TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS
Palácio da Justiça Rio Tocantins, Praça dos Girassóis, sn - Bairro Centro - CEP 77015007 - Palmas - TO - http://wwa.tjto.jus.br
Tribunal de Justiça

Contrato Nº 137/2020 - PRESIDÊNCIA/DIGER/DIADM/DCC

PREGÃO ELETRÔNICO - SRP Nº 79/2019
ATA DE REGISTRO DE PREÇOS Nº 107/2020
PROCESSO ORIGINÁRIO 19.0.000023571-0
PROCESSO 20.0.000016856-5

CONTRATO QUE CELEBRAM ENTRE SI O TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS E A EMPRESA LINK CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO - EIRELI.

Pelo presente Instrumento e na melhor forma de direito, o **TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS**, inscrito no CNPJ/MF sob o nº 25.053.190/0001-36, com sede na Praça dos Girassóis, s/nº, centro, em Palmas/TO, neste ato representado por seu Presidente, o Excelentíssimo Senhor Desembargador **HELVÉCIO DE BRITO MAIA NETO**, brasileiro, portador do RG nº 125.824, 2ª Via - SSP/TO, inscrito no CPF/MF sob nº 103.573.945-34, residente e domiciliado nesta Capital, doravante designado **CONTRATANTE** e, do outro lado, a empresa **LINK CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO - EIRELI**, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº **23.114.739/0001-20**, com sede na SRTVS Qd. 701 Conj. L Bloco 01, nº 38 sala 17 Parte "A" – Sobreloja – Asa Sul, Brasília/DF, doravante designada **CONTRATADA**, neste ato representada por seu procurador, o Senhor **WARLEN SOARES BRANDÃO,** brasileiro, portador do RG nº 2171667 - SSP/DF, inscrito no CPF/MF sob o nº 983.963.071-72, tem entre si, justo e avençado o presente Contrato, observadas as disposições da Lei nº. 10.520/2002 e, subsidiariamente pela Lei nº. 8.666/1993, mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO:

1.1. O presente Instrumento tem por objeto a aquisição de solução de segurança, para atender as demandas do Poder Judiciário do Estado do Tocantins, conforme especificações e quantitativos estabelecidos abaixo:

GRUPO	ITEM	DESCRIÇÃO	UND.	QTDE.	VALOR UNITÁRIO	VALOR TOTAL
3	10	**Equipamento web application firewall:** **Marca:** F5; **Fabricante:** F5; **Modelo:** F5-BIG-LTM-I2600 Descrição: BIG-IP SWITCH: LOCAL TRAFFIC MANAGER I2600 (16G, BASE SSL & COMP) / 05 ANOS BIG-IP SERVICE: PREMIUM CAT HW53 EDI ONLY / 2 x 250W AC POWER SUPPLY (I2XXX) / 4 x SFP COPPER CONNECTOR (10/100/1000 RJ45) / BIG-IP ADDON: APPLICATION SECURITY MANAGER MODULE (I2XXX)/ BIG-IP SERVICE: PREMIUM CAT SW50 5 ANOS/ BIG-IP; **PRODUCT:** SBS IP INTELLIGENCE LICENSE 5 (CINCO) ANOS (3600)	Und.	2	R$ 479.000,00	R$ 958.000,000
	11	Instalação e configuração - **web application firewall.**	Und.	1	R$ 46.706,67	R$ 46.706,67
	12	Treinamento básico e avançado – **web application firewall.**	Und.	1	R$ 11.000,00	R$ 11.000,00
Valor total						**R$ 1.015.706,67**

1.2. A aquisição citada na subcláusula 1.1 obedecerá ao estipulado neste Contrato, bem como as especificações técnicas, forma de execução/entrega e as disposições dos documentos adiante enumerados, constantes do Processo Administrativo 19.0.000023571-0 e 20.0.000016856-5 do CONTRATANTE, e que, independentemente de transcrição, fazem parte integrante e complementar deste, no que não o contrariarem. São eles:

1.2.1. O Edital do Pregão Eletrônico – SRP 79/2019, do CONTRATANTE;

1.2.2. A Ata de Registro de Preços nº 107/2020, resultado do Pregão Eletrônico – SRP nº 79/2019; e

1.2.3. A proposta de preços e documentos que o acompanham, firmada pela CONTRATADA em 25 de junho de 2020.

1.3. A aquisição do objeto deste Contrato foi realizada por meio de procedimento licitatório, de acordo com o disposto no art. 1º e parágrafo único e art. 2º parágrafo 1º da Lei nº. 10.520/2002, sob a modalidade Pregão, na forma eletrônica, para registro de preços, conforme Edital e Processo Administrativo acima citados.

1.4. A CONTRATADA fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

1.5. Nenhum acréscimo poderá exceder os limites estabelecidos no subitem anterior, salvo as supressões que poderão exceder os limites legais, quando acordadas entre as Partes.

CLÁUSULA SEGUNDA – DAS ESPECIFICAÇÕES TÉCNICAS MÍNIMAS:

2.1. Características Gerais Comuns a Todos Equipamentos:

2.1.1. Os equipamentos deverão ser do tipo *appliance*, novos, de primeiro uso, sem qualquer tipo de recondicionamento;

2.1.2. Por appliance, entende-se o conjunto de hardware, software e licenças necessárias para o seu completo funcionamento e atendimento de todas as funcionalidades deste Termo de Referência;

2.1.3. Na data de apresentação da proposta, nenhum dos modelos ofertados poderá estar caracterizado como *end-of-life* ou *end-of-sale* pelo fabricante;

2.1.4. Os *appliances* deverão suportar o monitoramento remoto através do protocolo SNMP, nas versões 2 e/ou 3;

2.1.5. Caso o equipamento possua interfaces combinadas (combo), apenas um tipo de conectividade das mesmas será considerado para quantificar o total de interfaces do equipamento;

2.1.6. Caso o equipamento necessite de algum tipo de licenciamento, o mesmo deve ser providenciado em caráter perpétuo, de forma a viabilizar a operação mesmo após o término da garantia;

2.1.7. Características que dependam de atualização junto ao fabricante (ex.: assinaturas de aplicações) devem continuar operacionais por tempo indeterminado, valendo-se da última atualização disponível dentro do prazo de vigência da garantia;

2.1.8. Automaticamente e sem custos adicionais, deverá ser possível o acesso ao conteúdo mais recente dos produtos, funcionalidades adicionais e correções de produtos disponibilizadas pelo fabricante (*features, releases, fixes, service packs, patches* de segurança e outros);

2.1.9. A CONTRATADA deve prover notificações automáticas de atualizações/correções disponíveis, alertas de segurança e divulgações de atualizações;

2.1.10. Na atualização de versões, a CONTRATADA deverá garantir o apoio técnico necessário para instalação e operação das últimas versões, sem custos adicionais.

2.2. Características Gerais - Equipamento Firewall Tipo 1, 2 e 3:

2.2.1. Os equipamentos devem possuir, no mínimo, as seguintes funcionalidades:

2.2.1.1. Suportar a definição de VLANs conforme o padrão IEEE 802.1q, permitindo o estabelecimento de regras de filtragem *stateful;*

2.2.1.2. Suportar o protocolo 802.3ad, permitindo a configuração de *port aggregation* (*ethernet bonding*) de interfaces, seja para aumento de *throughput* ou para alta disponibilidade. Aplicável apenas aos equipamentos tipo 2 e 3;

2.2.1.3. Suportar a implementação de sub-interfaces *ethernet* lógicas;

2.2.1.4. Suportar aplicação de *policy based routing* ou *policy based fowarding;*

2.2.1.5. Suportar roteamento *multicast;*

2.2.1.6. Suportar DHCP em modo *server* ou *relay;*

2.2.1.7. Suportar *Jumbo Frames.* Aplicável apenas aos equipamentos tipo 2 e 3;

2.2.1.8. Suportar os seguintes tipos de NAT:

2.2.1.8.1. *Many-to-one*;

2.2.1.8.2. *Many-to-many*;

2.2.1.8.3. *One-to-one*;

2.2.1.8.4. *One-to-many*;

2.2.1.8.5. *Source* NAT e *destination* NAT simultâneos;

2.2.1.8.6. *Port translation* (PAT).

2.2.1.9. Prover mecanismo de prevenção de falsificação de endereço (IP *Spoofing*), permitindo especificar qual interface de rede a comunicação deve se originar;

2.2.1.10. Suportar integralmente o protocolo IPv6, bem como permitir que sejam criados objetos que utilizem endereços IPv4 ou IPv6. Aplicável apenas aos equipamentos tipo 2 e 3;

2.2.1.11. Suportar roteamento estático IPv4 e dinâmico através dos protocolos RIPv2, BGP e OSPFv2;

2.2.1.12. *Hardware* e *software* que compõem o *appliance* devem ser do mesmo fabricante;

2.2.1.13. O licenciamento do *appliance* deverá contemplar um número ilimitado de usuários e endereços de rede, sendo o único limitador a capacidade tecnológica especificada neste Instrumento e no Termo de Referência, não a quantidade de usuários;

2.2.1.14. Os equipamentos firewall tipo 1, 2 e 3 deverão ser obrigatoriamente do mesmo fabricante.;

2.2.2. Gerenciamento de Políticas:

2.2.2.1. Deve prover *stateful inspection* com base na análise granular de comunicação e de estado de conexão para monitorar e controlar o fluxo de rede;

2.2.2.2. Deve prover a construção de regras utilizando objetos de rede baseados no protocolo TCP/IP. Durante a criação das regras, os respectivos objetos poderão ser associados às suas interfaces de rede ou zonas correspondentes;

2.2.2.3. Monitoramento de *links* de internet, através de teste de conectividade com endereços específicos e implementar alertas em caso de quedas;

2.2.2.4. Controle de políticas por porta e protocolo;

2.2.2.5. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

2.2.2.6. Controle de políticas por usuários, grupos de usuários, IPs, redes e grupos de redes;

2.2.2.7. Controle de políticas por geolocalização, ou seja, permitir ou bloquear o tráfego com base no país associado ao endereço ou rede;

2.2.2.7.1. Deve possibilitar a visualização dos países de origem e destino nos logs de acessos;

2.2.2.8. Descriptografar tráfego em conexões negociadas com TLS 1.2. Para equipamento tipo 1 o requisito aplica-se ao tráfego *inbound* ou *outbound*. Para equipamentos tipo 2 e 3 o requisito aplica-se ao tráfego *inbound* e *outbound;*

2.2.2.9. Possibilitar o bloqueio, no mínimo, dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg, de acordo com a necessidade, configuráveis através da solução fornecida;

2.2.2.10. Permitir *traffic shaping* QoS, ou seja, permitir a priorização de tráfego de dados baseada em políticas;

2.2.2.11. Suportar o agendamento para habilitar e desabilitar automaticamente políticas em horários pré-definidos;

2.2.2.12. Inspecionar e bloquear tráfego operando nas camadas 2 (L2) e 3 (L3), em uma ou mais instâncias;

2.2.2.13. Inspecionar e bloquear dados em linha e controle de tráfego em nível de aplicações;

2.2.2.14. Inspecionar e bloquear os dados operando como default *gateway* das redes protegidas e controlar o tráfego em nível das aplicações;

2.2.2.15. Deve permitir a verificação de regras por intervalo de tempo ou período, ou seja, data e horário para início e fim da validade;

2.2.2.16. Permitir a integração com o Microsoft Active Directory para autenticação de usuários, de modo que o Firewall possa utilizar das informações armazenadas para realizar autenticações;

2.2.2.17. Deverá permitir a configuração e administração do firewall via CLI (SSH) e interface gráfica (web HTTPs ou console do fabricante);

2.2.2.18. A solução deverá ser capaz de apresentar consumo ou percentual de consumo da regra de acordo com a utilização. Aplicável apenas aos equipamentos tipo 2 e 3;

2.2.2.19. A solução deverá disponibilizar *hotfixes* de segurança e upgrade de versão configuráveis e instaláveis pelo próprio ambiente;

2.2.2.20. Possuir a funcionalidade proxy HTTP e HTTPs. Para equipamento tipo 1 o requisito aplica-se ao tráfego *inbound* ou *outbound*. Para equipamentos tipo 2 e 3 o requisito aplica-se ao tráfego *inbound* e *outbound*.

