2.17.11 A console do XDR deve correlacionar os dados recebidos e armazenados no DataLake e gerar evidências de ataques ou eventos suspeitos existentes dentro do ambiente;

2.17.12 Tais detecções e evidencias devem conter todos os detalhes do evento, bem como uma análise do próprio fabricante sobre a classificação de risco de tal evento;

2.17.13 Deve possibilitar também que investigações sejam realizadas a partir destes eventos, coletando dados e executando consultas dentro do Datalake ou nos próprios dispositivos a fim de coletar mais evidências para determinar a realidade do ataque presente na console;

2.17.14 Deve possuir console para gerenciamento de investigações, podendo adicionar de forma automática ou manual, diversos eventos e detecções encontradas na console;

2.17.15 A console de gerenciamento de investigações deve permitir atribuir analistas que acompanharão a investigação;

2.17.16 Será necessário também que exista uma trilha de auditoria para cada investigação, de tal forma que os administradores da console consigam auditar os detalhes da condução da investigação;

2.18 SLA PARA ATENDIMENTO

2.18.1 A CONTRATADA deverá cumprir prazos máximos para respostas aos acionamentos, de acordo com o nível de severidade de cada chamado, conforme detalhado seguir, onde as horas definidas são corridas a partir da abertura do chamado de atendimento (solicitação e incidente).

Estado do Ambiente	Tipo	Tipo de Chamado	Tempo para primeiro Atendimento	Tempo para solução de contorno ou definitiva
Parado	Crítico	Incidente	30 minutos corridos	2 horas corridas
Intermitente	Alerta	Incidente	1 hora corrida	4 horas corridas
Operando	Ações preventivas, criação e alteração de novas regras e pequenos ajustes de configuração (de baixo impacto)	Solicitação	4 horas úteis	12 horas úteis
Informacional	Esclarecimento de dúvidas, consultas técnicas, criação de relatórios e análise de vulnerabilidades	Solicitação	4 horas úteis	24 horas úteis

2.19 ABERTURA DE CHAMADOS

a) Deverá ser possível a abertura de chamado técnico (Solicitações de Atendimento) via ferramenta WEB, telefone (fixo ou celular), e-mail.

b) O registro via ferramenta WEB será à principal forma de abertura de chamados (Solicitações de Atendimento) e de relacionamento técnico entre o CONTRATANTE e a CONTRATADA.

c) A empresa CONTRATADA deverá disponibilizar funcionalidade de internet para registro de chamados (Solicitações de Atendimento), devendo esta ferramenta ser capaz de gerenciar todo o ciclo de atendimento, desde a solicitação até o encerramento do atendimento. Alternativamente, a empresa atenderá a Solicitações de Atendimento através de e-mail, devendo a CONTRATADA gerenciar a troca de e-mails de forma a permitir o acompanhamento de todo o ciclo de atendimento.

d) A CONTRATADA deverá responsabilizar-se e permitir o registro de todos os fatos e dados a partir do recebimento das Solicitações de Atendimento nesta ferramenta WEB, de maneira a evidenciar as variáveis para atendimento e posterior faturamento dos serviços.

2.20 OS SERVIÇOS DE SUPORTE ESPECIALIZADO SOLUÇÃO DE ANTIVÍRUS NO MÍNIMO, AS SEGUINTES ATIVIDADES:

a) Execução de serviços de suporte, disponível durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

b) A CONTRATADA deverá manter em regime de sobreaviso, em regime de 24x7, profissionais especializados nas atividades inerentes ao serviço de suporte especializado. Nas situações de sobreaviso, a CONTRATADA deverá disponibilizar aos técnicos contratados os mecanismos tecnológicos (tais como telefones celulares, telefones fixos, e-mails ou outros), que permitam o acionamento nos casos de necessidade, sem ônus adicional para a CONTRATANTE.

c) Os serviços de suporte especializado serão executados preferencialmente de forma remota a partir das dependências da CONTRATADA, onde os técnicos ficarão alocados, exceto quando a presença do técnico nas dependências da CONTRATANTE for indispensável.

