ANEXO I – TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO
CONSELHO REGIONAL DE MEDICINA DO ESTADO DA BAHIA
PREGÃO ELETRÔNICO Nº 05/2022
(Processo Administrativo PCS Nº 040/2022)

1. DO OBJETO

1.1 O presente instrumento tem por objeto a contratação de solução de TI que contempla a renovação e aquisição de Software de segurança para usuário final, incluindo garantia e atualização, Software de segurança para cargas de trabalho híbridas com detecção e resposta, incluindo garantia e atualização de versão e Serviço de Suporte especializado para Instalação, Migração e Suporte Preventivo/Corretivo, de acordo com os termos e especificações do presente documento e seus anexos.

GRUPO	Item	Descrição do item	COD. COMPRASNET	Qtd.
GRUPO UNICO	1	Software de segurança para usuário final, incluindo garantia, atualização e suporte. Período de 12 meses.	27502	200
	2	Software de segurança para cargas de trabalho híbridas com detecção e resposta, incluindo garantia, atualização e suporte. Período de 12 meses	27502	20
	3	Serviço de Suporte Especializado para Instalação, Migração e Suporte Preventivo/Corretivo por 30 dias.	26972	01

1.2 objeto da licitação tem a natureza de serviço comum de tecnologia da informação - SAAS (Software As A Service);
1.3 Os quantitativos e respectivos códigos dos itens são os discriminados na tabela acima.
1.4 A presente contratação adotará como regime de execução a Empreitada de Preço Global por Grupo.
1.5 A decisão pelo critério de julgamento pelo Menor Preço Global se deve ao fato de que a execução do objeto, por mais de uma empresa, poderia gerar elevado custo de administração e comprometeria a qualidade e efetividade dos resultados para o CREMEB.
1.6 A divisão do objeto a ser licitado em itens isolados acarretaria também, prejuízos quanto à instalação, configuração e operação de todo o sistema, uma vez que se exige total compatibilidade entre os soluções, a instalação precisa ser uniforme, assegurando o funcionamento correto e seguro do software. Por essas razões, o critério de adjudicação por contratação única, revela-se o mais adequado.

2. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

2.1 A indicação de marca/desenvolvedor para aquisição e renovação das licenças se dá pelo fato de que a primeira licitação para aquisição de antivírus para o parque de informática do CREMEB, teve como proposta vencedora a solução da empresa Trend Micro, que à época, ofertara o menor preço atendendo todos os requisitos da contratação, bem como atendendo na plenitude todos as necessidades técnicas para prevenção e detecção das ameaças cibernéticas.

2.2 Necessidade de ampliação de novas licenças para atender as licenças reservas, novos equipamentos e os equipamentos que serão utilizados no novo sistema do Conselho Federal de Medicina PAE (Processo Administrativo Eletrônico), além da necessidade de renovar as licenças já existentes, a fim de manter o serviço de suma importância para a segurança digital da instituição e garantir o serviço de suporte e atualização dos softwares acima citados pelo proprietário e mantenedor Trend Micro.

2.3 Como é sabido as ameaças virtuais são reais e se mantém em constante evolução e sempre com as intenções negativas de sequestrar informações, dados sigilosos de instituições e até mesmo causar danos nos sistemas e equipamentos utilizados no nosso cotidiano, desse modo, a contratação de uma solução antivírus, por si só não é capaz de garantir a segurança vitalícia das informações e dos equipamentos, de maneira que a manutenção dessas licenças são essenciais para acompanhar a evolução de tais ameaças, identificá-las e dar o devido tratamento e destinação.

3. DESCRIÇÃO DA SOLUÇÃO

3.1 CARACTERÍSTICAS GERAIS

3.1.1 A fim de facilitar a gestão do ambiente, todas as soluções devem ser do mesmo fabricante;

3.1.2 O fabricante deve possuir experiência comprovada oficialmente de, pelo menos 10 anos, em pesquisas de vulnerabilidades e ameaças;

3.1.3 As soluções deverão, dependendo do escopo, ser entregues como serviço (nuvem) ou em caso de solicitação por parte da CONTRATANTE, local (on-premises).

3.2 SOFTWARE DE SEGURANÇA PARA USUÁRIO FINAL, CONTENDO AMBIENTE ISOLADO E SEGURO PARA TESTE DE NOVAS AMEAÇAS, COM VISIBILIDADE, INCLUINDO GARANTIA E ATUALIZAÇÃO POR 12 MESES

3.2.1 Características gerais

3.2.2 As soluções deverão, dependendo do escopo, ser entregues como serviço (nuvem) ou em caso de solicitação por parte da CONTRATANTE, local (on-premises).

3.2.2.1 Possuir console Web para gerenciamento e administração da ferramenta;

3.2.2.2 A solução deverá ser toda de um único fabricante;

3.2.2.3 A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações e Controle de dispositivos em um único agente.

3.2.3 Módulo de Proteção Anti-Malware

3.2.3.1 Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

3.2.3.1.1 Windows 7 SP1 (x86/x64);

3.2.3.1.2 Windows 8.1 (x86/x64);

3.2.3.1.3 Windows 10 (x86/x64).

3.2.3.1.4 Windows 11 (x86/x64), se já disponível.

3.2.3.2 Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;
3.2.3.3 Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;
3.2.3.4 Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:
3.2.3.4.1 Processos em execução em memória principal (RAM);
3.2.3.4.2 Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);
3.2.3.4.3 Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, CAB;
3.2.3.4.4 Arquivos recebidos por meio de programas de comunicação instantânea (MSN messenger, yahoo messenger, google talk, icq, dentre outros).
3.2.3.5 Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, VBScript/Activex;
3.2.3.6 Deve possuir detecção heurística de vírus desconhecidos;
3.2.3.7 Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada;
3.2.3.8 Deve permitir diferentes configurações de detecção (varredura ou rastreamento):
3.2.3.8.1 Em tempo real de arquivos acessados pelo usuário;
3.2.3.8.2 Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;
3.2.3.8.3 Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;
3.2.3.8.4 Automáticos do sistema com as seguintes opções:
3.2.3.8.4.1 Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;
3.2.3.8.4.2 Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente ou mover automaticamente para área de segurança (quarentena);
3.2.3.8.4.3 Frequência: horária, diária, semanal e mensal;
3.2.3.8.4.4 Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados.
3.2.3.9 Deve possuir mecanismo de cache de informações dos arquivos já escaneados;
3.2.3.10 Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;
3.2.3.11 Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;
3.2.3.12 Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;
3.2.3.13 Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-

in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

3.2.3.14 Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;

3.2.3.15 Deve possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo os demais intactos

3.2.3.16 Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

3.2.3.17 Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

3.2.3.18 Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

3.2.3.19 Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;

3.2.3.20 Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de obfuscação que o módulo de Machine Learning em pré-execução não consiga detectar;

3.2.3.21 Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;

3.2.3.22 Deve bloquear processos comuns associados a ransomware;

3.2.3.23 Em casos de ataques de ransomware, a solução deve ter a capacidade de interromper o processo de criptografia e restaurar os arquivos originais aos seus respectivos diretórios

3.2.3.24 Deve possuir funcionalidade de detecção de malwares conhecidos e desconhecidos por comportamento;

3.2.3.25 Deve permitir a integração com solução de análise de artefatos suspeitos (sandbox) do próprio fabricante.

3.2.4 Funcionalidade de Atualização

3.2.4.1 Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

3.2.4.2 Deve permitir atualização incremental da lista de definições de vírus;

3.2.4.3 Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

3.2.4.4 Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

3.2.4.5 Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

3.2.4.6 Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

3.2.4.7 O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

3.2.5 Funcionalidade de Administração

3.2.5.1 Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;
3.2.5.2 Deve possibilitar instalação "silenciosa";
3.2.5.3 Deve permitir o bloqueio por nome de arquivo;
3.2.5.4 Deve permitir o travamento de pastas e diretórios;
3.2.5.5 Deve permitir o travamento de compartilhamentos;
3.2.5.6 Deve permitir o rastreamento e bloqueio de infecções;
3.2.5.7 Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;
3.2.5.8 Quando on-premises, deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;
3.2.5.9 Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;
3.2.5.10 Deve permitir a desinstalação através da console de gerenciamento da solução;
3.2.5.11 Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;
3.2.5.12 Quando on-premises, deve ter a possibilidade de backup da base de dados da solução através da console de gerenciamento;
3.2.5.13 Quando on-premises, deve ter a possibilidade de designação do local onde o backup automático será realizado;
3.2.5.14 Quando on-premises, deve permitir realização do backup da base de dados através de mapeamento de rede controlado por senha;
3.2.5.15 Quando on-premises, deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;
3.2.5.16 Deve permitir a deleção dos arquivos quarentenados;
3.2.5.17 Deve permitir remoção automática de clientes inativos por determinado período de tempo;
3.2.5.18 Deve permitir integração com serviço de autenticação como Active Directory para acesso a console de administração;
3.2.5.19 Quando on-premises, identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada. Em caso de soluções em nuvem, será aceita utilização de ferramenta do próprio fabricante para varredura local;
3.2.5.20 Deve permitir criação de diversos perfis e usuários para acesso a console de administração;
3.2.5.21 Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

3.2.5.22 Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;
3.2.5.23 Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory, tipo ou IP;
3.2.5.24 Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;
3.2.5.25 Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
3.2.5.26 Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional;
3.2.5.27 Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;
3.2.5.28 Deve prover criptografia para as comunicações entre o servidor e os agentes de proteção;
3.2.5.29 Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;
3.2.5.30 Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;
3.2.5.31 Deve permitir a criação de usuários locais de administração da console de anti-malware;
3.2.5.32 Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;
3.2.5.33 Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;
3.2.5.34 Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;
3.2.5.35 Deve permitir a gerência de domínios separados para usuários previamente definidos;
3.2.5.36 Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido no console de administração;
3.2.5.37 Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

3.2.6 Funcionalidade de Controle de Dispositivos

3.2.6.1 As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por usuário;
3.2.6.2 Deve permitir políticas e ações diferentes para dispositivos conectados à rede interna e aqueles utilizados na rede externa (conectado à Internet, por exemplo);
3.2.6.3 Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

3.2.6.4 Deve possuir o controle de acesso a drives de mídias de armazenamento como CD-ROM, DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;
3.2.6.5 Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;
3.2.6.6 Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;
3.2.6.7 Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, CD-ROM) mesmo com a política de bloqueio total ativa;
3.2.6.8 Para ação de restrição como o bloqueio, a solução deve permitir adicionais dispositivos USB autorizados, bem como apontar executáveis específicos como exceção ao bloqueio;
3.2.6.9 Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;
3.2.6.10 Deve permitir controle de permissão ou bloqueio para dispositivos que não armazenam dados tendo, pelo menos, os seguintes tipos de dispositivos: adaptadores bluetooth, dispositivos de imagem, modems, interfaces wireless externas, cartões PCMCIA, dispositivos infravermelhos e portas COM/LPT.