2.2.3. Controle de Aplicações:

2.2.3.1. Possuir ferramentas de visibilidade e controle de aplicações *web* integradas no próprio *appliance* de segurança, que permitam a criação de políticas de liberação ou bloqueios baseando-se aplicações *web* 2.0;

2.2.3.2. A solução deverá ser capaz de identificar qualquer tipo de aplicação *web*, independentemente da porta e protocolo e ser capaz de bloqueá-las;

2.2.3.3. Reconhecer e tratar tráfego relacionado a *peer-to-peer*, redes sociais, acesso remoto, *update* de *software*, protocolos de rede, voip, áudio, vídeo, *proxy*, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

2.2.3.4. Reconhecer e tratar nativamente no mínimo as seguintes aplicações: *bitorrent, skype, facebook, instagram, linked-in, twitter, snapchat, logmein, teamviewer, vnc, gmail, outlook, youtube, whatsapp, telegram, 4shared, dropbox, google drive, itunes, webex, evernote, onedrive, google drive, dropbox, amazon cloud drive;*

2.2.3.5. Possuir controle de regras de aplicações, grupos de aplicações, categorias de aplicações, com controle granular para usuários ou grupos de usuários;

2.2.3.6. Deverá possibilitar a inspeção de HTTPs. Para equipamento tipo 1 o requisito aplica-se ao tráfego *inbound* ou *outbound*. Para equipamentos tipo 2 e 3 o requisito aplica-se ao tráfego *inbound* e *outbound;*

2.2.3.6.1. Possuir controle granular para quais funcionalidades de proteção e para quais endereços IP será executada a inspeção e descriptografia de SSL. É obrigatório que seja possível desligar a inspeção para sites de bancos, baseadas em categorização automática executada pelo Fabricante. Para equipamento tipo 1 o requisito aplica-se ao tráfego *inbound* ou *outbound*. Para equipamentos tipo 2 e 3 o requisito aplica-se ao tráfego *inbound* e *outbound;*

2.2.3.7. Deverá possibilitar a criação de regras de liberação e bloqueio com múltiplas aplicações e/ou grupo de aplicações;

2.2.3.8. Deverá possibilitar a liberação ou bloqueio de aplicações, no mínimo, pelos seguintes critérios:

2.2.3.8.1. Aplicações *Web*;

2.2.3.8.2. Categorias;

2.2.3.8.3. Nível de risco;

2.2.3.8.4. IP, *Range* de IPs, Redes;

2.2.3.8.5. Usuários do Active Directory;

2.2.3.8.6. Diferentes grupos de usuários.

2.2.3.9. Deve atualizar a base de assinaturas de aplicações automaticamente (ou sem horários agendados) sem a necessidade de reiniciar os *gateways* e gerência;

2.2.3.10. Deve permitir o bloqueio total de aplicações *proxies* de terceiros;

2.2.3.11. Deve possibilitar a integração com o Microsoft Active Directory para criação de políticas utilizando a categoria individualmente ou a combinação de usuários e grupos;

2.2.3.12. O mecanismo de Controle de aplicação *Web/URL* deve apresentar contagem de utilização de regra de acordo com a utilização;

2.2.3.13. A solução deve possibilitar a categorização por fator de risco das aplicações;

2.2.3.14. A solução deve prover a opção de editar a notificação de bloqueio;

2.2.3.15. A solução deverá incluir o mecanismo de listas (*blacklist* e *whitelist*) permitindo ao administrador do sistema negar ou permitir o acesso a determinadas URLs independentemente da categoria;

2.2.3.16. Deve inspecionar o *payload* de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante, independentemente de porta e protocolo;

2.2.3.17. Para tráfego criptografado (SSL), deve descriptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante;

2.2.3.18. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;

2.2.3.19. Reconhecer aplicações tanto em IPv6 quanto IPv4;

2.2.3.20. Permitir a limitação de banda (*download*/*upload*) usada por aplicações (*traffic shaping*), baseado no IP de origem, usuários e grupos do LDAP/AD;

2.2.3.21. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente nas estações dos usuários;

2.2.3.22. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

2.2.3.23. Para manter a segurança da rede eficiente, deve suportar o monitoramento ou bloqueio de aplicações desconhecidas e não somente sobre aplicações conhecidas;

2.2.3.24. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;

2.2.3.25. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações junto ao fabricante;

2.2.3.26. Deve possibilitar a diferenciação de tráfegos de *Instant Messaging (AIM, Facebook Chat, Whatsapp)* possuindo granularidade de controle/políticas para os mesmos;

2.2.3.27. Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o *whatsapp* e bloquear a transferência de arquivos;

2.2.3.28. Deve ser possível a criação de grupos baseados em características das aplicações:

2.2.3.28.1. Nível de risco da aplicação;

2.2.3.28.2. Categoria de aplicações;

2.2.3.28.3. Aplicações que usem técnicas evasivas, utilizadas por *malwares*/*botnet*, como transferência de arquivos e/ou uso excessivo de banda.

2.2.4. Filtro de URL:

2.2.4.1. Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no firewall;

2.2.4.2. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

2.2.4.3. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes e grupos de redes;

2.2.4.4. O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização;

2.2.4.5. A solução de filtro de URL deverá ser totalmente integrada com a solução de Aplicações Web 2.0, para melhor gerenciamento;

2.2.4.6. Deve possibilitar a inspeção de tráfego HTTPS. Para equipamento tipo 1 o requisito aplica-se ao tráfego *inbound* ou *outbound*. Para equipamentos tipo 2 e 3 o requisito aplica-se ao tráfego *inbound* e *outbound*.

2.2.4.7. Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que, antes de iniciar a navegação, expanda-se um portal de autenticação residente no *firewall* (Captive Portal);

2.2.4.8. A solução deve fornecer um mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;

2.2.4.9. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local;

2.2.4.10. Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

2.2.4.11. Suportar a criação de políticas baseadas no controle por URL e categoria de URL;

2.2.4.12. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente da opção Safe Search estar habilitada no navegador do usuário;

2.2.4.13. Suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

2.2.4.14. Suportar a criação de categorias de URLs customizadas;

2.2.4.15. Suportar a exclusão de URLs do bloqueio, por categoria;

2.2.4.16. Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente;

2.2.4.17. A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL;

2.2.4.18. Permitir a personalização de página de bloqueio;

2.2.4.19. Suportar a inclusão de informações das atividades dos usuários nos logs.

2.2.5. Identificação de Usuários:

2.2.5.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações e URLs, através da integração com serviços de diretório, autenticação via LDAP, *Microsoft Active Directory, Radius* ou base de dados local;

2.2.5.2. Deve possuir integração com *Microsoft Active Directory* para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

2.2.5.3. Os equipamentos tipo 2 e 3 deverão suportar:

2.2.5.3.1. Integração com *Radius* e LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

2.2.5.3.2. Recebimento de eventos de autenticação de controladoras *wireless*, dispositivos 802.1x e soluções NAC via *Radius*, para a identificação de endereços IP e usuários ou autenticar via portal web sobre SSL;

2.2.5.3.3. A solução deve ser capaz de fornecer uma autenticação baseada em navegador (*Captive Portal*), sem a necessidade de agente para usuários não registrados ou não reconhecidos no domínio;

2.2.5.3.4. Suporte a autenticação *Kerberos* ou *Radius*;

2.2.5.3.5. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes *Citrix* e *Microsoft Terminal Server*, permitindo visibilidade e controle granular;

2.2.5.4. A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no *Microsoft Active Directory*;

2.2.5.5. Deve suportar autenticação para smartphones e *tablets*;

2.2.5.6. Na integração com o AD, todos os *Domain Controllers* (controladores de domínio) em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de *scritps* de comando;

2.2.5.7. A solução deverá suportar grupos LDAP "*nested*";

2.2.6. QoS (Quality of Service):

2.2.6.1. Com a finalidade de controlar aplicações cujo consumo de banda possa ser excessivo, como streaming, a solução deve possibilitar a liberação ou bloqueio de tais aplicações e controlá-las por políticas de controle de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de streaming de áudio como de vídeo;

2.2.6.2. Suportar a criação de políticas de QoS por: endereço de origem, endereço de destino, usuário e grupo do LDAP/AD e por porta.

2.2.6.3. O QoS deve possibilitar a definição de classes por: banda garantida; banda máxima e fila de prioridade.

2.2.6.4. Deverá permitir o monitoramento do uso que as aplicações fazem por *bytes*, sessões e por usuário;

2.2.7. VPN IPSEC:

2.2.7.1. A solução deve suportar CA Interna ou CA Externa de terceiros;

2.2.7.2. Solução deve suportar:

2.2.7.2.1. 3DES;

2.2.7.2.2. AES 128 e 256 (*Advanced Encryption Standard*);

2.2.7.2.3. Algoritmo *Internet Key Exchange* (IKE) fase I e II, IKEv2;

2.2.7.2.4. VPN *Site-to-Site e Cliente-to-Site*, autenticação MD5 e SHA-1;

2.2.7.2.5. Autenticação via certificado IKE PKI;

2.2.7.2.6. Integridade dos dados com SHA-256 ou SHA-192;

2.2.7.3. Deve possuir interoperabilidade com outros fabricantes de acordo com o padrão IPSEC através de RFCs;

2.2.7.4. A solução deve suportar VPNs baseadas em redes e VPNs através de rotas com suporte a protocolos de roteamento dinâmico;

2.2.7.5. A solução deve incluir a capacidade de estabelecer VPNs com *gateways* com IPs públicos dinâmicos;

2.2.8. VPN SSL – Equipamentos tipo 2 e 3:

2.2.8.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface *web*;

2.2.8.2. Cadastro do usuário para realização da conexão, com informações necessárias e data de expiração de acesso;

2.2.8.3. As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

2.2.8.4. Atribuição de endereço IP nos clientes remotos de VPN;

2.2.8.5. Atribuição de DNS nos clientes remotos de VPN;

2.2.8.6. Deve permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

2.2.8.7. Suportar autenticação via AD/LDAP e base de usuários local;

2.2.8.8. Leitura e verificação de CRL (*certificate revocation list*);

2.2.8.9. Permitir a aplicação de políticas de segurança e visibilidade para o tráfego que circulam dentro dos túneis SSL;

2.2.8.10. O agente de VPN a ser instalado nos equipamentos *desktop* e *laptops* deve ser capaz de ser distribuído de maneira automática via *Active Directory* ou ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN.