2.21 A CONTRATADA executará as atividades com autonomia, cabendo a CONTRATANTE a fiscalização do cumprimento do contrato, de forma assegurar a execução do contrato.

2.22 A CONTRATADA se obriga pelo sigilo das informações e nem poderá tornar-se de conhecimento de terceiros, por constituir falta grave e falta de ética dos serviços prestados por parte da CONTRATADA.

2.23 Fornecer à CONTRATANTE todas as informações necessárias à plena execução do serviço contratado.

2.24 Realizar os serviços conforme preceitua o objeto deste contrato, nos locais e condições que melhor atenderem às necessidades e conveniências da CONTRATANTE.

2.25 Requerer a exclusão da CONTRATANTE, individual ou coletivamente, no polo passivo dos eventuais processos judiciais ou administrativos em que a CONTRATADA deu causa, na ocorrência de ação contra a CONTRATANTE, ou qualquer outro ato de natureza administrativa ou judicial, que venha a ser proposto contra a CONTRATANTE, seja a que título for e a que tempo ocorrer, em virtude do presente contrato. A CONTRATADA concorda ainda, desde já, que a CONTRATANTE denuncie à lide ou chame ao processo, se necessário, a CONTRATADA, na forma do artigo 125 do Código de Processo Civil.

2.26 Responsabilizar-se por todos os riscos e despesas decorrentes da contratação de funcionários utilizados na execução do presente contrato, bem como se responsabilizando quanto ao comportamento e eficiência deles, devendo a CONTRATADA substituir em 24 (vinte e quatro) horas, o profissional que não atender às necessidades descritas neste contrato e seus respectivos aditivos e anexos e/ou que não atenda aos princípios da ética, bem como das normas vigentes da Instituição, afastando-o de forma imediata de todas as unidades geridas pela AEBES.

2.27 Não admitir e nem aliciar qualquer empregado que esteja à disposição da CONTRATANTE ou que integre o seu quadro de pessoal.

2.28 Manter, durante a execução do contrato, em compatibilidade com as obrigações assumidas pela CONTRATADA, todas as condições de qualificação, habilitação técnica, jurídica, bem como de regularidade fiscal e trabalhista, exigidas no momento da assinatura deste contrato.

2.29 Manter em condições legais as contribuições trabalhistas e previdenciárias do(s) profissional (s) recrutado(s) para executar os serviços objeto deste contrato.

2.30 A CONTRATADA se obriga em prestar os serviços, objeto deste contrato, observando prazo, qualidade e zelo dos serviços.

2.31 Assumir integralmente a responsabilidade por danos causados à CONTRATANTE ou a terceiros, decorrentes de negligência, imprudência ou imperícia na execução dos serviços contratados.

2.32 Cumprir integralmente todas as obrigações relativas à Segurança do Trabalho utilizando dos equipamentos de proteção individual (EPI'S) necessários à execução dos serviços objeto deste contrato, apresentando os documentos, conforme portaria 3.214/78 do Ministério do Trabalho, a Consolidação das Leis do Trabalho e demais órgãos fiscalizadores.

2.33 Fornecer sempre que forem solicitados, mantendo atualizado junto a CONTRATANTE, os seguintes documentos: cópia do Contrato Social e suas alterações, certidões de regularidade e responsabilidade técnica de conselho regulador, caso tenha, e eventuais alvarás inerentes as atividades prestadas.

2.34 Em caso de descumprimento das obrigações, a CONTRATANTE se reserva no direito de emitir notificação de descumprimento contratual à CONTRATADA, e, em havendo reincidência, caberá imposição de multa, progressivamente até o limite de 10% (dez por cento) do valor do contrato.