3.2.7 Módulo de Proteção Anti-Malware para estações MacOs

3.2.7.1 O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:
3.2.7.1.1 macOS 10.15 (Catalina);
3.2.7.1.2 macOS 10.14 (Mojave);
3.2.7.1.3 macOS 10.13 (High Sierra);
3.2.7.1.4 macOS 10.12 (Sierra);
3.2.7.1.5 OS X 10.11 (El Capitan).
3.2.7.2 Suporte ao Apple Remote Desktop para instalação remota da solução;
3.2.7.3 Gerenciamento integrado à console de gerência central da solução
3.2.7.4 Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;
3.2.7.5 Permitir a verificação das ameaças da maneira manual e agendada;
3.2.7.6 Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;
3.2.7.7 Permitir as ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;
3.2.7.8 Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;
3.2.7.9 Deve possuir no mecanismo de autoproteção as seguintes proteções:
3.2.7.9.1 Autenticação de comandos IPC;
3.2.7.9.2 Proteção e verificação dos arquivos de assinatura;
3.2.7.9.3 Proteção dos processos do agente de segurança;
3.2.7.9.4 Proteção das chaves de registro do agente de segurança;
3.2.7.9.5 Proteção do diretório de instalação do agente de segurança.

3.2.8 Funcionalidade de HIPS – Host IPS e Host Firewall

3.2.8.1 Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais:

3.2.8.1.1 Windows 7 SP1 (x86/x64);

3.2.8.1.2 Windows 8.1 (x86/x64);

3.2.8.1.3 Windows 10 (x86/x64).

3.2.8.1.4 Windows 11 (x86/x64), se já disponível.

3.2.8.2 Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;

3.2.8.3 As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;

3.2.8.4 Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

3.2.8.5 Deve permitir ativar e desativar o produto sem a necessidade de remoção;

3.2.8.6 Deve permitir que o usuário altere as configurações de níveis de segurança e exceções;

3.2.8.7 Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo;

3.2.8.8 O modulo de IDS deverá prevenir contra os seguintes tipos de ataque: Too Big Fragment, Ping da morte, Conflito de ARP, SYN Flood, Overlapping Fragment, Teardrop, Tiny Fragment Attack, Fragmented IGMP e Land Attack;

3.2.8.9 O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança;

3.2.8.10 O modulo de HIPS deverá possuir regras pra proteger contra ameaças do tipo Ransomware;

3.2.8.11 O modulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genéricas protegendo contra ameaças conhecidas ou desconhecidas;

3.2.8.12 O módulo de HIPS deverá permitir que o administrador monitore apenas ou realize o bloqueio das tentativas de exploração de vulnerabilidades;

3.2.8.13 Deve suportar configuração de parâmetros de pacotes como quantidade máxima de conexões TCP e timeout para pacotes UDP;

3.2.8.14 Deve ter a capacidade de proteção contra exploração de vulnerabilidades do sistema operacional e de aplicações terceiras instaladas na estação de trabalho;

3.2.8.15 A lista de regras deve permitir que o administrador realize buscas e tenha rápida visibilidade do tipo da aplicação, em que modo a regra encontra-se (bloqueio ou monitoramento), CVE, CVSS score, quando aplicável.

3.2.9 Módulo para Controle De Aplicações

3.2.9.1 Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

3.2.9.1.1 Windows 7 SP1 (x86/x64);

3.2.9.1.2 Windows 8.1 (x86/x64);

3.2.9.1.3 Windows 10 (x64).

3.2.9.1.4 Windows 11 (x86/x64), se já disponível.
3.2.9.2 As regras de controle de aplicação devem permitir as seguintes ações:
3.2.9.2.1 Permissão de execução;
3.2.9.2.2 Bloqueio de execução;
3.2.9.2.3 Bloqueio de novas instalações.
3.2.9.3 A regra de liberação para o controle de aplicação deverá permitir que o programa liberado efetue ou não a execução de outros processos,
3.2.9.4 As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;
3.2.9.5 As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:
3.2.9.5.1 Assinatura SHA-1 e SHA-256 do executável;
3.2.9.5.2 Atributos do certificado utilizado para assinatura digital do executável;
3.2.9.5.3 Caminho lógico do executável;
3.2.9.5.4 Base de assinaturas de certificados digitais válidos e seguros.
3.2.9.6 As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;
3.2.9.7 As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;
3.2.9.8 O módulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionadas para bloqueio e monitoramento tendo, pelo menos, as categorias de KeyLoggers, anonimizadores de proxy, P2P, crackers de senhas;
3.2.9.9 Deve permitir a busca por aplicações ou fabricante destas;
3.2.9.10 Deve possuir ferramenta para extrair o hash de um ou um grupo de executáveis, permitindo a importação destes hashes através de arquivo CSV.

3.2.10 Funcionalidade de Criptografia de disco:

3.2.10.1 Possuir a capacidade de realizar a criptografia nos seguintes sistemas operacionais:
3.2.10.1.1 Windows 7 SP1 (x86/x64);
3.2.10.1.2 Windows 8.1 (x86/x64) e;
3.2.10.1.3 Windows 10 (x86/x64).
3.2.10.1.4 Windows 11 (x86/x64), se já disponível.
3.2.10.2 Possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), permitindo criptografia para: Disco completo (FDE – full disk encryption); Pastas e arquivos; Mídias removíveis; Anexos de e-mails e Automática de disco;
3.2.10.3 Possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;
3.2.10.4 Possuir a capacidade de exceções para criptografia automática;
3.2.10.5 Possuir compatibilidade de autenticação por múltiplos fatores;
3.2.10.6 Permitir atualizações do sistema operacional mesmo quando o disco está criptografado;
3.2.10.7 Possuir auto ajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;

3.2.10.8 Possuir mecanismos para wipe (limpeza) remoto;
3.2.10.9 Possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);
3.2.10.10 Possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook;
3.2.10.11 O ambiente de autenticação pré-inicialização deve permitir a conexão a redes sem fio (wireless);
3.2.10.12 Permitir, em nível de política, a indicação de pastas a serem criptografadas;
3.2.10.13 Possibilitar que cada política tenha uma chave de criptografia única;
3.2.10.14 Permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;
3.2.10.15 Possibilitar a desativação de dispositivos de gravação de mídias óticas e de dispositivos de armazenamento USB;
3.2.10.16 Possibilitar deletar todos os dados do dispositivo na ocorrência de um número personalizável de tentativas inválidas de autenticação.

3.2.11 Módulo de proteção para smartphones e tablets

3.2.11.1 O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais:
3.2.11.1.1 IOS e Android;
3.2.11.2 As funcionalidades estarão disponíveis de acordo com cada plataforma
3.2.11.3 Deve permitir o provisionamento de configurações de:
3.2.11.3.1 Wi-fi, Exchange Activesync, vpn, proxy http global e certificados;
3.2.11.4 Deve possuir proteção de anti-malware para Android;
3.2.11.5 Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão sd e após atualização de vacinas;
3.2.11.6 Possuir capacidade de detecção de spam proveniente de SMS;
3.2.11.7 Possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número bloqueados para recebimento de chamadas;
3.2.11.8 Possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número permitidos para efetuação de chamadas;
3.2.11.9 Possuir funcionalidade de firewall para bloqueio de tráfego de entrada e saída, com possibilidades de enumeração de regras de exceção;
3.2.11.10 Permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL's acessadas;
3.2.11.11 Permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;
3.2.11.12 Permitir o bloqueio de aplicativos de acordo com sua faixa etária indicativa;
3.2.11.13 Possuir controle da política de segurança de senhas, com critérios mínimos de: Padrão de senha; Uso obrigatório de senha; Tamanho mínimo; Tempo de expiração; Bloqueio automático da tela; Bloqueio por tentativas inválidas.
3.2.11.14 Controle de acesso à seguinte lista funções e status de ativação de funções dos dispositivos móveis:
3.2.11.15 Bluetooth;

3.2.11.16 Câmera;
3.2.11.17 Cartões de memória;
3.2.11.18 Wlan/Wi-fi;
3.2.11.19 GPS;
3.2.11.20 Microsoft Activesync;
3.2.11.21 MMS/SMS;
3.2.11.22 Alto-falante;
3.2.11.23 Armazenamento USB;
3.2.11.24 3G;
3.2.11.25 Modo de desenvolvedor;
3.2.11.26 Ancoragem (tethering).

3.2.12 Proteção avançada com filtro de conteúdo para navegação web

3.2.12.1 Características gerais

3.2.12.1.1 A solução deve ser capaz de detectar malware conhecido e desconhecido;
3.2.12.1.2 As assinaturas e inteligência utilizadas pela solução devem pertencer ao mesmo fabricante da solução;
3.2.12.1.3 A funcionalidade de anti-malware deve estar contida no licenciado fornecido, sem necessidade de taxas ou licenciamento adicional;
3.2.12.1.4 Não serão aceitas combinações com soluções open-source como Squid;
3.2.12.1.5 A solução deve ser capaz de detectar documentos exploráveis. Deve incluir suporte para tipos de arquivos do Microsoft Office e PDF. Todas as explorações críticas baseadas em CVE nesses arquivos devem ser detectadas;
3.2.12.1.6 A solução deve ser capaz de detectar e bloquear malware desconhecido (não baseado em assinaturas) em tempo real de acordo com funcionalidade de Machine Learning;
3.2.12.1.7 Deve ser compatível com arquivos Windows PE;
3.2.12.1.8 O arquivo suspeito pode ser bloqueado de acordo com a ação definida logo na primeira conexão;
3.2.12.1.9 A solução deve ser capaz de detectar botnet com URL's e IP's;
3.2.12.1.10 A solução deve ser capaz de detectar sites maliciosos através de mecanismos pela pontuação/classificação;
3.2.12.1.11 A solução deve ser capaz de bloquear sites maliciosos por "categoria web". O requisito mínimo de categoria deve incluir: Ransomware, Phishing, Scam, Spam, C&C, Vetor de doença (site de malware conhecido) e conexões IOT inseguras (detecção de botnet IoT);
3.2.12.1.12 A solução deve ser capaz de detectar e bloquear conteúdo por tipo de arquivo verdadeiro (true file type) como política de usuário/grupo;
3.2.12.1.13 Deve suportar a configuração da ação por política;
3.2.12.1.14 Deve ser compatível com os seguintes tipos de arquivos: EPS, CHM, GZ, RAR, SIT, TAR, ZIP, AIF, FLV, M4A, MID, MOV, MP4, MP3, RA/RM, SWF, WAV, AVI, ASF, COM, DLL, EXE, LNK, MSI, BMP, GIF, JPG, PNG, PSD, PSP, TIF, DOC/X, ODT, PDF, PPT/X, WPD, XLS/X;
3.2.12.1.15 A solução deve oferecer suporte à filtragem de URL para restringir o acesso dos usuários por categoria da web;