2.2.8.11. Permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas: após autenticação do usuário na estação ou sob demanda do usuário;

2.2.8.12. Deverá manter uma conexão segura com o portal durante a sessão;

2.2.8.13. O agente de VPN SSL *client-to-site* deve ser compatível com pelo menos: Windows 7, Windows 10 e Mac OS X;

2.2.9. Inspeção SSL:

2.2.9.1. A solução deverá suportar inspeção e descriptografia SSL com desempenho líder em todas as tecnologias de mitigação de ameaças;

2.2.9.2. A solução deverá utilizar a base de URL *Filtering*, permitindo ao administrador a criação de políticas de inspeção HTTPS com base nas categorias da funcionalidade de URL *Filtering*;

2.2.10. Balanceamento de Links:

2.2.10.1. Possuir capacidade de agregar e balancear circuitos de dados (*links* de Internet) nos modos ativo/ativo e ativo/passivo;

2.2.10.2. Possibilidade de configurar um valor de *threshold* baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento, conforme requisitos 2.2.10.2.1 ou 2.2.10.2:

2.2.10.2.1. latência, *jitter* e perda de pacotes;

2.2.10.2.2. ping por intervalo, tempo de resposta e resolução DNS;

2.2.10.3. Deve permitir a configuração do tempo de checagem para cada um dos *links*;

2.2.10.4. Deve possibilitar o balanceamento entre os *links* com base nos requisitos 2.2.10.4.1 ou 2.2.10.4.2:

2.2.10.4.1. número de sessões, volume de tráfego, IP de origem, IP de destino, aplicações;

2.2.10.4.2. capacidade de cada *link*, percentual de banda (ou número de sessões), volume de tráfego, IP de origem, IP de destino e aplicações;

2.2.10.5 A funcionalidade de balanceamento de *links* deverá ser integrada ao *firewall* ou composta por mais de um equipamento, desde que seja uma solução *on-premise* e com gerenciamento integrado e centralizado.

2.2.11. Características Específicas - Equipamento Firewall Tipo 1 – Item 1:

2.2.11.1. Deve ser fornecido com fonte de alimentação e demais acessórios necessários ao funcionamento;

2.2.11.2. Deve possuir indicadores luminosos frontais e individuais que indiquem os *status* de operação do equipamento e interfaces de rede;

2.2.11.3. Deve possuir altura máxima de 1U (uma unidade) no rack;

2.2.11.4. Cada *appliance* de segurança deverá possuir no mínimo as seguintes capacidades:

2.2.11.4.1. 150 (cento e cinquenta) Mbps de *throughput* de *threat prevention* (*firewall*, IPS, controle de aplicação, antivírus e todas as funcionalidades ativadas, baseando-se em protocolo HTTP ou mescla de protocolos);

2.2.11.4.2. 4.000 (quatro mil) conexões por segundo;

2.2.11.4.3. 60.000 (sessenta mil) conexões simultâneas;

2.2.11.4.4. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será considerado;

2.2.11.5. O *appliance* deve possuir os seguintes quantitativos mínimos de interfaces de rede:

2.2.11.5.1. 06 (seis) interfaces 1GbE RJ45 para E/S (entrada/saída);

2.2.11.5.2. 01 (uma) interface serial RJ45 ou USB para acesso à console local, integrada ao equipamento ou via cabos e conversores externos.

2.2.12. Características Específicas - Equipamento Firewall Tipo 2 – Item 2:

2.2.12.1. Deverá ter altura máxima de 1U (uma unidade) no rack;

2.2.12.2. Deverá ser fornecido com 2 (duas) fontes de alimentação redundante 100 a 240 VAC, com potência suficiente para suprir a configuração máxima do equipamento;

2.2.12.3. Deverá ser fornecido acessórios do próprio fabricante ou homologado pelo fabricante, para instalação dos equipamentos em rack padrão 19";

2.2.12.4. Cada *appliance* de segurança deverá possuir no mínimo as seguintes capacidades:

2.2.12.4.1. 700 (setecentos) Mbps de *throughput* de *threat prevention* (*firewall*, IPS, controle de aplicação, antivírus e todas as funcionalidades ativadas, baseando-se em protocolo HTTP ou mescla de protocolos);

2.2.12.4.2. 12.000 (doze mil) conexões por segundo;

2.2.12.4.3. 180.000 (cento e oitenta mil) conexões simultâneas;

2.2.12.4.4. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será considerado;

2.2.12.5. O *appliance* deve possuir os seguintes quantitativos mínimos de interfaces de rede:

2.2.12.5.1. 5 (cinco) interfaces 1GbE RJ45 para E/S (entrada/saída), fixas ou via SFP com *transceivers* 1GbE RJ45;

2.2.12.5.2. 1 (uma) interface de rede para alta disponibilidade;

2.2.12.5.2.1. Caso a interface de alta disponibilidade não seja 1GbE RJ45, a mesma deve vir acompanhada dos acessórios necessários ao funcionamento em alta disponibilidade tais como *transceiver*, cordão de fibra, cabo twinax/dac, etc.

2.2.12.5.3. 2 (duas) interfaces 10GbE SFP+ para E/S (entrada/saída), cada uma acompanhada de um par de *transceivers* 10GBase-SR com conector LC;

2.2.12.5.4. 1 (uma) interface 1GbE RJ45 para gerenciamento fora da banda (*out-of-band*);

2.2.12.5.5. 1 (uma) interface serial RJ45 ou USB para acesso à console local, integrada ao equipamento ou via cabos e conversores externos.

2.2.13. Características Específicas - Equipamento Firewall Tipo 3 – Item 3:

2.2.13.1. Deverá ter altura máxima de 3U (três unidades) no rack;

2.2.13.2. Deverá ser fornecido com 2 (duas) fontes *hotswap* de alimentação redundante 100 a 240 VAC, com potência suficiente para suprir a configuração máxima do equipamento;

2.2.13.3. Deverá ser fornecido com acessórios do próprio fabricante ou homologado pelo fabricante, para instalação dos equipamentos em rack padrão 19";

2.2.13.4. Recurso para detecção de falhas na temperatura e ventiladores com notificação de alerta para o administrador do sistema;

2.2.13.5. Deverá suportar a configuração de alta disponibilidade em modo cluster, de modo transparente, permitindo as configurações ativo-ativo e ativo-passivo;

2.2.13.6. Na ocorrência de falhas, as conexões existentes em um firewall deverão ser mantidas pelo outro, sem perda de conexões, não acarretando interrupções no tráfego da rede e nem de redução de desempenho da solução;

2.2.13.7. Suportar o protocolo NTP (*Network Time Protocol*);

2.2.13.8. Cada *appliance* de segurança deverá possuir no mínimo as seguintes capacidades:

2.2.13.8.1. 3.6 (três ponto seis) Gbps de *throughput* de *threat prevention* (*firewall*, IPS, controle de aplicação, antivírus e todas as funcionalidades ativadas, baseando-se em protocolo HTTP ou mescla de protocolos);

2.2.13.8.2. Suportar 90.000 (noventa mil) conexões por segundo;

2.2.13.8.3. Suportar 2.000.000 (dois milhões) de conexões simultâneas;

2.2.13.8.4. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será considerado;

2.2.13.9. O *appliance* deve possuir os seguintes quantitativos mínimos de interfaces de rede:

2.2.13.9.1. Pelo menos 14 (quatorze) interfaces 1GbE RJ45 para E/S (entrada/saída), fixas ou via SFP com *transceivers* 1GbE RJ45;

2.2.13.9.2. Pelo menos 2 (duas) interfaces 1GbE SFP para E/S (entrada/saída), cada uma acompanhada de um par de *transceivers* 1000Base-SX com conector LC;

2.2.13.9.3. Pelo menos 1 (uma) interface de rede para alta disponibilidade;

2.2.13.9.3.1. Caso a interface de alta disponibilidade não seja 1GbE RJ45, a mesma deve vir acompanhada dos acessórios necessários ao funcionamento em alta disponibilidade tais como *transceiver*, cordão de fibra, cabo twinax/dac, etc.

2.2.13.9.4. Pelo menos 2 (duas) interfaces 10GbE SFP+ para E/S (entrada/saída), cada uma acompanhada de um par de *transceivers* 10GBase-SR com conector LC;

2.2.13.9.5. Pelo menos 1 (uma) interface de gerenciamento fora da banda (*out-of-band*) 1GbE RJ45;

2.2.13.9.6. 1 (uma) interface serial RJ45 ou USB para acesso à console local integrada ao equipamento ou via cabos e conversores externos.

2.2.13.10. Prevenção Contra Ameaças:

2.2.13.10.1. Deve incluir assinaturas de prevenção de intrusão (IPS) e suporte ao bloqueio de arquivos maliciosos;

2.2.13.10.2. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de antivírus e *anti-malware* integrados no próprio *appliance* sem a necessidade de uso de quaisquer interfaces externas, com console de gerência integrada à console centralizada dos *appliances* de segurança;

2.2.13.10.3. Deve sincronizar as assinaturas de IPS, antivírus e *anti-malware* quando implementado em alta disponibilidade, nos modos ativo/ativo e ativo/passivo;

2.2.13.10.4. As assinaturas devem suportar ativação e desativação, além de ativação apenas em modo de monitoração;

2.2.13.10.5. Exceções por IP de origem ou de destino devem ser possíveis, de forma geral ou assinatura a assinatura;

2.2.13.10.6. Deve suportar granularidade nas políticas de antivírus e *anti-malware*, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço ou assinatura e a combinação de todos esses itens;

2.2.13.10.7. Deve suportar o bloqueio de vulnerabilidades;

2.2.13.10.8. Deve suportar o bloqueio de *exploits* (comandos ou programas que conseguem tirar proveito de vulnerabilidades) conhecidos;

2.2.13.10.9. Deve possuir assinaturas contra ataques de negação de serviços (DoS/DDoS);

2.2.13.10.10. A solução de IPS deverá possuir os seguintes mecanismos de detecção:

2.2.13.10.10.1. Assinaturas, anomalias de protocolos, controle de aplicações e detecção por comportamento;

2.2.13.10.10.2. Inspeção de toda a sessão, independentemente do tamanho;

2.2.13.10.10.3. Inspeção de todo o tráfego de forma bidirecional, analisando qualquer tamanho de sessão sem degradar a performance total do equipamento;

2.2.13.10.10.4. O mecanismo de inspeção deve receber e implementar, em tempo real, atualizações para os ataques emergentes sem a necessidade de reiniciar o *appliance*.