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DA CONTRATANTE

3.1 A CONTRATANTE deverá:

a) Para à intervenção remota nos equipamentos de TI da CONTRATANTE, as estações de trabalho dos técnicos deverão estar equipadas com recursos de controle remoto, mediante autenticação e autorização do usuário, estando estes recursos obrigatoriamente acessíveis à equipe de Infraestrutura de TI;

b) Acompanhar, fiscalizar e avaliar a prestação do serviço objeto deste Contrato;

c) Comunicar oficialmente à CONTRATADA, quaisquer falhas verificadas no cumprimento deste Contrato.

d) Facilitar o acesso da CONTRATADA para a consecução do objeto deste Contrato.

e) Pagar à CONTRATADA o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste instrumento.

3.2 Estando o objeto do presente contrato de prestação de serviços, diretamente vinculado e relacionado ao Contrato de Gestão e Operacionalização do Hospital Estadual de Urgência e Emergência, firmado entre a CONTRATANTE e a

SECRETARIA ESTADUAL DE SAÚDE DO ESTADO DO ESPÍRITO SANTO, obriga-se a CONTRATANTE a efetuar o pagamento do valor devido à CONTRATADA, conforme cláusula de pagamento, contados do efetivo recebimento dos recursos financeiros, quer oriundo do Estado ou da União. Para tanto, observada a necessidade prévia da emissão de Nota Fiscal de Serviços pela CONTRATADA, que não poderá em nenhuma hipótese efetuar faturamento direto de quaisquer procedimentos a outro CONTRATANTE ou tomador eventual de serviços, incluindo o poder público, sendo esta prerrogativa exclusiva da CONTRATANTE no âmbito do Hospital Estadual de Urgência e Emergência, neste Estado do Espírito Santo.

3.3 Fornecer e permitir acesso a todas as informações pertinentes e necessárias ao bom andamento dos serviços a serem desenvolvidos pela CONTRATADA, assim como quaisquer outras informações que tão somente digam respeito às atividades da CONTRATADA.

3.4 Fiscalizar o presente contrato, cabendo verificar se as obrigações assumidas contratualmente estão sendo cumpridas.

3.5 Efetuar os pagamentos devidos à CONTRATADA decorrente da prestação de serviços, de acordo com o disposto na cláusula de pagamento deste instrumento.

3.6 Notificar a CONTRATADA em caso de descumprimento das suas obrigações contratuais.

CLÁUSULA QUARTA – DA REMUNERAÇÃO

4.1 A CONTRATANTE pagará à CONTRATADA pelos serviços prestados, (conforme proposta comercial).

4.2 Por ocasião dos pagamentos serão efetuados os descontos legais por tributos que incidam ou venham a incidir sobre a prestação do serviço contratado e efetivamente executado.

4.3 O pagamento será efetuado, mensalmente, em até 15 (quinze) dias, posterior ao envio da Nota Fiscal.

4.4 É expressamente vedado a qualquer das partes desconto ou cobrança de duplicata através de rede bancária ou de terceiros, bem como a cessão de crédito dos valores objetos deste contrato ou sua dação em garantia.

4.5 Os reajustes contratuais serão negociados entre as partes, estando eventual concessão, limitado ao prévio reajuste autorizado pela Secretaria de Saúde do Espírito Santo.

CLÁUSULA QUINTA – DO PRAZO CONTRATUAL

5.1 O prazo de vigência do presente contrato será por 60 (sessenta) meses, contados a partir da data da assinatura do Contrato, conforme Contrato de Gestão, firmado entre a Contratante e Secretaria Estadual de Saúde do Estado Do Espírito Santo - SESA, ressalvando os casos de rescisão previstos na cláusula sexta.

5.2 Qualquer alteração contratual deverá ser feita mediante termo aditivo.

CLÁUSULA SEXTA – DA RESCISÃO CONTRATUAL

6.1 O presente contrato poderá ser rescindido por acordo entre as partes, mediante celebração de "Distrato" ou unilateralmente, de forma imotivada, pela CONTRATANTE, concedendo-se, à CONTRATADA, aviso prévio de 30 (trinta) dias sendo que, nesta hipótese, não será devido qualquer tipo de multa, à parte que solicitar a rescisão.