3.2.12.1.16 A solução deve oferecer suporte a pelo menos 85 categorias da web para filtragem de URL;
3.2.12.1.17 A solução deve suportar o controle de, pelo menos, 700 aplicações distintas;
3.2.12.1.18 O mecanismo de controle de aplicações deve permitir a configuração das ações por política, tendo, pelo menos, as ações de Bloquear e Permitir;
3.2.12.1.19 A solução deve ser capaz de restringir o acesso da conta "pessoal" (não assinada pela empresa) aos serviços abaixo. Google G-Suite, Microsoft Office 365, Microsoft Azure e Dropbox;
3.2.12.1.20 A solução deve ser capaz de configurar a política com base em:
3.2.12.1.20.1 (Diretório / Domínio) usuário ou grupo
3.2.12.1.20.2 Gateway (local, breakout) e opção de exceção com endereço IP
3.2.12.1.20.3 Tipo de tráfego (categoria de filtragem de URL, controle de aplicativos, aplicativo em nuvem;
3.2.12.1.20.4 Tipo de arquivo (MIME, True Filetype ou nome de arquivo);
3.2.12.1.20.5 Agendamento de horários;
3.2.12.1.20.6 Ação: Bloquear e Permitir.
3.2.12.1.21 A solução deve ser capaz de configurar listas de permissão ou bloqueio em escopo globais;
3.2.12.1.22 A solução deve ser capaz de descriptografar o tráfego HTTPS;
3.2.12.1.23 A solução deve ser capaz de importar CA de raiz intermediária para descriptografias HTTPS;
3.2.12.1.24 A solução deve ser capaz de tomar ação quando uma comunicação com uma CA falhar na validação. Em caso de falha, deve incluir a CA como não confiável, CA expirada. A ação deve incluir Bloquear, Permitir;
3.2.12.1.25 A solução deve ser capaz de executar a função de túnel automático. Enquanto qualquer um dos servidores falhar, a 2ª conexão deve ser auto-tunelada por causa do erro do lado do servidor;
3.2.12.1.26 A solução deve ser capaz de registrar o domínio principal do site auto-tunelado;
3.2.12.1.27 A solução deve ser capaz de permitir que o administrador verifique o site com túnel automático, esse administrador deve ser capaz de configurar a política para esses sites com túnel como de "continuar túnel" ou "não-túnel automático";
3.2.12.1.28 A solução deve ser capaz de oferecer suporte a várias CA raiz para descriptografia HTTPS na política;
3.2.12.1.29 A solução deve ser capaz de configurar a política para descriptografar o tráfego HTTPS para, pelo menos, 85 categorias da web;
3.2.12.1.30 A solução deve ser capaz de gerenciar todas as políticas na nuvem e no proxy local em uma única console. O gerenciamento da política deve ser realizado via console de gerenciamento baseado em GUI não deve ser realizado como baseado em comando (por exemplo, CLI, SSH);
3.2.12.1.31 A solução deve ser capaz de definir o PAC em um console. O PAC deve ser editável por meio do console de gerenciamento baseado em GUI;
3.2.12.1.32 Os meios para análise do tráfego devem incluir, pelo menos, arquivo PAC configurado nos browsers e agente para forçar o direcionamento do tráfego para o gateway web;

3.2.12.1.33 Deve ter a capacidade de filtrar tráfego de dispositivos móveis através de VPN configurada para direcionar o tráfego para o gateway web;
3.2.12.1.34 A solução deve ser capaz de configurar várias contas de administrador;
3.2.12.1.35 A solução deve ser capaz de mostrar as estatísticas dos últimos 7 dias no painel;
3.2.12.1.36 A solução deve ser capaz de realizar análises de log para violações;
3.2.12.1.37 O dashboard deve exibir, tendo a opção de customizar o tempo, pelo menos: estatísticas de tráfego por tamanho, detecções de malware, categorias de URL's detectadas, aplicações detectadas, tráfego por localidade;
3.2.12.1.38 O dashboard deve permitir a personalização dos dados para exibir, pelo menos, gráficos de barra, tabelas e gráfico de pizza;
3.2.12.1.39 O dashboard deve permitir customização dos componentes exibidos, permitindo sua inclusão e exclusão, de acordo com a necessidade do administrador;
3.2.12.1.40 A solução deve permitir incluir gateways por localidade para que a classificação do tráfego possa ser feita localmente. Nos casos de usuários em trabalho remoto, o tráfego deve ser identificado pelo IP de origem, bem como pelo usuário que está navegando;
3.2.12.1.41 A solução deve permitir a criação de categorias personalizadas de sites, com os quais o administrador possa utilizá-las nas políticas de acesso;
3.2.12.1.42 Deve permitir a personalização das notificações enviadas para os usuários contendo, pelo menos, as seguintes notificações: bloqueio de acesso por política, bloqueio de acesso por URL maliciosa, aviso de acesso ilegal, regras de bypass através de senha, detecção de ameaças, falha de validação de certificado;
3.2.12.1.43 Deve possuir mecanismo de classificação dinâmica do conteúdo do site, de acordo com o que está sendo carregado, a ferramenta deve atribuir uma categoria automática ao conteúdo e aplicar a política configurada;
3.2.12.1.44 A solução deve permitir consolidar todos os logs em uma única console;
3.2.12.1.45 Deve permitir criar buscas nos logs utilizando parâmetros como período, ação, nome da regra, nome do malware, dispositivo, domínio, dentre outros;
3.2.12.1.46 Baseado no resultado de uma consulta, a solução deve permitir que o administrar possa salvar a consulta como favorita ou como um relatório em PDF;
3.2.12.1.47 A solução deve permitir alterar o tipo de exibição das informações dos logs para, pelo menos, gráficos de pizza, gráficos de linhas, gráficos de barras e tabela;
3.2.12.1.48 Deve permitir a criação de relatórios sob demanda e agendados (diário, semanal, mensal e definindo o período manualmente). Os relatórios devem possuir filtros por localidade/gateway e usuários;
3.2.12.1.49 Deverá fornecer pelo menos os seguintes relatórios: Aplicações mais utilizadas, Categorias e sites mais acessados, Usuários com maior número de acessos, Políticas violadas, maiores infratores, principais ameaças filtradas, dentre outros;
3.2.12.1.50 A solução deve possuir mecanismo que permita auditar as ações dos administradores, registrando as principais ações executadas. Os logs de auditoria devem ser exportados para arquivo offline como CSV;
3.2.12.1.51 Deve permitir o backup das políticas em arquivo;
3.2.12.1.52 O agente de monitoramento do tráfego deve possuir opção de desabilitar a filtragem temporariamente através de uma chave definida pelo administrador;

3.2.12.1.53 Para que o agente seja desinstalado, a solução deve prover mecanismo de proteção para que isso esteja disponível mediante senha configurada;
3.2.12.1.54 A solução deve permitir que o administrador receba notificações que incluam, pelo menos, notificações de sistema (falhas de autenticação, erro nos gateways), segurança (conteúdo malicioso, botnets) e uso de Internet (violação de políticas de tráfego);
3.2.12.1.55 Os alertas devem ser configurados para serem enviados a escopos distintos de usuários/administradores;
3.2.12.1.56 O agente de monitoramento de acesso deve possuir compatibilidade com Windows e MacOS.
3.2.12.1.57 O proxy local da solução deve ser capaz de permitir que o cliente instale a plataforma abaixo:
3.2.12.1.58 Qualquer plataforma compatível com Redhat Enterprise 7.x ou CentOS 7.x
3.2.12.1.59 Baremetal;
3.2.12.1.60 Plataforma virtualizada (VMWare, HyperV, KVM);
3.2.12.1.61 Servidores em nuvem Microsoft Azure e Amazon AWS.
3.2.12.1.62 O proxy local da solução deve ser totalmente controlado pelo cliente.
3.2.12.1.63 O administrador deve ser capaz de adicionar mais recursos no gateway local sem mais assinaturas ou licenças.
3.2.12.1.64 O administrador deve ser capaz de acessar o gateway local via SSH para gerenciamento de rede.
3.2.12.1.65 A solução deve ser capaz de suportar o protocolo/método abaixo para autenticação do usuário:
3.2.12.1.65.1 Microsoft AD (até AD 2016);
3.2.12.1.65.2 Microsoft Azure AD;
3.2.12.1.65.3 Okta;
3.2.12.1.65.4 Microsoft ADFS;
3.2.12.1.65.5 Microsoft AD.
3.2.12.1.66 A solução deve ser capaz de sincronizar as informações do usuário do diretório para configurações de política;
3.2.12.1.67 A solução deve ser capaz de suportar vários domínios ao fazer as autenticações do usuário.

3.2.13 Proteção avançada para e-mails

3.2.13.1Características Gerais da Solução

3.2.13.1.1 Em caso de nuvem, a solução deverá atender, no mínimo, os níveis de serviço abaixo:

Disponibilidade do serviço	98% ou maior de uptime
Proteção contra Vírus	Nenhum e-mail com vírus
Efetividade no bloqueio de SPAM	99% ou maior
Ocorrência de Falsos-positivos	Não mais que 0,0004%
Latência máxima na entrega de mensagens	Não mais que um minuto

3.2.13.1.2 A solução deverá possuir Single Sign-On para acessar o console de administração;
3.2.13.1.3 A solução deverá permitir a criação de regras para entrada (inbound) e saída (outbound) de e-mails;
3.2.13.1.4 A solução deverá possuir console de gerenciamento web;
3.2.13.1.5 A solução deverá possuir console centralizada, incluindo:
3.2.13.1.5.1 Configurações de administração;
3.2.13.1.5.2 Objetos de política;
3.2.13.1.5.3 Objetos suspeitos;
3.2.13.1.5.4 Gerenciamento de usuário final;
3.2.13.1.5.5 Gerenciamento de diretório;
3.2.13.1.5.6 Informações sobre licenciamento;
3.2.13.1.5.7 Logs;
3.2.13.1.5.8 Relatórios.
3.2.13.1.6 A solução deverá possuir dashboards possibilitando no mínimo a visualização de ameaças, ransomwares, detalhes de autenticação baseada em domínio, sandbox, BEC, SPAM, principais violações, eventos de DLP, consumo de banda, proteção Time-of-Click;
3.2.13.1.7 A solução deverá possuir configurações de dashboard sendo possível selecionar:
3.2.13.1.7.1 Direção do tráfego: entrada e saída de e-mails (inbound/outbound);
3.2.13.1.7.2 Período: data, semana e mês.
3.2.13.1.8 A solução deverá possuir métodos de autenticação como: Correspondência de IP do remetente, SPF (Sender Policy Framework); DKIM (DomainKeys Identified Mail) e DMARC (Authentication Message Reporting, Reporting & Conformity) baseado em domínio para proteger contra falsificação de e-mail;
3.2.13.1.9 A solução deverá ser capaz de permitir a filtragem baseada em reputação IP para no mínimo: Remetentes permitidos com base no endereço IP e país
3.2.13.1.10 Remetentes bloqueados com base no endereço IP e país;
3.2.13.1.11 A solução deverá ser capaz de permitir a filtragem de remetente e destinatários para no mínimo: Remetentes aprovados por endereço de e-mail ou domínio, Remetentes bloqueados por endereço de e-mail ou domínio e validar destinatário de entrada de e-mail;
3.2.13.1.12 A solução deverá possibilitar incluir X-Header no cabeçalho da mensagem para mensagens de e-mail correspondentes a remetentes aprovados;
3.2.13.1.13 A lista de remetentes aprovados e remetentes bloqueados deverão exibir no mínimo as seguintes informações:
3.2.13.1.13.1 Remetente;
3.2.13.1.13.2 Domínio do destinatário;
3.2.13.1.13.3 Data.
3.2.13.1.14 A solução deverá possuir Correspondência de IP do remetente, possibilitando especificar um IP ou um intervalo de endereços IP em um domínio do remetente identificado pelo endereço do cabeçalho da mensagem para permitir mensagens de e-mail apenas desses endereços;