2.2.13.10.11. Em cada proteção de segurança, devem estar inclusas informações, como: código CVE (*common vulnerabilities and exposures*) ou outro código de referência, severidade, tipo de ação que a mesma irá executar;

2.2.13.10.12. A solução deve fazer captura de pacotes para proteções específicas ou através de filtros pré-definidos;

2.2.13.10.13. Deve detectar e bloquear pelo menos os seguintes ataques conhecidos: SQL *injection*; ICMP *denial of service*; força bruta (*brutal force*) e *scanning* de portas, *Port overflow*, *Non compliant* SSL;

2.2.13.10.14. As regras de exceção deverão possuir: origem, destino ou a combinação dos dois;

2.2.13.10.15. A solução deve ser capaz de inspecionar tráfego HTTPS (*inbound*/*outbound*);

2.2.13.10.16. A solução de IPS deve permitir a configuração de assinaturas em modo de detecção para fins de *troubleshooting*;

2.2.13.10.17. Para melhor administração da solução, a solução deve permitir incorporar de forma automática novas proteções de IPS;

2.2.13.10.18. O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de email, web e DNS, onde os mesmos poderão ser assinalados no momento da criação do objeto de rede na solução;

2.2.13.10.19. A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo, pelo menos, os seguintes serviços: aplicações web, serviços de e-mail, DNS e FTP;

2.2.13.10.20. A solução deve permitir que o administrador possa configurar, nativamente ou por assinaturas customizadas, quais métodos e comandos HTTP são permitidos e quais são bloqueados;

2.2.13.10.21. Deve incluir proteção contra vírus em conteúdo ActiveX, *applets* Java, worms e outros;

2.2.13.10.22. A solução deve permitir a configuração de políticas baseada em países;

2.2.13.10.23. A solução deverá ser capaz de inspecionar e proteger apenas *hosts* internos;

2.2.13.10.24. A solução deve permitir que o administrador possa bloquear facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os *ranges* de endereços IP dos países que deseja bloquear;

2.2.13.10.25. Ser imune e capaz de impedir ataques básicos como: *Synflood, ICMPflood, UDPfloof*;

2.2.13.10.26. Detectar e bloquear a origem de *portscans*;

2.2.13.10.27. Possuir assinaturas para bloqueio de ataques de *buffer overflow*;

2.2.13.10.28. Suportar o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, SMB/CIFS e SMTP;

2.2.13.10.29. Identificar e bloquear comunicação com *botnets*;

2.2.13.10.30. Os eventos devem identificar o país de onde partiu a ameaça;

2.2.13.10.31. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo *Firewall* com endereços IPv4 ou IPv6;

2.2.13.10.32. Deve suportar proteção contra vírus em conteúdo HTML e *javascript*, *software* espião (*spyware*) e *worms*;

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

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

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

2.2.13.10.36. A solução *antibotnet* deve utilizar um mecanismo de detecção em multicamadas, que inclui reputação de endereço IP, URLs e endereços DNS;

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

2.2.13.10.38. Implementar interface gráfica Web segura, utilizando o protocolo HTTPS ou console do próprio fabricante;

2.2.13.10.39. Implementar mecanismo de verificação através da interface gráfica *Web* (ou console do próprio fabricante), com no mínimo as seguintes informações: versão do *firmware*, versão de *patch*, versão da base de dados, nível de processamento, status dos discos rígidos, taxa de transferência atual e status das interfaces de rede;

2.2.13.10.40. Possuir antivírus em tempo real, para ambiente de *gateway* internet, integrado à plataforma de proteção para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3 e FTP;

2.2.13.10.41. A solução deve atuar na prevenção de forma granular através de políticas por usuário / máquina ou rede, sendo possível escolher um perfil diferente para cada regra;

2.2.13.10.42. Implementar geração de relatórios através da interface gráfica, a qual possua, no mínimo, as seguintes informações, com recursos de *drill-down* entre níveis: tipo de malware e id de evento, severidade da ameaça, horário do último evento, IP de origem, IP de destino, usuário infectado com base no *Domain Controller*;

2.2.13.10.43. Implementar, através da interface gráfica ou console do próprio fabricante, pesquisa aos eventos já reconhecidos;

2.2.13.10.44. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de *hosts* ou incidentes referentes a incidentes de vírus e *bots*;

2.2.13.10.45. A solução deve permitir de forma anônima compartilhar ou não informações sobre ataques ou arquivos maliciosos para o serviço na nuvem do fabricante;

2.2.13.10.46. A solução deve permitir a criação de *whitelists* (listas brancas – com acesso liberado) baseadas no hash do arquivo ou no FQDN do site;

2.2.13.10.47. Permitir o bloqueio de *malwares* (*adware*, *spyware*, e *keyloggers*);

2.2.13.10.48. A solução deve suportar a detecção e prevenção de vírus *cryptors* & *ransmoware* e seus variantes utilizando análises estáticas e dinâmicas;

2.2.13.10.49. A solução deve ser capaz de proteger contra diversos ataques DNS, tais como:

2.2.13.10.49.1. Capacidade para detectar e prevenir C&C;

2.2.13.10.49.2. Realizar engenharia reversa do malware com a finalidade de descobrir seu DGA (*Domain Generation Algorithm*), C&C ou tecnologia proprietária capaz de identificar variações de malwares;

2.2.13.10.49.3. Capacidade para detectar e prevenir ataque DNS *tunneling*;

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

2.2.13.10.51. Deve suportar a inspeção em arquivos comprimidos (zip, rar, gzip);

2.2.13.11. Prevenção Avançada Contra Ameaças:

2.2.13.11.1. A solução deverá prover inspeção de tráfego de entrada de *malwares* não conhecidos ou do tipo APT (*Advanced Persistent Threat*) com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de *callbacks*;

2.2.13.11.2. Possuir a capacidade de prevenção de ameaças não conhecidas;

2.2.13.11.3. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise na nuvem ou em *appliance* local, onde o arquivo será executado e simulado em ambiente controlado;

2.2.13.11.4. Suportar os protocolos HTTP, SMTP assim como inspeção de tráfego criptografado através de HTTPS e TLS;

2.2.13.11.5. A solução deve ser capaz de inspecionar o tráfego criptografado SSL;

2.2.13.11.6. A solução deve possuir *engine* de DNS *Trap*, onde é possível identificar *hosts* infectados tentando acessar os endereços maliciosos;

2.2.13.11.7. Identificar e bloquear a existência de *malware* em comunicações de entrada e saída, incluindo destinos de servidores do tipo C&C;

2.2.13.11.8. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, sendo eles: Windows 7 e Windows 10;

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

2.2.13.11.10. Todas as máquinas virtuais utilizadas na solução de vem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

2.2.13.11.11. A solução deve possuir nuvem de inteligência proprietária do fabricante que seja responsável por atualizar toda a base de segurança dos *appliances* através de assinaturas;

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

2.2.13.11.13. Implementar integração com ferramentas de SIEM (*Security Information and Event Management*);

2.2.13.11.14. Implementar mecanismo de integração com servidores *syslog*;

2.2.13.11.15. Toda análise deverá ser realizada de forma interna na nuvem ou em *appliance* local, não sendo aceitas soluções que necessitem de módulos e/ou servidores externos para a implementação de qualquer funcionalidade solicitada;

2.2.13.11.16. Salvo necessidade de customização, toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

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

2.2.13.11.18. Implementar a emulação, detecção e bloqueio de qualquer *malware* e/ou código malicioso detectado.

2.2.13.11.19. O sistema de análise na nuvem ou local deve prover informações sobre as ações do *malware* na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de contenção automaticamente, definir URLs não confiáveis utilizadas pelo novo *malware* e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);

2.2.13.11.20. O sistema automático de analise na nuvem ou local deve emitir relatório com identificação do *malware*;

2.2.13.11.21. O sistema de emulação deve exibir quota de percentual ou quantidade de arquivos scaneados;

2.2.13.11.22. A solução de possuir os indicadores abaixo referentes ao último dia, última semana ou últimos 30 (trinta) dias:

2.2.13.11.22.1. Arquivos inspecionados;

2.2.13.11.22.2. Arquivos maliciosos;

2.2.13.11.23. A solução deve ser capaz de fazer atualizações de *engines*;

2.2.13.11.24. Deve suportar a monitoração de arquivos trafegados na internet (HTTP, HTTPS, SMTP);

2.2.13.11.25. Deve permitir visualizar os resultados das análises de *malwares* de dia zero nos diferentes sistemas operacionais suportados;

2.2.13.11.26. Deve permitir reclassificar ocorrências na análise de *malwares* de dia zero, a partir da própria interface de gerência, conforme as classificações dos critérios 2.2.13.11.26.1 ou 2.2.13.11.26.2:

2.2.13.11.26.1 falso-positivo e falso negativo;

2.2.13.11.26.2 *fail-open* e *fail-close*;

2.3. Equipamento de armazenamento de logs e gerência:

2.3.1. Deve ser separada do *gateway* de segurança e gerenciar políticas de segurança de todos os *firewalls* e funcionalidades solicitadas neste projeto, assim como armazenar os logs e gerar os relatórios de forma unificada.

2.3.2. A solução deve fornecer uma ferramenta de gestão centralizada capaz de reunir todos os equipamentos sob uma única interface gráfica, possibilitando o gerenciamento unificado de políticas e regras de todos os firewalls ofertados.

2.3.3. A solução deve oferecer as funcionalidades de *backup* e *restore*, permitindo que o administrador possa agendar procedimentos de backup em dias ou horários específicos.

2.3.4. A solução pode ser entregue em um único componente, ou em dois componentes separados (armazenamento de log e gerência). Se ofertado em uma única solução, deverá possuir *hardware* com capacidade suficiente para atender a todos os requisitos deste item;

2.3.5. Caso a solução de gerência seja separada da solução de armazenamento de logs, ambas devem suportar todos os dispositivos contemplados, bem como sua licença caso necessário;

2.3.6. Deve centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento;

2.3.7. A solução deverá permitir seu gerenciamento por: CLI (*Command Line Interface*) via SSH, *Web* GUI utilizando protocolo HTTPS ou console gráfica;

2.3.8. Implementar gerenciamento centralizado das licenças de utilização da solução;

2.3.9. Deve possuir mecanismo de ajuda de comandos via SSH, facilitando a localização e parâmetros dos mesmos;

2.3.10. Deve manter um canal de comunicação segura, com encriptação baseada em certificados ou chaves, entre todos os componentes que fazem parte da solução de *firewall*, gerência, armazenamento de logs e emissão de relatórios;

2.3.11. A solução deve suportar alta disponibilidade de gerenciamento, utilizando um servidor de gerencia em *standby* que é automaticamente sincronizado com o servidor primário;

2.3.12. A solução deve possuir ao menos um perfil pré-configurado que permita sua utilização assim que o equipamento for configurado;

2.3.13. Para melhor análise e administração do ambiente de segurança, a solução deve prover em cada regra, a informação da utilização da mesma para equipamentos tipo 2 e 3;

2.3.14. A gerência deve possuir console de log onde deve ter a capacidade de visualizar os logs de segurança em tempo real permitindo ao administrador realizar as devidas análises para fins de *troubleshooting*;

2.3.15. A solução de gerência deve prover fácil administração na aplicação das políticas para os *gateways*, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, que pode ser aplicada nos *gateways* remotos em uma única sessão, evitando qualquer tipo de retrabalho de configuração e aplicação de regra;

2.3.16. Deve possuir mecanismo de painel de controle onde seja possível a visualização de, no mínimo, as seguintes informações: sumário de detecção e proteção, gráfico de *top* infecções, e gráfico da taxa de transferência de tráfego monitorado;

2.3.17. Solução deve incluir o status de todos os túneis VPN *site-to-site* e *client-to-site*, túneis permanentes e seu estado de conexão e túneis e suas comunidades;