6.2 Havendo rescisão do contrato pela CONTRATANTE, e havendo cumprimento de aviso prévio, a CONTRATADA deverá deixar de efetuar a prestação de serviço no último dia de vigência do aviso prévio, sob pena de multa diária equivalente a 10% do valor do contrato.

6.3 A CONTRATADA poderá rescindir o contrato unilateralmente, de forma imotivada, concedendo-se à CONTRATANTE, aviso prévio de 60 (sessenta) dias, de modo a evitar a desassistência e, consequentemente, assegurar o interesse público, sob pena de multa diária equivalente a 10% do valor do contrato.

6.4 O presente contrato poderá, ainda, ser rescindido unilateralmente, por qualquer uma das partes, sem concessão de aviso prévio na ocorrência de uma das seguintes situações:

a) Justo Motivo, decorrente de condutas que levem a quebra de confiança;
b) Falência, recuperação judicial, e insolvência de qualquer uma das partes.
c) Descumprimento de qualquer cláusula ou condição estabelecida este contrato;
d) Negligência, imprudência, imperícia, incapacidade, dolo ou má-fé por parte da CONTRATADA ou dos profissionais no desempenho dos serviços contratados.

6.5 Este contrato será imediatamente rescindido no caso de encerramento do Contrato de Gestão do Hospital Estadual de Urgência e Emergência, hipótese em que a AEBES não poderá ser responsabilizada ao pagamento de indenizações ou multas de qualquer natureza.

CLÁUSULA SÉTIMA – DA LEI ANTICORRUPÇÃO

7.1 A CONTRATADA declara conhecer as normas de prevenção à corrupção prevista na legislação brasileira, a Lei nº 12.846/2013 e seus regulamentos e se compromete a cumpri-las fielmente, por si e por seus sócios, administradores e colaboradores. Ainda, se obrigada a CONTRATADA, no exercício dos direitos e obrigações previstos neste Contrato e no cumprimento de qualquer uma de suas disposições: **(i)** não dar, oferecer ou prometer qualquer bem de valor ou vantagem de qualquer natureza a agentes públicos ou a pessoas a eles relacionadas ou ainda quaisquer outras pessoas, empresas e/ou entidades privadas, com o objetivo de obter vantagem indevida, influenciar ato ou decisão ou direcionar negócios ilicitamente e **(ii)** adotar as melhores práticas de monitoramento e verificação do cumprimento das leis anticorrupção, com o objetivo de prevenir atos de corrupção, fraude, práticas ilícitas ou lavagem de dinheiro por seus sócios, administradores, colaboradores e/ou terceiros por elas contratados. A comprovada violação de qualquer das obrigações previstas nesta cláusula é causa para a rescisão unilateral deste Contrato, sem prejuízo da cobrança das perdas e danos causados à parte inocente.

CLÁUSULA OITAVA – DO CÓDIGO DE CONDUTA

8.1 A CONTRATADA se obriga a adotar conduta justa e ética, respeitando as diretrizes estabelecidas no Código de Conduta da CONTRATANTE, disponível no endereço eletrônico https://www.evangelicovv.com.br/aebes/codigo-conduta, o qual desde já declara conhecer e estar vinculada.

8.2 A CONTRATADA se compromete, ainda, a treinar seus Colaboradores alocados na execução das atividades deste Contrato, a fim de instruí-los sobre o cumprimento obrigatório das diretrizes contidas no Código de Conduta da CONTRATANTE para a execução do objeto deste instrumento.

CLÁUSULA NONA – DA PROTEÇÃO DE DADOS PESSOAIS NA RELAÇÃO CONTROLADOR E OPERADOR

9.1 Para fins deste contrato, são considerados:

I. “DADOS PESSOAIS”: qualquer informação relativa a uma pessoa natural (TITULAR DE DADOS) que é capaz de identificá-la de forma direta ou indireta, como por exemplo um nome, número de CPF e RG, endereço residencial, dados de localização, ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social de uma pessoa.