3.2.13.1.15 A solução deverá detectar malwares, worms, e outras ameaças baseadas em assinatura e padrões;
3.2.13.1.16 A solução deverá ser capaz de detectar spam baseado em assinatura e padrões;
3.2.13.1.17 A solução deverá identificar e-mails marketing como redes sociais, fóruns e boletins de informações;
3.2.13.1.18 A solução deverá permitir criar exceções para e-mails marketing;
3.2.13.1.19 A configuração de spam deverá possuir no mínimo três níveis: baixo, meio e alto;
3.2.13.1.20 A solução deverá detectar ataques de comprometimento de e-mail;
3.2.13.1.21 A solução deverá possuir detectar phishing e conteúdos suspeitos;
3.2.13.1.22 A solução deverá detectar mensagens de graymail;
3.2.13.1.23 A solução deverá varreduras JSE e VBE para identificar ameaças de macro;
3.2.13.1.24 A solução deverá detectar ameaças desconhecidas utilizando machine learning;
3.2.13.1.25 A solução deverá permitir visualizar relatório detalhado para cada detecção Machine Learning;
3.2.13.1.26 A solução deverá possuir engine própria para detecção de explorações de documentos, ameaças de dia zero, vulnerabilidades conhecidas e outras ameaças usadas em ataques direcionados;
3.2.13.1.27 A solução deverá possuir Proteção anti-ransomware;
3.2.13.1.28 A solução deverá possuir analise de URL's no corpo do e-mail;
3.2.13.1.29 A solução deverá possuir o recurso para analisar as URL's no momento do clique do usuário e as bloquear se forem maliciosas;
3.2.13.1.30 A solução deve possuir ações de bloqueio, liberação e alerta para as seguintes categorias ou equivalentes: perigoso, altamente suspeito, não testado e suspeito;
3.2.13.1.31 A solução deve possuir ações de bloqueio, liberação e alerta para as seguintes categorias ou equivalentes: perigoso, altamente suspeito, não testado e suspeito;
3.2.13.1.32 A solução deverá possuir Proteção contra Comprometimento de E-mail;
3.2.13.1.33 Deverá permitir adicionar usuários de alto perfil, possibilitando exportar a lista em CSV;
3.2.13.1.34 Deverá possibilitar importar usuários de alto perfil através de arquivo CSV;
3.2.13.1.35 A solução deverá fornecer informações detalhadas bem como razões para mensagens de e-mail detectadas como possíveis ataques analisados ou prováveis do Business E-mail Compromise (BEC);

3.2.13.1.36 A solução deverá possuir Proteção contra-ataques de Engenharia Social;
3.2.13.1.37 A solução deverá fornecer informações detalhadas bem como razões para mensagens de e-mail detectadas como possíveis ataques de engenharia social;
3.2.13.1.38 A solução deverá ser capaz utilizar no mínimo os seguintes bancos de dados de reputação que:
3.2.13.1.38.1 Tenham uma lista de endereços IP de servidores de correio que são conhecidos por serem fontes de spam;
3.2.13.1.38.2 Tenham uma lista de endereços IP identificados como envolvidos em ransomware ativos, malware ou outras campanhas de ameaças por e-mail;
3.2.13.1.38.3 Tenham uma lista de IP's atribuídos dinamicamente.

3.2.13.1.39 A solução deverá possibilitar configurar diferentes tipos de exceções de varredura em um e-mail através de definições de condições e possibilitando executar as ações ou equivalentes de bypass, deleção do e-mail incluindo anexos e quarentenar quando:

3.2.13.1.39.1 O número de arquivos em um arquivo compactado excede 353;

3.2.13.1.39.2 A taxa de descompactação de um arquivo compactado excede 100;

3.2.13.1.39.3 O número de camadas de descompactação em um arquivo compactado excede 20;

3.2.13.1.39.4 O tamanho de um único arquivo descompactado excede 60 MB;

3.2.13.1.39.5 Um arquivo do Office contém mais de 353 subarquivos.

3.2.13.1.40 As ações de verificação configuradas para cada exceção deverão ser aplicadas a todos os remetentes e destinatários;

3.2.13.1.41 Deverá possibilitar incluir Tag;

3.2.13.1.42 A solução deverá possuir regras de varredura avançadas que permitam especificar as condições que a regra se aplica às mensagens verificadas pela solução;

3.2.13.1.43 Deverá possuir as seguintes condições:

3.2.13.1.43.1 Tamanho da mensagem;

3.2.13.1.43.2 Assunto;

3.2.13.1.43.3 Corpo do e-mail;

3.2.13.1.43.4 Cabeçalho;

3.2.13.1.43.5 Conteúdo do anexo;

3.2.13.1.43.6 Nome e/ou Extensão:

3.2.13.1.43.6.1 .386, .ACM,.ASP,.AVP, .BAT,.CGI, .CHM, .CLA, .CLASS,.CMD, .CNV, .COM, .CS, .DLL, .DRV, .EXE, .HLP, .HTA, .HTM, .JS*, .LNK, .OCX, .OPO, .PHP, .PL. .SH, .SYS, .VBS, VBE, VXD, .WBS, .WIZ. WSH, .DOC, .DOCM, DOCX, .DOT, .DOTM, .DOTX, .DVB, .EML, .MD*, .PPA, .PPAM, .PPS, .PPSM, .PPSX, .PPT, .PPTM, .PPTX, XL,XLA, XLAM, .XLC, .XLK, XLL,.XLM, .XLR, .XLS, .XLSB, .XLSM, XLSX, .XLT, .XLTM, XLTX;

3.2.13.1.43.7 MIME content-type: vídeo, áudio, imagens, documentos e outros;

3.2.13.1.43.8 Tamanho do anexo;

3.2.13.1.43.9 Anexo protegido por senha: .7z, .ace, .arj, .docx, .pptx, .rar, .xlsx, .zip;

3.2.13.1.43.10 Quantidade de anexos;

3.2.13.1.43.11 Número de destinatários.

3.2.13.1.44 A solução deverá as ações da regra permitindo definir o que acontecerá com as mensagens que atendem às condições dos critérios da regra:

3.2.13.1.44.1 Criptografar mensagem de e-mail;

3.2.13.1.44.2 Monitorar, permitindo os administradores o monitoramento das mensagens. As ações de monitoramento incluem o envio de uma mensagem de notificação para outras pessoas ou o envio de uma cópia oculta (Cco) da mensagem para outras pessoas;

3.2.13.1.44.3 Bloqueio, deverá interceptar a mensagem, impedindo que ela atinja o destinatário original. As ações de bloqueio incluem excluir a mensagem inteira, colocar em quarentena e enviar para um destinatário diferente;

3.2.13.1.44.4 Modificar, permitindo alterar a mensagem e/ou seus anexos. As ações de modificação incluem limpeza de vírus que podem ser limpos, exclusão de anexos de mensagens, inserção de um carimbo no corpo da mensagem ou TAG de assunto.

3.2.13.1.45 A solução deverá possibilitar selecionar de Todas as correspondências ou equivalente para acionar a regra somente quando todos os critérios configurados selecionados fizerem correspondência;

3.2.13.1.46 A solução deverá possibilitar selecionar de qualquer correspondência ou equivalente para acionar a regra quando qualquer critério configurado fizer correspondência;

3.2.13.1.47 Deve ser possível criar políticas de malwares, spam e filtragem de conteúdo com:

3.2.13.1.47.1 Definição do destinatário, possibilitando selecionar domínios cadastrados, domínios específicos e grupos de usuários;

3.2.13.1.47.2 Especificação de endereços de remetente;

3.2.13.1.47.3 Exceções.

3.2.13.1.48 A solução deverá possibilitar importar e exportar os destinatários, remetentes e listas de exceções;

3.2.13.1.49 Deve ser possível criar políticas que executem ações em mensagens que contêm malware, worms ou outros códigos maliciosos;

3.2.13.1.50 Deve ser possível realizar a limpeza de malwares ou códigos maliciosos, onde o malware pode ser removido com segurança do conteúdo do arquivo infectado, resultando em uma cópia não infectada da mensagem ou anexo original;

3.2.13.1.51 A solução deverá possuir o serviço de banner para customização do portal com a logo;

3.2.13.1.52 A solução deverá possuir integração com o Active Directory;

3.2.13.1.53 A solução deverá permitir o gerenciamento de múltiplos domínios;

3.2.13.1.54 A solução deverá permitir a integração com Microsoft Office 365, Google G-Suite e outros servidores de e-mail;

3.2.13.1.55 O uso das REST API's deve permitir executar operações para no mínimo: criação, leitura, atualização e exclusão.

3.2.13.2Criptografia de E-mail

3.2.13.2.1 A solução deverá ser capaz de criptografar e-mails baseado em políticas;

3.2.13.2.2 A solução deverá assegurar a comunicação através da utilização do protocolo TLS;

3.2.13.2.3 A solução deverá permitir a configuração da checagem do TLS;

3.2.13.2.4 A solução deverá suportar: TLS 1.2, TLS 1.1 and TLS 1.0.

3.2.13.3Rastreamento de e-mail e Auditoria

3.2.13.3.1 A solução deve permitir o rastreamento de mensagens de forma centralizada e por meio da interface de gerenciamento, não sendo aceito pesquisa via linha de comando;

3.2.13.3.2 A solução deverá possuir permitir o rastreamento de mensagens enviadas e recebidas;

3.2.13.3.3 A solução deverá possibilitar pesquisas de log de rastreamento de e-mail por até 30 dias;

3.2.13.3.4 A solução deverá fornecer buscas para rastreamento de e-mail por: período, direção do tráfego, remetente, destinatário, tipo (bloqueado/liberado), ação, assunto, ID da mensagem e Hash do anexo SHA256;

3.2.13.3.5 Deverá possibilitar exportar a busca no formato .CSV;
3.2.13.3.6 A solução deverá possuir permitir a consulta de eventos com os logs das políticas aplicadas por até 30 dias;
3.2.13.3.7 A solução deverá fornecer consulta de eventos com os logs das políticas por: período, direção do tráfego, remetente, destinatário, nome da regra, tipo de ameaça, anexo, BEC, conteúdo, DLP, Graymail, ransomware, phishing, spam, malware, web reputation, ID da mensagem e ação;
3.2.13.3.8 A solução deverá permitir rastrear os cliques de URL por até 30 dias;
3.2.13.3.9 A solução deverá fornecer permitir rastrear os cliques de URL por: data, direção do tráfego, remetente, destinatário, ID da mensagem, URL, ação e a hora em que um URL foi clicada;
3.2.13.3.10 A solução deverá ser possível consultar os logs de auditoria da console da solução por até 30 dias;
3.2.13.3.11 Deverá ser possível encaminhar os logs para syslog.