2.3.18. A solução deve prover informações gerais de cada *gateway* como volume de pacotes aceitos ou largura de banda, conexões concorrentes, novas conexões e licenciamento, informando o seu prazo de validade;

2.3.19. A solução de monitoração deve ser capaz de possuir filtro para monitorar todos os usuários remotos conectados;

2.3.20. A filtragem de logs deve ser intuitiva, ou seja, a partir de uma palavra chave sendo suficiente para que um analista, com nenhum ou pouco conhecimento sobre a operação da ferramenta, possa aplicar filtros utilizando apenas um único parâmetro para a busca;

2.3.21. Solução deve ser capaz de reconhecer falhas e problemas de conectividade entre dois pontos conectados através de uma VPN, assim como registrar e alertar quando o túnel VPN está desconectado;

2.3.22. A solução dever ser capaz de criar filtro que permita a visualização de múltiplos logs como:

2.3.22.1. *Top* origem;

2.3.22.2. *Top* destino;

2.3.22.3. *Top* usuários;

2.3.22.4. Principais acessos a determinados serviços;

2.3.22.5. Principais ações ou listar porcentagem de tráfego liberado e bloqueado por sessão;

2.3.22.6. Principais funcionalidades de segurança utilizadas do *firewall* ou descriminar tráfegos por funcionalidade;

2.3.22.7. Principais regras que foram utilizadas de acordo com o filtro criado;

2.3.22.8. Principais aplicações web utilizadas de acordo com a funcionalidade de segurança disponível no *firewall*.

2.3.23. Com o intuito otimizar a pesquisa de eventos e abrangência de período de busca do log, a solução deve ter a capacidade de possuir logs indexados;

2.3.24. A solução de armazenamento de log deve possuir a capacidade criar múltiplos filtros customizados, sendo possível salvar em favoritos para visualizar em um momento posterior ou através de uma rotina constante;

2.3.25. Para evitar grandes customizações da solução, a console de análise de logs, deve prover filtros pré-definidos de eventos com maior importância;

2.3.26. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais *Windows* ou *Linux*;

2.3.27. A solução de gerência centralizada deve possuir capacidade de analisar logs e eventos com intuito de mitigar qualquer anomalia no ambiente independente se o *appliance* de segurança estiver sofrendo ataque com elevado consumo de CPU;

2.3.28. O gerenciamento deve permitir/possuir:

2.3.28.1. Criação e administração de políticas de *Firewall*;

2.3.28.2. Controle de aplicação e IPS;

2.3.28.3. Criação e administração de políticas de IPS;

2.3.28.4. Antivírus e *anti-malware*;

2.3.28.5. Criação e administração de políticas de Filtro de URL e prevenção contra ameaças avançadas;

2.3.28.6. Monitoração de logs;

2.3.28.7. Ferramentas de investigação de logs;

2.3.28.8. Acesso concorrente de administradores.

2.3.29. Deve permitir usar palavras chaves ou cores para facilitar identificação de regras;

2.3.30. Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;

2.3.31. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, alteração de configurações;

2.3.32. Autenticação integrada à base de dados local ou servidor *Radius*;

2.3.33. Deve possuir ferramenta para localização de objetos (por exemplo: endereço IP, Range de IP, sub-rede) na base de regras;

2.3.34. Deve atribuir sequencialmente um número a cada regra de *Firewall* ou NAT;

2.3.35. Criação de regras que fiquem ativas em horário definido;

2.3.36. Criação de regras com data de expiração;

2.3.37. *Backup* das configurações e *rollback* de configuração para a última configuração salva;

2.3.38. Suportar *rollback* de sistema operacional para a última versão local através da ferramenta de gerenciamento ou diretamente no *firewall*;

2.3.39. Habilidade de *upgrade* via SCP ou TFTP ou interface de gerenciamento;

2.3.40. A solução deve possuir recurso de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (*shadowing*);

2.3.41. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

2.3.42. Deverá ter a capacidade de gerar relatórios gráficos, que permitam visualizar as mudanças na utilização de aplicações na rede, no quem se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações, no tempo presente com relação ao passado;

2.3.43. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, antivírus, *anti-malware* e emulação) e URLs, para melhor diagnóstico e resposta a incidentes;

2.3.44. Deve possuir relatórios de utilização dos recursos por aplicações, URLs, ameaças (IPS, antivírus e *anti-malware*);

2.3.45. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, antivírus, *anti-malware* e emulação), e URLs que passaram pela solução;

2.3.46. Deve ser possível exportar os logs em CSV;

2.3.47. Disponibilizar relatório gráfico ou tabela de eventos por CVE (*Common Vulnerabilities and Exposures*);

2.3.48. Deve suportar rotação automática dos arquivos de log;

2.3.49. A console de monitoração deve permitir a visualização das seguintes informações, de forma histórica e em tempo real:

2.3.49.1. Principais aplicações;

2.3.49.2. Principais aplicações por risco;

2.3.49.3. Administradores autenticados na gerência da plataforma de proteção;

2.3.49.4. Número de sessões simultâneas;

2.3.49.5. *Status* das interfaces;

2.3.49.6. Uso de CPU;

2.3.50. A solução deve gerar relatórios com, no mínimo, as características:

2.3.50.1. Resumo gráfico ou tabela de aplicações utilizadas;

2.3.50.2. Principais aplicações por taxa de transferência de *bytes*;

2.3.50.3. Principais hosts por número de ameaças identificadas;

2.3.51. Atividades de um usuário específico ou grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, antivírus e *anti-malware*), de redes vinculadas a este tráfego;

2.3.52. A solução de relatório deve apresentar via interface gráfica as seguintes informações no relatório:

2.3.52.1. Sumário executivo;

2.3.52.2. Relatório de servidores de *callback*;

2.3.52.3. Relatório de hosts infectados;

2.3.52.4. Atividade de malware e detalhes dos alertas.

2.3.52.5. Deve permitir a criação de relatórios personalizados;

2.3.52.6. Possibilidade de impressão sem marcas d'água;

2.3.52.7. Possibilidade de exportar, copiar ou salvar gráficos ou tabelas produzidas;

2.3.52.8. Deve ser possível incluir nos critérios de pesquisa várias redes e IPs destinos, exceto no campo horário, onde deve ser possível definir uma faixa de tempo como critério de pesquisa;

2.3.52.9. A solução deve possuir, na própria interface de gerência, gráfico ou tabela contendo informações em tempo real sobre as atividades recentes de *malwares* detectados na rede, sendo que essas informações deverão ser apresentadas em mapa geográfico por país, através de IP ou URL;

2.3.52.10. Gerar alertas automáticos via email e SNMP;

2.3.52.11. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de proteção;

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

2.3.52.13. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de proteção;

2.3.52.14. Deve permitir a criação de objetos e políticas compartilhadas;

2.3.52.15. Deve consolidar logs de todos os dispositivos administrados;

2.3.52.16. Deve permitir exportar *backup* de configuração automaticamente, via agendamento;

2.3.52.17. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

2.3.52.18. Prover uma visualização sumarizada de todas as aplicações, ameaças e URLs que passaram pela solução;

2.3.52.19. Deverá possuir mecanismo *drill-down* para navegação e análise dos logs em tempo real;

2.3.52.20. Nas opções de *drill-down*, ser possível identificar o usuário que fez determinado acesso;

2.3.52.21. Permitir que os logs de auditoria possuam identificação;

2.3.52.22. Permitir que todas as alterações em regras e objetos produzam log de auditoria;

2.3.52.23. Deve possuir mecanismo, na ferramenta de gerenciamento ou no próprio *firewall*, para identificar e informar aos administradores problemas de configuração de *anti-spoofing*;

2.3.52.24. Deve possuir mecanismo de validação da base de objetos, informando sobre a quantidade total de objetos, objetos não utilizados e duplicados;

2.3.52.25. Deve possuir mecanismo para checar e informar sobe uso de disco rígido, licenças, usuários e políticas da gerência centralizada;

2.3.52.26. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, o país de origem e destino;

2.3.52.27. Disponibilizar informações gráficas ou tabeladas, na linha tempo que informe o número de eventos ocorridos;

2.3.52.28. Disponibilizar recursos interativos de navegação nos eventos informados;

2.3.52.29. A solução deve exportar relatórios via HTML ou CSV, PDF ou XML;

2.3.52.30. A solução deve possibilitar a visualização geográfica dos eventos de segurança correlacionados;

2.3.52.31. A solução deve permitir ao administrador ser capaz de atribuir filtros para diferentes gráficos ou tabelas, que são atualizados em intervalos regulares, permitindo ao operador a concentrar-se sobre os eventos mais importantes;

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

2.3.52.33. Visualizar quantidade de tráfego utilizado de aplicações e navegação;

2.3.52.34. Gráficos com principais eventos de segurança, de acordo com um filtro específico;

2.3.52.35. Estatísticas para comparativo de período (hora, dia, mês ou ano);

2.3.52.36. Deve permitir a geração de relatórios com horários predefinidos, diários, semanais e mensais. Incluindo principais eventos, principais origens, principais destinos, principais origens e os seus principais eventos, principais destinos e seus principais eventos;

2.3.52.37. Deve apresentar a distribuição dos diferentes eventos filtrados por país em um mapa, onde deve estar incluso principais eventos de origem ou destino, por país;

2.3.52.38. Deve suportar a programação de relatórios automáticos, para as informações básicas que precisa extrair de forma diária, semanal e mensal. Também deve permitir ao administrador definir a data e a hora que o sistema de informação começa a gerar o relatório agendado;

2.3.52.39. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos e incidentes de ataque de forma completamente visual, utilizando para tanto gráficos, com consumo de banda utilizado pelas aplicações e quantidade de eventos ocorridos e prevenidos;

2.3.53. Deve ser fornecido com acessórios para instalação em rack padrão 19", com *hardware* e *software* do mesmo fabricante ou *hardware* homologado pelo fabricante do *software*;

2.3.54. A solução de armazenamento de log deve possuir ao menos 6TB de disco após implementação de RAID;

2.3.55. Deve possuir pelo menos 2 (duas) interfaces 1GbE RJ45.

2.3.56. Caso *hardware* e *software* não sejam do mesmo fabricante, a solução deverá possuir também:

2.3.56.1. No mínimo 2 (dois) processadores de no mínimo 8 (oito) núcleos, frequência de 2,0 GHz e 10Mb de cache;

2.3.56.2. No mínimo 32 (trinta e dois) GB de memória RAM;

2.3.56.3. 2 (dois) discos SSD de no mínimo 480 GB configurados em RAID 1 destinados exclusivamente à instalação do sistema operacional e software de backup;

2.3.56.4. 7 (sete) TB de armazenamento líquido interno por meio de discos NL-SAS ou tecnologia superior, configurados em RAID 5 ou RAID 6, não aplicando-se o requisito 2.3.54;

2.3.56.4.1. O armazenamento líquido interno deve ser expansível a pelo menos 10TB (dez terabytes), por meio da adição de discos de igual capacidade aos ofertados, configurados em RAID 5 ou RAID 6;

2.3.56.5. Deverá possuir trilhos deslizantes com gerenciamento de cabos para montagem do equipamento em rack 19";

2.3.56.6. Deve ser apresentado na proposta comercial documento que comprove que o equipamento ofertado (fabricante e modelo) seja homologado pelo fabricante do *software* de armazenamento de logs e gerência;

2.3.56.7. Possuir todo o licenciamento necessário ao funcionamento do equipamento;

2.3.56.8. As especificações de *hardware* supracitadas servem como referencial mínimo e não limitam a oferta de características, capacidades e recursos superiores ou adicionais eventualmente recomendados pelos fabricantes dos componentes da solução.