II. “DADOS PESSOAIS SENSÍVEIS”: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

III. “TRATAMENTO”: qualquer operação ou conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

IV. “CONTROLADOR”: parte que determina as finalidades e os meios de tratamento de dados pessoais.

V. “OPERADOR”: parte que trata dados pessoais de acordo com as instruções do CONTROLADOR.

VI. “AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS”: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

9.2 DEFINIÇÃO DAS FUNÇÕES

Esta cláusula aplica-se ao tratamento de dados pessoais, dentro do âmbito da Lei Geral de Proteção de Dados Pessoais - LGPD, pelo OPERADOR em nome do CONTROLADOR.

Para os propósitos deste contrato, as partes supra qualificadas, concordam que a AEBES é o CONTROLADOR dos dados pessoais e a CONTRATADA é o OPERADOR de tais dados, dentro da relação negocial entre as partes.

As PARTES declaram ter conhecimento da Lei 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais - LGPD") e das demais legislações vigentes sobre Proteção de dados pessoais, e se comprometem a cumprir com todas as obrigações legais e contratuais relacionadas às Operações de Tratamento de Dados Pessoais e à proteção, sigilo e privacidade de Dados Pessoais, adotando as medidas técnicas e administrativas cabíveis visando sua conformidade com a privacidade, exigindo de

seus colaboradores; prestadores de serviços e fornecedores o mesmo nível aceitável de segurança da informação e confidencialidade, com base nas melhores práticas de mercado.

9.3 OBRIGAÇÕES DO CONTROLADOR

O CONTROLADOR deve:

Implementar medidas técnicas e organizacionais apropriadas para assegurar e demonstrar que o tratamento é realizado de acordo com a LGPD. Essas medidas devem ser revistas e atualizadas sempre que necessário.

Implementar medidas técnicas e organizacionais apropriadas para garantir que, somente os dados pessoais necessários para cada propósito específico sejam tratados. Essa obrigação se aplica à quantidade de dados pessoais coletados, à extensão do tratamento, ao período de armazenamento e à acessibilidade, sempre observando os princípios e fundamentos da LGPD.

Orientar ao OPERADOR, quanto às medidas e limites para o tratamento de dados pessoais, a fim de garantir que o tratamento seja realizado dentro dos padrões técnicos e legais, garantindo a proteção dos dados pessoais tratados pelas partes.

9.4 OBRIGAÇÕES DO OPERADOR

O OPERADOR deve:

Tratar os dados pessoais somente de acordo com as instruções documentadas do CONTROLADOR.

Tratar apenas os dados pessoais e dados pessoais sensíveis estritamente necessárias para atendimento da finalidade/objeto expressamente previsto neste contrato e em observância das regras específicas previstas na Lei nº 13.709/1918 (“LGPD”).

É vedado ao OPERADOR a realização de imagens dos pacientes sem seu respectivo consentimento, sob pena de rescisão do presente instrumento contratual, bem como ressarcimento de todo e qualquer eventual prejuízo sofrido pelo CONTROLADOR, incluindo multas, condenações judiciais, honorários advocatícios e demais penalidades pecuniárias previstas pela legislação vigente.

Manter o sigilo absoluto de todas as informações e dados pessoais a que tenham acesso e garantir que as pessoas autorizadas para o tratamento dos dados pessoais estejam comprometidas com a confidencialidade, em razão da função ou estão sob obrigação contratual.

Adotar todas as ações necessárias para implementar medidas técnicas e organizacionais apropriadas para assegurar um nível de segurança adequado ao risco aos direitos e liberdades das pessoas.

Respeitar as condições de contratação de terceiros, sendo que o OPERADOR não pode contratar outro OPERADOR (Sub Operador) para processamento de dados sem a prévia autorização do CONTROLADOR.