3.2.13.4Relatórios
3.2.13.4.1 A solução deverá fornecer relatórios com base em uma programação diária, semanal, mensal e trimestral;
3.2.13.4.2 Os relatórios deverão ser, pelo menos, no formato PDF;
3.2.13.4.3 Deverá ser possível criar relatório agendados e manuais;
3.2.13.4.4 Deverá ser possível obter relatório sobre com resumo do tráfego de e-mail de todos os domínios e por domínio, detecções de ameaças, detecções de arquivos da sandbox, detecções de URL da sandbox e os principais destinatários comprometidos por e-mail (BEC).

3.2.13.5Notificações
3.2.13.5.1 A solução deverá suportar via notificação via e-mail;
3.2.13.5.2 A solução deverá possuir modelos de notificação pré-definidas para violação de políticas;
3.2.13.5.3 A solução deverá suportar notificar quando o e-mail possuir um anexo compactado;
3.2.13.5.4 A solução deverá notificar quando o e-mail quando o tamanho da mensagem excedido;
3.2.13.5.5 A solução deverá notificar quando uma regra for desencadeada;
3.2.13.5.6 A solução deverá notificar quando houver uma configuração de violação de segurança;
3.2.13.5.7 A solução deverá notificar quando um vírus e spam.

3.2.13.6Prevenção contra Vazamento de Dados
3.2.13.6.1 A solução deverá permitir gerenciar as mensagens de e-mail com dados confidenciais e proteger contra perda de dados, monitorando as mensagens de e-mail de saída;
3.2.13.6.2 A solução deverá possibilitar criar regras por expressões regulares, palavras chaves e atributos do arquivo;
3.2.13.6.3 A solução deverá possuir templates pré-definidos;
3.2.13.6.4 A solução deverá possuir templates customizados;

3.2.13.6.5 A solução deverá possuir uma base com no mínimo 200 modelos para criação de regras;
3.2.13.6.6 A solução deverá permitir a customização de modelos aderência a LGPD.

3.2.13.7Da quarentena
3.2.13.7.1 A solução deverá permitir visualizar as mensagens quarentenadas por data, direção do tráfego, remetente, destinatários e conteúdo;
3.2.13.7.2 A solução deverá permitir o gerenciamento da quarentena para múltiplos domínios;
3.2.13.7.3 A solução deverá permitir a customização da notificação de quarentena pela menos semanal, uma vez ou mais vezes durante o dia;
3.2.13.7.4 A notificação de quarentena deverá permitir a customização;
3.2.13.7.5 A notificação de quarentena deverá ser, no mínimo, em inglês e português;
3.2.13.7.6 A solução deverá possibilitar a gestão de quarentena de forma que seja possível que o administrador possa visualizar: a razão de um determinado bloqueio, o remetente, o destinatário, a data, o assunto, o IP do host de destino, a mensagem original, o tamanho da mensagem original;
3.2.13.7.7 Com base nos requisitos acima, deve ainda permitir as ações liberar e/ou excluir a mensagem;
3.2.13.7.8 A solução deverá permitir realizar o download da mensagem quarentenada
3.2.13.7.9 Caso uma mensagem seja bloqueada ou rejeitada, a solução deverá informar também a razão do bloqueio e quais as regras foram ativadas;
3.2.13.7.10 Deverá possuir single sign-on (SSO) para a quarentena de usuário;
3.2.13.7.11 Deverá possibilitar utilizar duplo fator de autenticação;
3.2.13.7.12 Deverá possibilitar que usuário tome as seguintes ações ou similar em sua própria quarentena:
3.2.13.7.12.1 Excluir e bloquear o remetente: possibilitando excluir permanentemente a mensagem e adicionar o endereço aos remetentes bloqueados;
3.2.13.7.12.2 Excluir, possibilitando excluir permanentemente a mensagem;
3.2.13.7.12.3 Entregar e aprovar o remetente, permitindo liberar a mensagem da quarentena e adicionar o endereço aos remetentes aprovados, para que mensagens futuras de remetentes aprovados não sejam mantidas em quarentena;
3.2.13.7.12.4 Entregar, permitindo assim liberar a mensagem da quarentena.
3.2.13.7.13 Deverá possibilitar que o usuário criar listas remetentes aprovados e remetentes bloqueados.

3.2.14 Módulo de proteção para ferramentas de e-mail e colaboração em nuvem (Office365)
3.2.14.1 A solução deve permitir a identificação e proteção contra ameaças no Microsoft Office 365 (Exchange Online, Sharepoint Online, Onedrive for Business e Microsoft Teams) e GSuite;
3.2.14.2 Identificar e bloquear arquivos maliciosos carregados para o Google Drive, Onedrive, Sharepoint e Microsoft Teams. Por exemplo, se um usuário tentar carregar um determinado arquivo malicioso ou proibido em uma das plataformas citadas, a solução deve fazer o bloqueio;
3.2.14.3 Bloquear upload de arquivos por tipo definido em política para as soluções supracitadas;

3.2.14.4 Identificar e bloquear URL's maliciosas em arquivos e URL's, incluindo URL's dentro de anexos;
3.2.14.5 Realizar escaneamentos de ameaças em tempo real nos serviços integrados, identificando componentes maliciosos;
3.2.14.6 Permitir realizar escaneamento retroativo de ameaças (sob demanda), isto é, em busca de ameaças já armazenadas nas caixas de e-mail dos usuários ou em diretórios do Google Drive, Onedrive e Sharepoint;
3.2.14.7 O nível de sensibilidade das URL's maliciosas deve ser configurável através de políticas;
3.2.14.8 Deve possuir capacidade de cadastro dos usuários importantes para focar a análise de ataques de Comprometimento de E-mail (BEC);
3.2.14.9 Deve permitir que os administradores configurem a periodicidade das notificações para, no mínimo, URL's maliciosas identificadas, SPAMs maliciosos, Phishing, Ransomware, arquivos analisados na sandbox e identificados como baixo, médio e alto risco;
3.2.14.10 Identificar tentativas de Comprometimento de E-mail baseado em uma análise dos estilos de escrita de cada usuário cadastrado como importante;
3.2.14.11 A solução deve permitir a visualização das estatísticas no dashboard por serviço integrado (Gmail, Google Drive, Exchange Online, Teams, Onedrive, Sharepoint) e alterar o período dos logs para, no mínimo, 24 horas, 7 dias e 30 dias;
3.2.14.12 Deve permitir a exibição da tendência para cada um dos tipos de serviço integrado em relação ao mesmo período anterior. Por exemplo, exibir aumento ou redução das ameaças no Exchange Online nos últimos 30 dias, comparando com os 30 dias anteriores;
3.2.14.13 Deve utilizar mecanismos de proteção que contemplem, pelo menos, malwares conhecidos por assinatura, malwares desconhecidos por Machine Learning, bloqueio de conteúdo (por tipo de arquivo, por exemplo), reputação de URL's;
3.2.14.14 A solução deve permitir compartilhamento de informações através de SIEM via API ou através da gerência centralizada;
3.2.14.15 A solução deve prover relatórios que contemplem, pelo menos, riscos de segurança (ameaças), ransomware, arquivos analisados em sandbox, auditoria e sobre a API;
3.2.14.16 Os relatórios devem ser exportáveis para, pelo menos, PDF;
3.2.14.17 Os relatórios devem ser enviados por e-mail, mediante configuração do administrador;
3.2.14.18 A solução ofertada deve contemplar uma plataforma de simulação de phishing e conscientização de usuários sem necessidade de licenciamento adicional;
3.2.14.19 A verificação Anti-malware deverá permitir a customização das ações a serem tomadas, por exemplo: quarentenar, deletar e passar.
3.2.14.20 Realizar integração nuvem-a-nuvem, através de API da Microsoft e Google;
3.2.14.21 As ações configuráveis nas políticas do serviço de e-mail devem contemplar, no mínimo, etiquetar a mensagem (inserir tag), quarentenar, deletar, ignorar e mover para lixeira;
3.2.14.22 Os demais serviços devem possuir ações pré-definidas e configuráveis para eliminar, quarentenar e ignorar os arquivos identificados;
3.2.14.23 As políticas deverão ser aplicáveis por usuário ou grupo sincronizado da estrutura de serviço online (Microsoft ou Google);
3.2.14.24 Possuir um dashboard com as principais ameaças detectadas, a exemplo dos tipos Ransomware, Phishing, Comprometimento de E-mail.
3.2.14.25 A solução deverá ser capaz de implementar políticas com base no filtro de conteúdo das mensagens;

3.2.14.26 A solução deverá ter a capacidade de compartilhar objetos suspeitos identificados através da análise em sandbox com a gerência centralizada do fabricante;
3.2.14.27 Cada política de serviço deve ser configurável para apenas monitorar ou tomar ação de proteção;
3.2.14.28 As notificações enviadas para o administrador e para os usuários devem ser customizáveis, permitindo tradução, inclusão ou exclusão de campos;
3.2.14.29 Deverá permitir a configuração dos níveis de detecção para SPAM;
3.2.14.30 Deverá permitir o administrador criar exceções para permitir ou bloquear determinados endereços de e-mail e URL's manualmente;
3.2.14.31 A solução deve possuir capacidade de ignorar e-mails já enviados para a lixeira do serviço de e-mail;
3.2.14.32 Deve permitir ao administrador bloquear mensagens de graymail por tipo (mensagens de marketing, notificações de fóruns e redes sociais, etc.);
3.2.14.33 Os logs devem ser interativos, permitindo ao administrador montar consultas baseadas nos parâmetros como serviço detectado, tipo/categoria da ameaça, usuários afetados, política acionada, nome da ameaça, dentre outros;
3.2.14.34 Os resultados das consultas de logs deverão ter opção de salvar como um relatório exportável;
3.2.14.35 A solução deve permitir que o administrador realize buscas pontuais nos logs, a partir de parâmetros previamente definidos;
3.2.14.36 Deve possuir áreas de quarentena distintas para cada um dos serviços integrados, permitindo a restauração, download ou exclusão de arquivos/e-mails quarentenados pela política;
3.2.14.37 Deve permitir a criação de exceções para detecções por Machine Learning e por Sandbox;
3.2.14.38 A solução deve ter a capacidade de integração com serviços de autenticação para logon único (single sign-on) com, pelo menos, Okta, ADFS e Azure AD.
3.2.14.39 Deve possuir capacidade de configuração de contas de administração com permissões granulares por administrador, permitindo visualização ou controle total dos itens de menu;
3.2.14.40 Deve suportar a integração com serviço de gerenciamento de incidentes do próprio fabricante através da plataforma de investigação.
3.2.14.41 Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e/ou maliciosas para identificação e categorização de ameaças no ambiente;
3.2.14.42 A solução deve ser capaz de associar diferentes modelos de ameaças e associá-los a um único incidente/evento;
3.2.14.43 Deve ter capacidade de apresentar informações relacionadas ao MITRE para cada um dos eventos detectados no ambiente, caso possuam;
3.2.14.44 Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;
3.2.14.45 Em caso de ameaça avançada por e-mail, a solução deve permitir tomar diferentes ações de resposta no ambiente, contemplando, no mínimo:
3.2.14.45.1 Permitir adicionar o remetente (sender) de um e-mail na lista de bloqueio, impedindo o mesmo de enviar novos e-mails os usuários internos;
3.2.14.45.2 Mover o e-mail selecionado para a área de quarentena de um específico usuário ou todos os usuários que contenham este e-mail em suas caixas;
3.2.14.45.3 Deletar o e-mail selecionado das caixas selecionadas.