2.4. Equipamento Mail Gateway:

2.4.1. Deve possuir pelo menos 2 (duas) interfaces 1GbE RJ45;

2.4.2. Deverá ser fornecido com 2 (duas) fontes de alimentação redundante 100 a 240 VAC, com potência suficiente para suprir a configuração máxima do equipamento;

2.4.3. Deve ser fornecido com acessórios para instalação em rack padrão 19", com *hardware* e *software* do mesmo fabricante ou *hardware* homologado pelo fabricante do *software*;

2.4.3.1. Caso *hardware* e *software* não sejam do mesmo fabricante, a solução deverá possuir também:

2.4.3.1.1. No mínimo 2 (dois) processadores de no mínimo 8 (oito) núcleos, frequência de 2,0 GHz e 10Mb de cache;

2.4.3.1.2.. No mínimo 24 (vinte e quatro) GB de memória RAM;

2.4.3.1.3. 2 (dois) discos SSD de no mínimo 480 GB configurados em RAID 1 destinados exclusivamente à instalação do sistema operacional e software de backup;

2.4.3.1.4. 1 (um) TB de armazenamento líquido interno por meio de discos NL-SAS ou tecnologia superior, configurados em RAID 1 ou RAID 5;

2.4.3.1.5. Deverá possuir trilhos deslizantes com gerenciamento de cabos para montagem do equipamento em rack 19";

2.4.3.1.6. Deve ser apresentado na proposta comercial documento que comprove que o equipamento ofertado (fabricante e modelo) seja homologado pelo fabricante do *software* de *mail gateway*;

2.4.3.1.7. Possuir todo o licenciamento necessário ao funcionamento do equipamento;

2.4.3.1.8. As especificações de *hardware* supracitadas servem como referencial mínimo e não limitam a oferta de características, capacidades e recursos superiores ou adicionais eventualmente recomendados pelos fabricantes dos componentes da solução.

2.4.4. Deve estar licenciada e ser capaz de suportar pelo menos 6500 caixas de email.

2.4.5. Desempenho:

2.4.5.1. Deve encaminhar pelo menos 14.000 mensagens de email por hora;

2.4.5.2. A solução deve fornecer proteção contra vírus, SPAM, *phishing*, e-*mail marketing*, *email* adulto e outras formas de ameaças virtuais;

2.4.6. Ser uma solução MTA (*Mail Transfer Agent*) com suporte às RFCs 5321, 5322, 6376, 6531, 7208, 7489, 7504;

2.4.7. A solução deve suportar a verificação da autenticidade dos remetentes utilizando DKIM, SPF ou DMARC;

2.4.8. O *appliance* deve tratar mensagens em ambos sentidos (*inbound* e *outbound*), possibilitando a aplicação de regras e políticas customizáveis e diferenciadas por sentido de tráfego;

2.4.9. A solução deve funcionar em alta disponibilidade e balanceamento de carga;

2.4.10. Caso um dos *appliances* em alta disponibilidade falhe a solução deve continuar a filtragem automaticamente, mantendo o serviço disponível;

2.4.11. Suportar o envio e recebimento de mensagens utilizando protocolo TLS/SSL e a configuração de domínios onde TLS é mandatório;

2.4.12. Prover mecanismo que impeça a utilização como retransmissor de mensagens originadas externamente;

2.4.13. Permitir a criação de regras para mensagens com base em dicionário de palavras com suporte a expressões regulares e pontuação máxima por palavra, atuando de forma independente no conteúdo do anexo, do corpo do *e-mail* e do assunto.

2.4.14. Controlar sessões SMTP e limitar o tráfego de mensagens baseado em endereço IP, faixa de IP, subrede IP, nome de domínio, nome DNS reverso, nome parcial de domínio e reputação do emissor;

2.4.15. Suportar monitoramento SNMPv2 e/ou SNMPv3;

2.4.16. Detectar anexos compactados em múltiplos formatos, incluindo zip, permitindo a definição da ação a ser executada;

2.4.17. Possuir integração com LDAP e *Microsoft Active Directory* para verificação de destinatários válidos e criação de regras de filtragem;

2.4.18. A integração LDAP deve permitir a conexão de maneira segura (LDAPS);

2.4.19. Permitir a aplicação de políticas de SPAM diferentes por domínio do destinatário, por destinatários específicos, permitindo o uso de expressões regulares e integrando-se com AD/LDAP;

2.4.20. Implementar limite personalizado pelo administrador do número de destinatários por mensagem;

2.4.21. Implementar limite personalizado pelo administrador do número máximo de conexões simultâneas;

2.4.22. Permitir a inclusão de múltiplas listas de remetentes bloqueados em tempo real (*realtime black list-RBL*), permitindo regras de bloqueio personalizadas;

2.4.23. Possuir funcionalidade de verificação de DKIM (*DomainKeys Identified Mail*) e SPF (*Sender Policy Framework*), permitindo regras individuais e personalizadas para usuários ou grupos de usuários, permitindo criar ações específicas de acordo com o resultado da consulta SPF;

2.4.24. Possuir funcionalidade de rDNS (*Reverse DNS Lookup*);

2.4.25. Possuir mecanismo para prevenção de ataque de diretório (*Directory Harvest Attack*);

2.4.26. Rejeitar mensagens para destinatários inválidos durante o diálogo SMTP (*NonDelivery Report Attack*);

2.4.27. Possuir módulo de detecção "Hora Zero" para a identificação de novas ameaças desconhecidas pelo antivírus;

2.4.28. Deve ser capaz de analisar vírus e spam tanto nos e-mails de entrada quanto nos emails de saída;

2.4.29. Deve controlar *e-mail bounce* (retorno de mensagem não enviada pelo usuário), permitindo ao administrador estabelecer regras específicas;

2.4.30. Deve ser capaz de filtrar as mensagens utilizando os seguintes critérios:

2.4.30.1. Assinaturas para corpo da mensagem e anexos;

2.4.30.2. Heurística, por meio de análise de cabeçalhos, conteúdo e estrutura da mensagem;

2.4.30.3. Filtro de reputação (IP/Domínio do remetente);

2.4.30.4. URLs;

2.4.30.5. Filtros *anti-phishing*.

2.4.31. O sistema de reputação utilizado pela solução deve utilizar dados de redes de monitoração de tráfego *web* e de email para definir a reputação dos remetentes, com cobertura global;

2.4.32. As bases de consulta de reputação devem oferecer atualizações periódicas em intervalos configurados pelo administrador;

2.4.33. Possuir listas negras e listas brancas para endereços IP, domínios e usuários;

2.4.34. Detectar anexos criptografados ou protegidos por senhas, permitindo a definição da ação a ser executada;

2.4.35. Identificar arquivos anexados pelo tipo real, pelo nome, pela extensão e pelo tipo MIME;

2.4.36. Executar, no mínimo, as seguintes ações nos *e-mails* classificados como SPAM:

2.4.36.1. Alterar o assunto da mensagem;

2.4.36.2. Adicionar cabeçalhos personalizados;

2.4.36.3. Descartar a mensagem;

2.4.36.4. Mover para quarentena definida pelo administrador;

2.4.37. Gerenciamento:

2.4.37.1. Possuir interface *web* de administração segura com HTTPS;

2.4.37.2. Suportar de forma centralizada a geração de relatórios, rastreamento de mensagens, gerenciamento de usuários e gerenciamento do *appliance;*

2.4.37.3. Possuir níveis granulares de administração, permitindo a criação de perfis diferentes de administradores e/ou visualizadores na console;

2.4.37.4. Realizar *backup*/restauração das configurações da ferramenta, com a possibilidade de exportação do(s) arquivo(s) de *backup;*

2.4.37.5. Permitir a liberação/entrega de mensagens na quarentena;

2.4.37.6. Permitir a notificação para o fabricante de mensagens classificadas como Falso Negativo ou Falso Positivo;

2.4.37.7. Possibilitar a exportação dos registros (logs) de mensagens nos formatos csv ou html;

2.4.37.8. Possibilitar o envio dos registros (logs) para servidor externo;

2.4.37.9. Possuir capacidade de registro e pesquisa das mensagens processadas pela solução. O número máximo de mensagens retidas com essa finalidade pode ser alterado de acordo com
critérios configuráveis, como espaço disponível/utilizado em disco e tempo de expiração das mensagens;

2.4.37.10. A pesquisa das mensagens eletrônicas processadas pela solução deve ser feita de forma centralizada e por interface única, utilizando, ao menos, os seguintes critérios:

2.4.37.10.1. Data e hora;

2.4.37.10.2. Intervalo de datas;

2.4.37.10.3. Destinatário(s);

2.4.37.10.4. Remetente;

2.4.37.10.5. IP de origem;

2.4.37.10.6. Identificador da regra de bloqueio;

2.4.37.10.7. Assunto;

2.4.37.10.8. Ação realizada (entrega, bloqueio, quarentena, etc).

2.4.37.11. A pesquisa das mensagens deve retornar, no mínimo, as seguintes informações:

2.4.37.11.1. Destinatário(s);

2.4.37.11.2. Remetente;

2.4.37.11.3. IP de origem;

2.4.37.11.4. Tamanho da mensagem;

2.4.37.11.5. Regra(s) de bloqueio (no caso de mensagens bloqueadas);

2.4.37.11.6. Regra(s) de quarentena. Caso a mensagem esteja em quarenta, deve ser possível visualizá- la;

2.4.37.11.7. Ação final (entrega, bloqueio por *spam*, bloqueio por vírus, bloqueio por reputação, etc).

2.4.37.12. Permitir a visualização de um sumário do estado geral da solução e filas de entrega.

2.4.37.13. Permitir a visualização das mensagens nas filas de entrega, agrupando pelos seguintes critérios:

2.4.37.13.1. E-mail do remetente;

2.4.37.13.2. E-mail do destinatário.

2.4.37.14. Possuir funcionalidade de exibição de gráficos com estatísticas no formato *dashboard* para acompanhamento em tempo real do fluxo de *e-mails* da solução.