Em caso de requisição de titulares, fica à cargo do CONTROLADOR responder ao titular de dados pessoais, devendo o OPERADOR (i) se abster de responder diretamente ao titular; (ii) notificar ao CONTROLADOR, imediatamente, caso requisitada; e (iii) cooperar e fornecer todas as informações necessárias para a efetivação dos direitos do titular.
Auxiliar o CONTROLADOR a garantir o cumprimento das obrigações relacionadas à segurança do tratamento, Violações de dados pessoais, avaliações de impacto de proteção de dados e plano de resposta à incidentes;

Informar o CONTROLADOR imediatamente, a ocorrência de incidente de segurança relativo ao tratamento de dados pessoais que possa acarretar risco ou dano relevante a esses titulares;

Indenizar o CONTROLADOR por quaisquer perdas e danos devidamente apurados e comprovados (incluindo multas, custos ou despesas e desembolsos legais) incorridos pelo OPERADOR em decorrência de qualquer violação de Dados Pessoais, nos termos da LGPD, por ato ou omissão em conexão com a execução deste Contrato.

Excluir ou devolver todos os dados pessoais ao CONTROLADOR após o término da prestação dos serviços relacionados ao tratamento, e excluir as cópias existentes, a menos que a lei aplicável exija o armazenamento destes dados.

Disponibilizar ao CONTROLADOR todas as informações imprescindíveis para demonstrar o cumprimento das obrigações estabelecidas na LGPD, sempre que necessário.

9.5 VIGÊNCIA DO CONTRATO E LEGISLAÇÃO APLICÁVEL

Este Contrato continuará em vigor enquanto o OPERADOR estiver tratando dados pessoais em nome do CONTROLADOR e será regido pela LGPD e demais legislações de proteção de dados pessoais e privacidade, bem como as normas aplicáveis ao negócio das partes.

CLÁUSULA DÉCIMA – DAS DISPOSIÇÕES GERAIS

10.1 O presente contrato é documento único que regula os direitos e obrigações entre as partes com relação aos serviços contratados, ficando cancelado qualquer outro acordo porventura existente.

10.2 É vedada a transferência deste contrato para terceiros sem a anuência expressa da CONTRATANTE.

10.3 A CONTRATADA obriga-se a comunicar à CONTRATANTE, por escrito, qualquer alteração que pretenda fazer em seu quadro funcional ou societário que implique substituição de membro(s) da equipe que efetivamente realize a prestadora dos serviços objeto do contrato.

10.4 Caso a CONTRATANTE venha a ser acionada judicialmente em razão de negligência, imprudência, imperícia, incapacidade, dolo ou má-fé, ou ainda, por descumprimento de qualquer cláusula ou condição prevista neste instrumento, por parte da CONTRATADA, esta, obriga-se a responder regressivamente pelos prejuízos causados.

10.5 A tolerância quanto a eventuais infrações do presente contrato não constituirá novação ou renúncia dos direitos conferidos a ambas as partes e/ou aos seus sucessores.

10.6 A CONTRATADA declara que não realizará nenhum investimento para prestação de serviço, objeto deste contrato.

CLÁUSULA DÉCIMA PRIMEIRA – DO FORO DE ELEIÇÃO

11.1 Fica eleito o Foro da Comarca de Vitória, Estado do Espírito Santo, para dirimir as questões oriundas do presente contrato, renunciando-se, desde já, a qualquer outro Foro.

As Partes, de comum acordo, concordam que o presente termo será assinado eletronicamente por seus representantes legais juntamente com duas testemunhas, nos termos dos artigos 219 e 220 do Código Civil, e do art. 10, parágrafos 1º e 2º da Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Neste sentido, as Partes reconhecem a veracidade, autenticidade, integridade, validade e eficácia deste Instrumento e seus termos, para todos os fins de direito.

Vitória (ES), data.

ASSOCIAÇÃO EVANGÉLICA BENEFICENTE ESPÍRITO SANTENSE
Nome completo do representante legal
Presidente

RAZÃO SOCIAL
Nome completo do representante legal
Cargo