3.3 **SOFTWARE DE SEGURANÇA PARA CARGAS DE TRABALHO HÍBRIDAS COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 12 MESES**

3.3.1 Características gerais da solução

3.3.1.1 A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:

3.3.1.1.1 Windows Server 2000;
3.3.1.1.2 Windows Server 2003 SP1 e 2003 R2 SP2;
3.3.1.1.3 Windows Server 2008 e 2008 R2;
3.3.1.1.4 Windows Server 2012 e 2012 R2;
3.3.1.1.5 Windows Server 2016;
3.3.1.1.6 Windows Server 2019;
3.3.1.1.7 Red Hat Enterprise 5, 6, 7 e 8;
3.3.1.1.8 CentOS 5, 6, 7 e 8;
3.3.1.1.9 Oracle Linux 5, 6, 7 e 8;
3.3.1.1.10 SUSE Linux Enterprise Server 10, 11, 12 e 15;
3.3.1.1.11 Ubuntu 10, 12, 14, 16, 18 e 20;
3.3.1.1.12 Debian 6, 7, 8, 9 e 10;
3.3.1.1.13 Cloud Linux 5, 6, 7 e 8;
3.3.1.1.14 Solaris 10 1/13 Sparc;
3.3.1.1.15 Solaris 10 1/13 (x86/x64);
3.3.1.1.16 Solaris 11.2/ 11.3 Sparc;
3.3.1.1.17 Solaris 11.2/ 11.3 (x86/x64);
3.3.1.1.18 Solaris 11.4 (x86, x64 ou SPARC)
3.3.1.1.19 Amazon Linux e Amazon Linux 2 (x64).

3.3.1.2 A solução deverá ser compatível e homologada com plataformas de virtualização tendo parceria com, pelo menos, Vmware, Microsoft e Nutanix;

3.3.1.3 A console de gerenciamento deverá ser em nuvem ou on-premises, permitindo o gerenciamento das políticas de segurança através da Internet;

3.3.1.4 A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer, Google Chrome e Firefox. Deve ainda suportar certificado digital para gerenciamento;

3.3.1.5 A solução deverá permitir a integração com pelo menos as seguintes plataformas de nuvem: Vmware vCloud, MS Azure e AWS;

3.3.1.6 Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;

3.3.1.7 A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;

3.3.1.8 A console de administração deverá permitir o envio de notificações via SMTP;

3.3.1.9 Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;

3.3.1.10 A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;
3.3.1.11 A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;
3.3.1.12 A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;
3.3.1.13 A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda ou agendado com o envio automático do relatório via e-mail;
3.3.1.14 A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;
3.3.1.15 A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;
3.3.1.16 A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS aplicadas e Firewall;
3.3.1.17 Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade;
3.3.1.18 A console deve se integrar com o Active Directory para que os usuários do Active Directory possam administrar a solução de acordo com as permissões;
3.3.1.19 A console deve se integrar com o Active Directory para que possa ser efetuado o controle das máquinas no Active Directory;
3.3.1.20 Para efeito de administração, deve ser possível de se replicar a estrutura do Active Directory na console de administração;
3.3.1.21 A solução de segurança ter a capacidade de identificar ataques entre contêineres;
3.3.1.22 Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";
3.3.1.23 Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas políticas de segurança;
3.3.1.24 A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;
3.3.1.25 Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;
3.3.1.26 A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;
3.3.1.27 Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;
3.3.1.28 Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;
3.3.1.29 Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;

3.3.1.30 Para efeito de administração, a solução deverá avisar quando um agente encontrar-se desconectado da sua console de gerenciamento;
3.3.1.31 A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;
3.3.1.32 Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;
3.3.1.33 A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação;
3.3.1.34 A solução deverá mostrar quais máquinas estão usando determinada política;
3.3.1.35 Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;
3.3.1.36 Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;
3.3.1.37 Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;
3.3.1.38 O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;
3.3.1.39 Também deverá ser possível realizar o rastreamento por portas abertas, identificando possíveis serviços ativos e escutando;
3.3.1.40 A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;
3.3.1.41 A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;
3.3.1.42 A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;
3.3.1.43 A solução deverá ter a capacidade de se integrar com o Amazon SNS e os principais softwares de SIEMs contemplando, no mínimo: Splunk, IBMQradar e HPArcSight de modo a permitir enviar os seus logs para essas soluções;
3.3.1.44 A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;
3.3.1.45 Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;
3.3.1.46 Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;
3.3.1.47 A lista de contatos de recebimento de relatório poderá ser obtida através do Active Directory;
3.3.1.48 As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;
3.3.1.49 Após a atualização deve ser informado o que foi modificado ou adicionado;
3.3.1.50 Deve ser possível baixar as assinaturas na console de gerenciamento, mas não distribuí-las aos clientes;
3.3.1.51 A console de gerenciamento deve apresentar a capacidade de gerar rollback de suas atualizações de regras;
3.3.1.52 A solução deverá ter capacidade de gerar pacote de auto diagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;
3.3.1.53 Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;

3.3.1.54 No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;
3.3.1.55 Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;
3.3.1.56 Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;
3.3.1.57 Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;
3.3.1.58 O fabricante deverá participar do programa "Microsoft Application Protection Program" para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;
3.3.1.59 A console de gerenciamento deve se integrar com o Vmware vCloud, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;
3.3.1.60 O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos;
3.3.1.61 A solução deve possuir API documentada para integração na esteira de automação;
3.3.1.62 A documentação da API deve conter exemplos prontos para implementação de determinadas funcionalidades, como cookbooks;
3.3.1.63 Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;
3.3.1.64 A solução deve permitir desabilitar os módulos individualmente;
3.3.1.65 Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador.

3.3.2 Anti-malware

3.3.2.1 A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;
3.3.2.2 A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;
3.3.2.3 A solução deve possuir listas de exclusão separadas por módulo da proteção anti-malware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;
3.3.2.4 A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;
3.3.2.5 A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;
3.3.2.6 A solução deverá oferecer escanear processos em memória em busca de Malware;
3.3.2.7 O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;

3.3.2.8 O scan de arquivos comprimidos do tipo OLE deverá ser de no mínimo 20 camadas de compressão;
3.3.2.9 A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;
3.3.2.10 A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado;
3.3.2.11 Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware;
3.3.2.12 Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;
3.3.2.13 Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no servidor;
3.3.2.14 A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs.

3.3.3 Proteção contra URL's maliciosas

3.3.3.1 Deve permitir a proteção contra acesso a websites ou URL's consideradas maliciosas ou de baixa reputação;
3.3.3.2 A lista de URL's deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URL's acessadas;
3.3.3.3 A solução deve permitir alterar o nível de sensibilidade para detecção de URL's maliciosas tendo, pelo menos, os níveis Alto, médio e baixo;
3.3.3.4 Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URL's especificadas pelo administrador do sistema;
3.3.3.5 Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;
3.3.3.6 Deverá ter capacidade de identificar acessos a URL's maliciosas além das portas padrão 80 e 443;
3.3.3.7 A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante para evitar falsos positivos;
3.3.3.8 A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.

3.3.4 Firewall

3.3.4.1 Operar como firewall de host, através da instalação de agente nos servidores protegidos;
3.3.4.2 Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;
3.3.4.3 Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP;
3.3.4.4 Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;
3.3.4.5 A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS Fingerprint por até 30 minutos;
3.3.4.6 Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

3.3.4.7 Precisa ter a capacidade de definição de regras para contextos específicos;
3.3.4.8 Precisa ter a capacidade de realização de varredura de portas nos servidores;
3.3.4.9 Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de IP'S, lista de MAC's, lista de portas;
3.3.4.10 Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);
3.3.4.11 Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;
3.3.4.12 O firewall deverá ser stateful bidirecional;
3.3.4.13 O firewall deverá permitir liberar ou apenas logar eventos;
3.3.4.14 O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;
3.3.4.15 As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;
3.3.4.16 A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;
3.3.4.17 As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;
3.3.4.18 Deverá realizar pseudo stateful em tráfego UDP;
3.3.4.19 Deverá logar a atividade stateful;
3.3.4.20 Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;
3.3.4.21 Deverá permitir limitar o número de meias conexões vindas de um computador;
3.3.4.22 Deverá prevenir ack storm;
3.3.4.23 Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;
3.3.4.24 Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período de tempo configurado pelo administrador;
3.3.4.25 Deverá permitir criar lista de exceções para identificar os IP's autorizados a realizar varreduras de portas ou da rede;
3.3.4.26 Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

3.3.5 Proteção de vulnerabilidades de SO e aplicações

3.3.5.1 Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;
3.3.5.2 Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;
3.3.5.3 A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;

3.3.5.4 Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

3.3.5.5 Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

3.3.5.6 Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

3.3.5.7 Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

3.3.5.8 Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;

3.3.5.9 Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

3.3.5.10 Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

3.3.5.11 Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;

3.3.5.12 Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);

3.3.5.13 Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

3.3.5.14 Deverá ser capaz de inspecionar tráfego criptografado de entrada;

3.3.5.15 Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;

3.3.5.16 As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

3.3.5.17 Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;

3.3.5.18 Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;

3.3.5.19 Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;

3.3.5.20 Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;

3.3.5.21 As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;

3.3.5.22 As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;
3.3.5.23 As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs;
3.3.5.24 As regras de IPS poderão ter sua capacidade de LOG desabilitado;
3.3.5.25 As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;
3.3.5.26 As regras devem ser atualizadas automaticamente pelo fabricante;
3.3.5.27 Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

3.3.6 Monitoramento de integridade

3.3.6.1 A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;
3.3.6.2 Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;
3.3.6.3 A solução deverá fazer uso da tecnologia Intel TPM/TXT para monitorar a integridade contra mudanças não autorizadas a nível do Hypervisor;
3.3.6.4 Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux;
3.3.6.5 Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional;
3.3.6.6 Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;
3.3.6.7 Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;
3.3.6.8 Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
3.3.6.9 O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;
3.3.6.10 Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real- time para ambiente Linux;
3.3.6.11 Deverá logar e colocar em relatório todas as modificações que ocorram;
3.3.6.12 As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;
3.3.6.13 Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;
3.3.6.14 Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;
3.3.6.15 Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.