2.4.37.15. Permitir a criação de diferentes *dashboards* de acordo com critérios estabelecidos por cada administrador, dentre os quais:

2.4.37.15.1. Status da solução;

2.4.37.15.2. Status do *appliance* (serviços em execução, memória, disco, processamento, *status* da alta disponibilidade);

2.4.37.15.3. Volume de mensagens;

2.4.37.15.4. Sumario de *e-mails* bloqueados;

2.4.37.15.5. Sumário de *e-mails* enviados e recebidos;

2.4.37.15.6. Estatísticas de ataques identificados por tipo;

2.4.37.15.7. Estatísticas de vírus;

2.4.37.15.8. Estatísticas de *spam*;

2.4.37.15.9. Estatísticas de conexões completadas e bloqueadas identificadas pelas regras de bloqueio;

2.4.37.15.10. Estatísticas de fluxo de tráfego.

2.4.37.16. Permitir a criação de múltiplas regras para tratamento diferenciado do tráfego de *e-mail*.

2.4.37.17. As regras devem ser configuradas considerando os seguintes critérios:

2.4.37.17.1. Endereço IP de origem;

2.4.37.17.2. *Sender HELO Domain*;

2.4.37.17.3. Envelope *Sender*;

2.4.37.17.4. Endereço de *e-mail* de origem;

2.4.37.17.5. Endereço de *e-mail* de destino;

2.4.37.17.6. Grupo do usuário de origem;

2.4.37.17.7. Grupo do usuário de destino;

2.4.37.17.8. Cabeçalhos SMTP;

2.4.37.17.9. Domínio de origem;

2.4.37.17.10. Domínio de destino;

2.4.37.18. Permitir a filtragem individual de mensagens, com base em políticas definidas por domínio, subdomínio, grupo de usuários e usuário individual, de forma integrada com ferramentas de LDAP, mesmo que a mensagem seja destinada a múltiplos destinatários em categorias distintas.

2.4.37.19. Permitir a criação de regras para tratamento de mensagens com arquivos anexos baseadas nos seguintes critérios:

2.4.37.19.1. Nome do arquivo;

2.4.37.19.2. Tamanho do arquivo ou da mensagem;

2.4.37.19.3. Extensão;

2.4.37.19.4. Arquivos com senha.

2.4.37.20. Deve ser possível a criação de regras combinando-se múltiplos critérios.

2.4.37.21. Permitir a criação de regras personalizadas para tratamento de mensagens de acordo com os seguintes critérios:

2.4.37.21.1. Endereço IP de origem;

2.4.37.21.2. Envelope *Sender*;

2.4.37.21.3. Cabeçalhos SMTP;

2.4.37.21.4. Usuário(s) específico(s).

2.4.37.22. A criação de regras personalizadas deve permitir a utilização de expressões regulares para filtrar informações presentes na comunicação SMTP, nos campos do cabeçalho SMTP, nos anexos e no corpo da mensagem.

2.4.37.23. As ações a serem tomadas pelas regras personalizadas especificadas acima devem incluir:

2.4.37.24.1. Descarte da mensagem;

2.4.37.24.2. Inclusão de informação personalizada nos cabeçalhos da mensagem;

2.4.37.24.3. Envio de cópia da mensagem para quarentena;

2.4.37.24.4. Adição de destinatários;

2.4.37.24.5. Remoção de anexos.

2.4.37.25. As regras de filtragem devem permitir a criação de exceções, por, no mínimo, os seguintes critérios:

2.4.37.25.1. Rotas;

2.4.37.25.2. Usuário(s) específico(s).

2.4.37.26. Deve possuir tecnologia *online* (nuvem do fabricante) para proteção de URLs em tempo real (no momento do clique).

2.4.37.27. Deve ser capaz de identificar URLs suspeitas no corpo da mensagem, permitindo a execução das seguintes ações:

2.4.37.27.1. Bloqueio da mensagem;

2.4.37.27.2. Bloqueio da URL;

2.4.37.27.3. Envio da mensagem para quarentena;

2.4.37.27.4. Redirecionamento para página contendo alerta sobre o bloqueio da URL;

2.4.37.27.5. Redirecionamento da URL para página responsável por realizar a análise toda vez em que ela for acessada;

2.4.37.27.6. Reescrever URLs suspeitas substituindo-as por outra segura, que direciona para uma página personalizada da ferramenta.

2.4.37.28. Deve implementar *sandbox* local ou em nuvem para análise profunda de arquivos anexos suspeitos.

2.4.37.28.1. A *sandbox* deve ser totalmente integrada com os demais módulos da solução.

2.4.37.28.2. A submissão dos arquivos suspeitos deve ocorrer de maneira transparente e automatizada, sem nenhuma necessidade de intervenção do administrador.

2.4.37.28.3. Caso seja ofertada *sandbox* em nuvem, os anexos suspeitos devem enviados de forma criptografada e anônima. Além disso, após a análise da ameaça os anexos suspeitos devem ser eliminados definitivamente da *sandbox*.

2.4.37.29. Deve permitir a criação de regras de exclusão baseadas nos seguintes critérios:

2.4.37.29.1. Endereço de origem;

2.4.37.29.2. Domínio de origem;

2.4.37.29.3. Domínio de destino;

2.4.37.29.4. Tipos de arquivos;

2.4.38. Quarentena:

2.4.38.1. Deve permitir controle de acesso para as mensagens em quarentena por usuários ou grupos específicos.

2.4.38.2. Deve permitir ao administrador configurar individualmente regras específicas para retenção em cada pasta da quarentena, de acordo com critérios como espaço em disco utilizado ou período de tempo máximo.

2.4.38.3. As mensagens devem ser excluídas automaticamente caso os limites para retenção sejam excedidos.

2.4.38.4. Deve permitir novo processamento para as mensagens, incluindo as seguintes ações:

2.4.38.4.1. Notificação de falso positivo/negativo;

2.4.38.4.2. Envio para o destinatário;

2.4.38.4.3. Encaminhamento para *e-mail*(s) específico(s);

2.4.38.4.4. Movimentação para outra pasta da quarentena;

2.4.38.4.5. Nova submissão da mensagem às regras configuradas pelo administrador.

2.4.38.5. Deve ser capaz de enviar notificação para os usuários, informando as mensagens consideradas como *SPAM* que foram inseridas na quarentena.

2.4.39. Monitoramento e alertas:

2.4.39.1. Possuir recurso de monitoramento do sistema, alertando o administrador caso ocorram falhas operacionais ou eventos que possam comprometer o funcionamento adequado da solução, tais como:

2.4.39.1.1. Baixo espaço em disco;

2.4.39.1.2. Fila de mensagens maior que limite;

2.4.39.1.3. Falha ao tentar atualizar repositório spam/vírus após número limite de tentativas;

2.4.39.1.4. Indisponibilidade de *appliance*;

2.4.39.1.5. Envio de e-mails acima de uma certa quantidade por determinado endereço/usuário.

2.4.40. Relatórios:

2.4.40.1. Permitir a geração de relatórios de forma centralizada e por interface única.

2.4.40.2. Permitir o agendamento de relatórios e o envio periódico para *e-mails* específicos.

2.4.40.3. Permitir seleção de dados para geração de relatórios por data específica ou intervalo de datas.

2.4.40.4. Permitir a exportação dos relatórios de mensagens para no mínimo dois dos seguintes formatos: csv, html, pdf.

2.4.40.5. Os relatórios devem ser disponibilizados em formato de gráfico, bem como em tabelas com dados dispostos em linhas e colunas, contemplando pelo menos os seguintes tipos:

2.4.40.5.1. Sumário com total de mensagens classificadas como: spam, vírus, aceitas, rejeitadas;

2.4.40.5.2. Relatórios sobre volume e tipo de *spam* recebido;

2.4.40.5.3. Relatórios de conexões SMTP: rejeitadas por reputação e rejeitadas por controle de conexões.

2.5. Equipamento Web Application Firewall:

2.5.1. Deverá ser fornecido com 2 (duas) fontes de alimentação redundante 100 a 240 VAC, com potência suficiente para suprir a configuração máxima do equipamento;

2.5.2. Deve ser fornecido com acessórios para instalação em rack padrão 19”.

2.5.3. *Hardware* e *software* que compõem o *appliance* devem ser do mesmo fabricante;

2.5.4. O licenciamento do *appliance* deverá contemplar um número ilimitado de usuários e endereços de rede, sendo o único limitador a capacidade tecnológica especificada neste Instrumento e no Termo de Referência, não a quantidade de usuários.

2.5.4. Desempenho:

2.5.4.1. Introduzir latência inferior a 5 milissegundos, a fim de não impactar no desempenho das aplicações Web;

2.5.4.2. Deve possuir *throughput* mínimo de 250 Mbps;

2.5.4.3. Deve possuir pelo menos 04 (quatro) interfaces 1GbE RJ45 ou SFP com *transceivers* 1GbE RJ45.

2.5.4.4. Deve possuir pelo menos 1 (uma) interface serial RJ45 ou USB para acesso à console local integrada ao equipamento ou via cabos e conversores externos.

2.5.5. Rede:

2.5.5.1. Possuir LEDs para a indicação do status e atividade das interfaces;

2.5.5.2. A solução deve ser capaz de ser implementada no modo *proxy* (transparente e reverso), passivo e *inline* transparente (*bridge*);

2.5.5.3. Suportar VLANs no padrão IEEE 802.1q.

2.5.5.4. Deve implementar o protocolo de negociação *Link Aggregation Control Protocol* (LACP) - IEEE 802.3ad;

2.5.5.5. Suportar endereçamento IPv4 e IPv6 nas interfaces físicas e virtuais (*VLANs*);

2.5.5.6. A solução deve suportar e oferecer cluster de alta disponibilidade entre dois dispositivos no modo ativo-passivo e ativo-ativo, para que em caso de falha do principal o tráfego possa continuar sendo processado;

2.5.5.7. A solução deve suportar a sincronização de configuração entre dois *appliances* iguais, com o objetivo de operar no modo ativo-ativo, com a distribuição de tráfego sendo realizada por balanceador de carga externo ou pela própria solução;

2.5.5.8. A solução deve suportar roteamento por política (*policy route*).

2.5.6. Gerência:

2.5.6.1. O sistema operacional / *firmware* deve suportar interface gráfica web para a configuração das funções do sistema operacional, utilizando navegadores disponíveis gratuitamente e protocolo HTTPS, ou através de CLI (interface de linha de comando) via porta de console local ou remotamente via SSH;

2.5.6.2. Deve possuir administração baseada em interface web HTTPS;

2.5.6.3. A solução deve possuir interface gráfica com informações sobre o sistema (informações do *cluster*, *hostname*, número de série, modo de operação, tempo em serviço, versão do *firmware*);

2.5.6.4. Deve ser possível visualizar através da interface gráfica de gerencia informações de licenças, assinaturas e contrato de suporte;

2.5.6.5. Deve prover, na interface de gerencia, as seguintes informações do sistema para cada *gateway*: consumo de CPU e estatísticas das conexões;

2.5.6.6. Deve ser possível visualizar na interface de gerência as informações de consumo de memória;

2.5.6.7. Deve possuir ferramenta na interface gráfica de gerência (*dashboard*) que permita visualizar os últimos logs de ataque detectados/bloqueados;

2.5.6.8. Deve prover as seguintes informações, na interface de gráfica de gerência: estatísticas de *throughput* HTTP em tempo real, estatísticas dos eventos de ataque detectados/bloqueados, estatísticas de requisições HTTP em tempo real e últimos logs de eventos do sistema;

2.5.6.9. Possuir na interface gráfica estatísticas de conexões concorrentes e por segundo, de políticas de segurança do sistema;

2.5.6.10. Possuir um painel de visualização com informações das interfaces de rede do sistema;

2.5.6.11. A configuração de administração da solução deve possibilitar a utilização de perfis;

2.5.6.12. Deve ser possível executar e restaurar *backup* via interface Web (GUI);

2.5.6.13. Deve ter a opção para criptografar o *backup* utilizando algoritmo AES 128-bit ou superior;

2.5.6.14. Deve ser possível executar e restaurar *backup* utilizando-se FTP e SFTP;

2.5.6.15. Deve ser possível instalar um *firmware* alternativo em disco e inicializá-lo em caso de falha do *firmware* principal;