3.3.7 Inspeção de logs

3.3.7.1 A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX;

3.3.7.2 Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;
3.3.7.3 Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
3.3.7.4 Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;
3.3.7.5 Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;
3.3.7.6 Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;
3.3.7.7 Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;
3.3.7.8 Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;
3.3.7.9 Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;
3.3.7.10 Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram;
3.3.7.11 As regras poderão ser modificadas por severidade de ocorrência de eventos;
3.3.7.12 As regras devem se atualizar automaticamente pelo fabricante;
3.3.7.13 Permitir modificação pelo administrador em regras para adequação ao ambiente.

3.3.8 Controle de aplicações

3.3.8.1 A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;
3.3.8.2 O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;
3.3.8.3 O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina;
3.3.8.4 A console deverá exibir eventos de no mínimo 30 dias;
3.3.8.5 A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período de tempo que deve ser no máximo 10 horas;
3.3.8.6 A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.

3.3.9 Detecção e Resposta (XDR)

3.3.9.1 A solução deve ser compatível com Linux e Windows Server 2008 R2 e superiores;
3.3.9.2 A solução deve possuir módulo de investigação, detecção integrados;
3.3.9.3 Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;
3.3.9.4 A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

3.3.9.5 Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;
3.3.9.6 O módulo de XDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;
3.3.9.7 Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;
3.3.9.8 A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;
3.3.9.9 A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;
3.3.9.10 A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;
3.3.9.11 Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;
3.3.9.12 Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;
3.3.9.13 Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;
3.3.9.14 Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;
3.3.9.15 Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;
3.3.9.16 Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;
3.3.9.17 A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);
3.3.9.18 Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

3.4 SERVIÇO DE SUPORTE ESPECIALIZADO PARA INSTALAÇÃO, MIGRAÇÃO E SUPORTE PREVENTIVO/CORRETIVO

3.4.1 Serviço de suporte especializado para ajustes, configurações, migrações e implementação da solução a ser fornecida;
3.4.2 Além do serviço inicial de instalação e configuração, neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução, seja este corretivo ou preventivo, bem como a transferência de conhecimento;
3.4.3 O serviço deverá ser realizado de forma remota, num período de 30 dias, juntamente ao processo de instalação, migração da solução, não podendo ser renovado além do período especificado;
3.4.4 Para prestação destes serviços, a CONTRATADA deverá empregar funcionários devidamente qualificados na utilização desse tipo de ferramenta, a ser comprovado através de apresentação de certificados emitidos pelo próprio fabricante, ou instituições por ele autorizados;

3.4.5 O serviço em questão deve atuar em conjunto com o suporte especializado do fabricante para atuação na manutenção e aplicação das melhores práticas no ambiente;

3.4.6 A CONTRATADA deverá prover equipe técnica especializada própria para atuar nas demandas da CONTRATANTE durante o processo de migração e transferência de conhecimento.

4. VISTORIA PARA LICITAÇÃO

4.1 Para esta contratação não se aplica Vistoria

5. REQUISITOS DA CONTRATAÇÃO

5.1 Declaração do licitante de que tem pleno conhecimento das condições necessárias para a prestação do serviço, bem como de que atende os requisitos de habilitação para contratar com a administração pública;

5.2 **Apresentação de declaração do fabricante, nominal ao processo, informando que a empresa é parceira autorizada a comercializar os softwares descritos no objeto deste documento**.

5.3 Período de vigência de 12 (doze) meses, podendo ser renovado até um prazo máximo de 60 nesses.

6. MODELO DE EXECUÇÃO DO OBJETO

6.1 A execução do objeto seguirá a seguinte dinâmica:

6.1.1 Os serviços serão prestados no Conselho Regional de Medicina do Estado da Bahia, localizada na Rua Guadalajara, 175, Morro do Gato, barra – Salvador – Ba (Remotamente ou por telefone) em horário comercial.

6.1.2 Os procedimentos, metodologias e tecnologias a serem empregadas deverão estar de acordo com o Termo de Referência e seus anexos.

6.1.3 Durante o período de vigência contratual, a CONTRATADA deverá garantir a atualização tecnológica dos produtos na forma de atualizações de programas.

6.1.4 As atualizações de programas deverão cobrir todos os programas de computador (software) de propriedade do CREMEB e incluir o fornecimento de correções (patches) e novas versões/revisões/distribuições (releases) assim que o fabricante as torne disponíveis;

6.1.5 Entende-se por atualização de programas qualquer correção, pequena modificação, aperfeiçoamento (update), ou desenvolvimento de nova versão (upgrade) efetuado pelo fabricante para os produtos em questão;

6.1.6 Os procedimentos, metodologias e tecnologias a serem empregadas deverão estar de acordo com o Termo de Referência e seus anexos.

6.1.7 O fabricante deve fornecer um canal através do seu web site para abertura de chamados, os quais serão continuados através de e-mail, contato telefone e eventualmente acesso remoto.

6.1.8 A Equipe Técnica do DETIN/CREMEB analisará periodicamente o andamento das atividades contratadas.

6.1.9 Estando o resultado da análise de acordo com as condições contratuais, a Equipe Técnica do DETIN/CREMEB atestará tecnicamente a execução dos serviços, informando ao gestor

do contrato via mensagem eletrônica (preferencialmente) ou via ofício (se alguma situação assim requerer).

6.1.10 Havendo alguma pendência técnica, a Equipe Técnica do DETIN/CREMEB solicitará à CONTRATADA a devida correção, sem prejuízo de eventuais penalidades que venham a ser aplicadas, informando ao gestor do contrato via mensagem eletrônica, preferencialmente; ou via ofício, se alguma situação assim requerer.

7. MODELO DE GESTÃO DO CONTRATO E CRITÉRIOS DE MEDIÇÃO:

7.1 Caberá ao Coordenador do Departamento de Tecnologia da Informação do CREMEB (DETIN/CREMEB), realizar a fiscalização *(execução e ações coordenadas junto à área de contratos)* do Contrato Administrativo decorrente da presente contração pretendida;

7.2 Caberá à área de Contratos do CREMEB (DECOMP/CREMEB) realizar a gestão do Contrato, no que se refere a intermediação de pagamentos, aplicação de sanções, apuração da avaliação da execução do serviço (avaliação do fornecedor) e etc.

7.3 Os mecanismos de comunicação a serem estabelecidos entre o CREMEB e a prestadora de serviços serão: contato presencial, contato telefônico e e-mail. Os endereços de e-mail e telefone deverão ser informados no momento de formalização do contrato.

8. GARANTIA, ASSISTÊNCIA TÉCNICA E DECLARAÇÕES

8.1 A contratação deve permitir que o fabricante preste atendimentos de suporte técnico através de chamados abertos em seu portal de chamados e permitir que a **CONTRATANTE** possa obter novas versões do software para manter sua solução instalada mais atualizada possível.

9. OBRIGAÇÕES DA CONTRATANTE

9.1 Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

9.2. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

9.3. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;

9.4. Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência;

9.5. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da contratada, no que couber, em conformidade com o item 6 do Anexo XI da IN SEGES/MP n. 5/2017.

9.6. Não praticar atos de ingerência na administração da Contratada, tais como: Direcionar a contratação de pessoas para trabalhar nas empresas Contratadas;

9.7. Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;

9.8. Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;

9.9. Arquivar, entre outros documentos: especificações técnicas, orçamentos, termos de recebimento, contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do serviço e notificações expedidas;

9.10. Fiscalizar o cumprimento dos requisitos legais, quando a contratada houver se beneficiado da preferência estabelecida pelo art. 3º, § 5º, da Lei nº 8.666, de 1993.

9.11. Providenciar local adequado para o recebimento do objeto;

9.12. Fiscalizar e inspecionar o objeto entregue, podendo rejeitá-lo quando este não atender ao especificado;

9.13. Fornecer, a qualquer tempo, mediante solicitação escrita da vencedora, informações adicionais, dirimir dúvidas e orientá-la em todos os casos omissos que ocorrerem.

9.14. Atestar a nota fiscal/fatura após o recebimento definitivo e enviar à área de gestão de contratos para efetuar o pagamento nas condições pactuadas.

10. OBRIGAÇÕES DA CONTRATADA

10.1. Fornecer os softwares e executar os serviços conforme especificações deste Termo de Referência e de sua proposta, além de fornecer e utilizar os equipamentos necessários, na qualidade e quantidade mínimas especificadas neste Termo de Referência e em sua proposta;

10.2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

10.3. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à União ou à entidade federal, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

10.4. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

10.5. Vedar a utilização, na execução dos serviços, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão Contratante, nos termos do artigo 7° do Decreto n° 7.203, de 2010;

10.6. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado.

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

10.8. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

10.9. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social, bem como as regras de acessibilidade previstas na legislação, quando a contratada houver se beneficiado da preferência estabelecida pela Lei nº 13.146, de 2015.

10.10. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

10.11. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o

atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

10.12. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;

10.13. Assegurar à CONTRATANTE, em conformidade com o previsto no subitem 6.1, "a"e "b", do Anexo VII – F da Instrução Normativa SEGES/MP nº 5, de 25/05/2017:

10.14. O direito de propriedade intelectual dos produtos desenvolvidos, inclusive sobre as eventuais adequações e atualizações que vierem a ser realizadas, logo após o recebimento de cada parcela, de forma permanente, permitindo à Contratante distribuir, alterar e utilizar os mesmos sem limitações;

10.15. Os direitos autorais da solução, do projeto, de suas especificações técnicas, da documentação produzida e congêneres, e de todos os demais produtos gerados na execução do contrato, inclusive aqueles produzidos por terceiros subcontratados, ficando proibida a sua utilização sem que exista autorização expressa da Contratante, sob pena de multa, sem prejuízo das sanções civis e penais cabíveis. Fornecer o objeto cotado em estrita conformidade com as especificações constantes deste Termo de Referência;

10.16. Entregar objeto no prazo fixado;

10.17. Substituir no prazo de 15 (quinze) dias o objeto que, após a entrega, apresentarem defeitos ou vierem a apresentar durante o período de garantia.

11. DA SUBCONTRATAÇÃO

11.1. Não será admitida a subcontratação do objeto licitatório.

12. ALTERAÇÃO SUBJETIVA

12.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

13. CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

13.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, que serão exercidos por um ou mais representantes da Contratante, especialmente designados, na forma dos Arts. 67 e 73 da Lei nº 8.666, de 1993.

13.2. O representante da Contratante deverá ter a qualificação necessária para o acompanhamento e controle da execução dos serviços e do contrato.

13.3. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

13.4. A fiscalização do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade

responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos no § 1º do artigo 65 da Lei nº 8.666, de 1993.

13.5. A conformidade do material/técnica/equipamento a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da Contratada que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste Termo de Referência, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

13.6. O representante da Contratante deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 67 da Lei nº 8.666, de 1993.

13.7. O descumprimento total ou parcial das obrigações e responsabilidades assumidas pela Contratada ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 77 e 87 da Lei nº 8.666, de 1993.

13.8. As atividades de gestão e fiscalização da execução contratual devem ser realizadas de forma preventiva, rotineira e sistemática, podendo ser exercidas por servidores, equipe de fiscalização ou único servidor, desde que, no exercício dessas atribuições, fique assegurada a distinção dessas atividades e, em razão do volume de trabalho, não comprometa o desempenho de todas as ações relacionadas à Gestão do Contrato.

13.9. A fiscalização técnica dos contratos avaliará constantemente a execução do objeto, devendo haver o redimensionamento no pagamento com base nos indicadores estabelecidos, sempre que a CONTRATADA:

a) não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou
b) Fornecer o objeto cotado em estrita conformidade com as especificações constantes deste Termo de Referência, bem como entregá-lo no prazo fixado;

13.9 Substituir no prazo de 15 (quinze) dias o objeto que, após a entrega, apresentarem defeitos ou vierem a apresentar durante o período de garantias e irregularidades constatadas.

13.10 O CONTRATANTE exercerá, através de seu preposto, Indaian Souza Barros – Coordenador do Departamento de Tecnologia da Informação, a fiscalização do objeto deste certame, o qual terá poder para:

a) Transmitir à CONTRATADA as instruções e determinações que julgar necessárias: Exigir da CONTRATADA o cumprimento rigoroso das obrigações assumidas;
b) Sustar o pagamento dos serviços pendentes, no caso de inobservância pela CONTRATADA das obrigações pactuadas;
c) Aceitar, quando julgar procedente, as justificativas apresentadas, por escrito, pela CONTRATADA, na hipótese de infração contratual deste.

13.11 As disposições previstas nesta cláusula não excluem o disposto no Anexo VIII da Instrução Normativa SLTI/MP nº 05, de 2017, aplicável no que for pertinente à contratação.

13.12 A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade

inferior e, na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes, gestores e fiscais, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

14 DO RECEBIMENTO E ACEITAÇÃO DO OBJETO

14.1 A emissão da Nota Fiscal/Fatura deve ser precedida do recebimento definitivo dos serviços, nos termos abaixo.

14.2 No prazo de até *5 dias corridos* a CONTRATADA deverá entregar toda a documentação comprobatória do cumprimento da obrigação contratual;

14.2.1 A Contratada fica obrigada a reparar, corrigir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução.

14.2.2 O recebimento definitivo ficará sujeito, quando cabível, à conclusão de todos os testes e à entrega dos Manuais e Instruções exigíveis.

14.2.3 A CONTRATADA poderá verificar junto ao fabricante a integridade da licença de software ofertada pela CONTRATANTE.

14.3 No prazo de até *10 dias corridos* a partir do recebimento dos documentos da CONTRATADA, o fiscal do contrato deverá elaborar Relatório Circunstanciado em consonância com suas atribuições, e encaminhá-lo ao gestor do contrato.

15 DO PAGAMENTO

15.1 O pagamento ocorrerá até o 5º (quinto) dia útil do mês subsequente a execução do objeto, mediante a apresentação da nota fiscal eletrônica/fatura, devidamente atestada pelo fiscal do contrato

15.2 A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

15.2.1 Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

15.3 O setor competente para proceder o pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

15.3.1 o prazo de validade;

15.3.2 a data da emissão;

15.3.3 os dados do contrato e do órgão contratante;

15.3.4 o período de prestação dos serviços;

15.3.5 o valor a pagar; e

15.3.6 eventual destaque do valor de retenções tributárias cabíveis.

15.4 Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante;

15.5 Nos termos do item 1, do Anexo VIII-A da Instrução Normativa SEGES/MP nº 05, de 2017, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

15.5.1 não produziu os resultados acordados;

15.5.2 deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

15.5.3 deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

15.6 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

15.7 Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

15.8 Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

15.9 Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

15.10 Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

15.11 Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

15.12 Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

15.12.1 Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

15.13 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1993, nos termos do item 6 do Anexo XI da IN SEGES/MP n. 5/2017, quando couber.

15.14 É vedado o pagamento, a qualquer título, por serviços prestados, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão contratante, com fundamento na Lei de Diretrizes Orçamentárias vigente.

15.15 Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) \qquad I = \frac{(6/100)}{365}$$

I = 0,00016438
TX = Percentual da taxa anual = 6%

16 REAJUSTE

16.1 Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

16.2 Após o interregno de um ano os preços iniciais serão reajustados, mediante a aplicação, pela CONTRATANTE, do índice IPCA/IBGE, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, com base na seguinte fórmula (art. 5º do Decreto n.º 1.054, de 1994):

R = V (I – Iº) / Iº, onde:
R = Valor do reajuste procurado;
V = Valor contratual a ser reajustado;
Iº = índice inicial - refere-se ao índice de custos ou de preços correspondente à data fixada para entrega da proposta na licitação;
I = Índice relativo ao mês do reajustamento;

16.3 Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste

16.4 Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

16.5 No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

16.6 Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

16.7 Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

16.8 Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

16.9 O reajuste será realizado por apostilamento.

17 GARANTIA DA EXECUÇÃO

17.1 As garantias de execução devem seguir as garantias descritas no item 8.1 deste termo de referência.

18 DAS SANÇÕES ADMINISTRATIVAS

18.1 Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a CONTRATADA que:

18.1.1 inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

18.1.2 ensejar o retardamento da execução do objeto;

18.1.3 falhar ou fraudar na execução do contrato;

18.1.4 comportar-se de modo inidôneo; ou

18.1.5 cometer fraude fiscal.

18.2 Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

18.2.1 Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

18.2.2 Multa de:

18.2.2.1 1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

18.2.2.2 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida;

18.2.2.3 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

18.2.2.4 0,2% a 3,2% por dia sobre o valor mensal do contrato, conforme detalhamento constante das tabelas 1 e 2, abaixo; e

18.2.2.5 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

18.2.2.6 as penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

18.2.3 Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

18.2.4 Sanção de impedimento de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos

18.2.4.1 A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 19.1 deste Termo de Referência.

18.2.5 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

18.3 As sanções previstas nos subitens 19.2.1, 19.2.3, 19.2.4 e 19.2.5 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

18.4 Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas 1 e 2:

Tabela 1

GRAU	CORRESPONDÊNCIA
1	0,2% ao dia sobre o valor mensal do contrato
2	0,4% ao dia sobre o valor mensal do contrato
3	0,8% ao dia sobre o valor mensal do contrato
4	1,6% ao dia sobre o valor mensal do contrato
5	3,2% ao dia sobre o valor mensal do contrato

Tabela 2

INFRAÇÃO		
ITEM	**DESCRIÇÃO**	**GRAU**
1	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento;	04
2	Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia;	02
Para os itens a seguir, deixar de:		
1	Cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência;	02
2	Indicar e manter durante a execução do contrato os prepostos previstos no edital/contrato;	01

18.5 Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

18.5.1 tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

18.5.2 tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

18.5.3 demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

18.6 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

18.7 As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

18.7.1 Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

18.8 Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

18.9 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

18.10 Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

18.11 A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

18.12 O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

18.13 As penalidades serão obrigatoriamente registradas no SICAF.

19 CRITÉRIOS DE SELEÇÃO DO FORNECEDOR.

19.1 As exigências de habilitação jurídica e de regularidade fiscal e trabalhista são as usuais para a generalidade dos objetos, conforme disciplinado no edital.

19.2 Os critérios de qualificação econômica a serem atendidos pelo fornecedor estão previstos no edital.

19.3 Os critérios de qualificação técnica a serem atendidos pelo fornecedor estão previstas no Edital:

19.4 Os critérios de aceitabilidade de preços serão:

18.4.1 Valor máximo Global: **R$ (118.985,93).**

18.4.2 Valores por itens: conforme planilha de composição de preços informa neste Termo de Referência.

19.5 O critério de julgamento da proposta é o menor preço global por grupo

19.6 As regras de desempate entre propostas são as discriminadas no edital.

20 ESTIMATIVA DE PREÇOS E PREÇOS REFERENCIAIS.

20.1 O valor máximo aceitável, por item, para a contratação, será conforme Planilha abaixo:

Item	Descrição do item	Qtd.	Preço Unit (R$)	Preço Total (R$)
1	Software de segurança para usuário final, incluindo garantia, atualização e suporte. Período de 12 meses.	200	R$ 406,63	R$ 81.326,00
2	Software de segurança para cargas de trabalho híbridas com detecção e resposta, incluindo garantia, atualização e suporte. Período de 12 meses	20	R$ 1.149,63	R$ 22.992,60
3	Serviço de Suporte Especializado para Instalação, Migração e Suporte Preventivo/Corretivo por 30 dias.	1	R$ 14.666,67	R$ 14.666,67
	Valor Global	**R$ 118.985,27**		

21 DAS PROPOSTAS DE PREÇOS

21.1 A proposta deverá compreender os encargos sociais bem com todas e quaisquer despesas de responsabilidade da proponente que direta ou indiretamente decorram do objeto licitado.

21.2 Os valores da proposta de preços deverão indicar o valor unitário e o valor total de cada um dos itens.

21.3 As propostas de preços deverão ser ofertadas em conformidade com as descrições e especificações detalhadas de cada um dos itens, atendendo a integralidade dos hardwares e softwares.

22 DOS RECURSOS ORÇAMENTÁRIOS.

22.1 As despesas referentes a aquisição do Objeto correrão através do Centro de custo nº 07.03 – AQUISIÇÃO DE SOFTWARE

22.2 A Classificação Orçamentária para efetivação da aquisição do objeto correrá através dos Elementos:

a) Aquisição de Software - Cód. 6.2.2.1.1.33.90.39.045

b) Manutenção De Sistemas De Informática – Software – Cód. 6.2.2.1.133.90.39.010

23 DO PRAZO DA ENTREGA E DA CONFERÊNCIA

23.1 O prazo máximo de entrega do objeto será 30 (trinta) dias corridos, a contar do envio da Autorização de Fornecimento.

23.2 Os objetos da licitação deverão ser entregues no endereço abaixo:

23.3 A entrega deverá ser realizada na sede do CREMEB, na Rua Guadalajara, 175 Morro do Gato – Barra, Salvador (BA), no horário das 08:00 às 11:00h e das 14:00 às 16:30h.

23.4 A entrega deverá ser realizada no horário das 08:00 às 11:00h e das 14:00 às 16:30h e na conferência dos itens recebidos para liberação da Nota Fiscal para pagamento, a descoberta de um item em desconformidade com o solicitado, será motivo de devolução da Nota Fiscal e de todos os itens para que a contratada proceda com os devidos ajustes, sem interrupção do prazo inicialmente dado para a entrega do pedido.

Salvador de 08 de agosto de 2022

Indaian Souza Barros
Coordenador do Departamento de Tecnologia - DETIN