2.5.6.16. Deve ter suporte ao protocolo de monitoração SNMP v2c e/ou SNMP v3;

2.5.6.17. Deve ser capaz de realizar notificações de eventos de segurança através de *e-mail*, *traps* SNMP e Syslog;

2.5.6.18. A solução deve ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo Syslog;

2.5.6.19. A solução deve ter a capacidade de enviar alertas por *email* de eventos baseados em severidades e/ou categorias;

2.5.6.20. A solução deve possuir dados analíticos contendo localização geográfica dos clientes *web;*

2.5.6.21. A solução deve possuir dados analíticos, sendo possível visualizar a contagem total de ataques e percentual de cada país de origem, o volume total de tráfego em bytes e percentual de cada país de origem e o total de acessos (*hits*) e percentual de cada país de origem;

2.5.6.22. Deve ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário;

2.5.6.23. Deve ter suporte a *RESTful* API para gerenciamento de configurações.

2.5.7. Autenticação:

2.5.7.1. Os usuários devem ser capazes de autenticar através de:

2.5.7.1.1. Cabeçalho de autorização HTTP / HTTPS;

2.5.7.1.2. Formulários HTML embutidos;

2.5.7.1.3. Certificados digitais pessoais.

2.5.7.2. Deve possuir base local para armazenamento e autenticação contas de usuários;

2.5.7.3. A solução deve ter a capacidade de autenticar usuários em bases externas/remotas LDAP e RADIUS;

2.5.7.4. Os usuários devem ser capazes de autenticar através de contas de usuários em base remota NTLM;

2.5.7.5. A solução deve ser capaz de criar grupos de usuários para acessos semelhantes na autenticação.

2.5.8. Filtragem:

2.5.8.1. Deverá ser capaz de identificar e bloquear ataques através de um banco de dados de assinaturas de vírus e IP *reputation*, atualizado de forma automática;

2.5.8.2. Possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários e o que se espera de cada campo;

2.5.8.3. O perfil aprendido de forma automatizada pode ser ajustado e editado;

2.5.8.4. A solução deve possuir geração de relatório com as informações obtidas em auto-aprendizagem, com as estatísticas e as políticas de tráfego coletados, os relatórios de ataques, eventos e relatórios de verificação de vulnerabilidade para fins de cumprimento das regulamentações;

2.5.8.5. Ter a capacidade de criação de assinaturas de ataque customizáveis;

2.5.8.6. Ter a capacidade de proteção para ataques do tipo *Adobe Flash binary* (AMF) protocol;

2.5.8.7. Ter a capacidade de proteção para ataques do tipo *Botnet* e Browser *Exploit Against* SSL/TLS (*BEAST*);

2.5.8.8. A solução deve possuir funcionalidade de proteção positiva contra ataques como acesso por força bruta;

2.5.8.9. Deve suportar detecção a ataques de *Clickjacking;*

2.5.8.10. Deve suportar detecção a ataques de alteração de *cookie;*

2.5.8.11. Identificar e prevenir ataques do tipo *Credit Card Theft;*

2.5.8.12. Identificar e prevenir ataque *Cross Site Request Forgery* (CSRF);

2.5.8.13. A solução deverá possuir funcionalidade de proteção positiva contra ataques como cross site *scripting* (XSS);

2.5.8.14. Deve possuir proteção contra ataques de *Denial of Service* (DoS);

2.5.8.15. Ter a capacidade de proteção para ataques do tipo:

2.5.8.15.1. HTTP *header overflow*.

2.5.8.15.2. *Local File inclusion* (FLI);

2.5.8.15.3. *Man-in-the-middle* (MITM);

2.5.8.15.4. *Remote File Inclusion* (RFI);

2.5.8.15.5. *Server Information Leakage*;

2.5.8.15.6. *Malformed* XML;

2.5.8.15.7. *SYN flood*;

2.5.8.15.8. *Forms Tampering*;

2.5.8.15.9. *Directory Traversal*;

2.5.8.15.10. *Slowloris;*

2.5.8.16. Proteção contra envios de comandos SQL ocultos nas requisições enviadas a bases de dados (SQL *Injection*);

2.5.8.17. Identificar e prevenir ataques do tipo *Low-rate* DoS;

2.5.8.18. Prevenção contra *Slow* POST *attack;*

2.5.8.19. A solução deverá possuir funcionalidade de proteção positiva contra ataques de manipulação de campo oculto;

2.5.8.20. Ter a capacidade de proteção do tipo *Access Rate Control;*

2.5.8.21. Reconhecer e remediar *Zero Day Attacks* (Um ataque de dia zero ocorre no mesmo dia em que um ponto fraco for descoberto no *software*);

2.5.8.22. Ter a capacidade de configurar proteção do tipo *TCP SYN flood-style* para prevenção de DoS para qualquer política, através de *Syn Cookie* e *Half Open Threshold;*

2.5.8.23. Permitir que sejam configuradas regras de limite de *upload* por tamanho de arquivo.

2.5.8.24. Deve permitir que o administrador bloqueie o tráfego de entrada e/ou tráfego de saída com base nos países, sem a necessidade de gerir manualmente os ranges de endereços IP correspondentes a cada país;

2.5.8.25. Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado país seja bloqueado;

2.5.8.26. Permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem;

2.5.8.27. Permitir a liberação temporária ou definitiva (*whitelist*) de endereços IP bloqueados por terem originados ataques detectados pela solução;

2.5.8.28. Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP *Reputation;*

2.5.8.29. Ter a capacidade de prevenção ao vazamento de informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP;

2.5.8.30. Ter a funcionalidade de proteger o *website* contra ações de desfiguração (*defacement*), com restauração automática e rápida do site caso ocorra à falha;

2.5.8.31. Ter a funcionalidade de antivírus integrada para inspeção de tráfego e arquivos;

2.5.8.32. Ter a capacidade de investigar e analisar todo o tráfego HTTP para atestar se está em conformidade com a respectiva RFC, bloqueando ataques e tráfego em não-conformidade;

2.5.8.33. Deverá ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados na solução e as requisições HTTP são enviadas aos servidores sem criptografia;

2.5.8.34. A solução deve ser capaz de funcionar como terminador de sessões SSL para a aceleração de tráfego;

2.5.8.35. Para SSL/TLS offload suportar no mínimo SSL 3.0, TLS 1.0, 1.1 e 1.2;

2.5.8.36. A solução deve ter a capacidade de armazenar certificados digitais de CAs;

2.5.8.37. A solução deve ser capaz de gerar CSR para ser assinado por uma CA;

2.5.8.38. A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL);

2.5.8.39. A solução deve conter as assinaturas de robôs conhecidos como *link checkers*, *indexadores* de *web*, *search engines*, *spiders* e *web crawlers* que podem ser colocados nos perfis de controle de acesso, bem como resetar tais conexões;

2.5.8.40. A solução deve ter um sistema de reputação de endereços IP públicos conhecidos como fontes de ataques DDoS, *botnets*, *spammers*, etc. Tal sistema deve ser atualizado automaticamente;

2.5.8.41. A solução deverá ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores;

2.5.8.42. A solução deve permitir a customização ou redirecionar solicitações e respostas *HTTP no HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body e HTTP Location;*

2.5.8.43. A solução deve permitir criar regras definindo a ordem em que as páginas devem ser acessados para prevenir ataques como *cross-site request forgery* (CSRF);

2.5.8.44. A solução deve ter a capacidade de definir restrições a métodos HTTP;

2.5.8.45. Permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares;

2.5.8.46. A solução deve incluir capacidade de atuar como um *scanner* de vulnerabilidades para diagnóstico e identificação de ameaças nos servidores *web*, *software* desatualizado e potenciais *buffers overflows*.

2.5.8.47. Deve gerar perfil de proteção automaticamente a partir de relatório em formato XML gerado por *scanner* de vulnerabilidade de terceiros;

2.5.8.48. Deve permitir agendar a verificação de vulnerabilidades;

2.5.8.49. A solução deve gerar um relatório da análise de vulnerabilidades no formato HTML;

2.5.8.50. A solução deve permitir a exclusão de URLs na análise de vulnerabilidades;

2.5.8.51. Deverá ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

2.5.8.52. Suportar redirecionamento e reescrita de requisições e respostas HTTP;

2.5.8.53. Permitir redirecionamento de requisições HTTP para HTTPS;

2.5.8.54. Permitir reescrita dos seguintes campos no cabeçalho de uma requisição HTTP:

2.5.8.54.1. URL;

2.5.8.54.2. *Host*;

2.5.8.54.3. *Referer*.

2.5.8.55. Permitir redirecionamento de requisições para outro *web site;*

2.5.8.56. Permitir envio de resposta *HTTP 403 Forbidden* para requisições HTTP;

2.5.8.57. Permitir reescrita do parâmetro "*Location*" no cabeçalho HTTP de uma resposta de redirecionamento HTTP de um servidor *web;*

2.5.8.58. Permitir reescrita do corpo ("*body*") de uma resposta HTTP de um servidor web.

2.5.8.59. Permitir adição do campo *X-Forwarded-For* para identificação do endereço real do cliente quando no modo de *proxy reverso;*

2.5.8.60. A solução deve suportar regras para definir se as solicitações HTTP serão aceitas com base na URL e a origem do pedido e, se necessário, aplicar uma taxa específica de transferência (*rate limit*)

2.5.8.61. Possuir capacidade de *caching* para aceleração *web;*

2.5.8.62. Deve ser capaz de submeter arquivos para solução de *sandboxing;*

2.5.8.63. Deve permitir ao administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes.

2.5.9. Balanceamento de Carga:

2.5.9.1. A solução deve incluir funcionalidade de balanceamento de carga entre servidores *web;*

2.5.9.2. Deve suportar configuração de portas não-padrão para aplicação *web* HTTP e HTTPS;

2.5.9.3. Deve balancear/distribuir tráfego e rotear o conteúdo através de vários servidores *web*.

2.5.9.4. Deve permitir a criação de grupos de servidores (*Server Farm* / *Pool*) para distribuir as conexões dos usuários;

2.5.9.5. O balanceamento de carga de servidores deve suportar os algoritmos:

2.5.9.5.1. *Round Robin*;

2.5.9.5.2. *Weighted Round Robin*;

2.5.9.5.3. *Least Connections*.

2.5.9.6. A solução deve ser capaz de criar servidores virtuais que definem a interface de rede/*bridge* e endereço IP por onde o tráfego destinado ao *Server Pool* é recebido.

2.5.9.7. Os servidores virtuais devem entregar o tráfego à um único servidor web e também possuir a opção de distribuir as sessões/conexões entre os servidores *web* do *Server Pool*.

2.5.9.8. Deve ser possível especificar o número máximo de conexões TCP simultâneas para um determinado servidor membro do *Server Pool*.

2.5.9.9. Deve possibilitar teste de disponibilidade de servidor *web* através de:

2.5.9.9.1. Método TCP;

2.5.9.9.2. Servidor *web* através do método *ICMP ECHO_REQUEST* (ping);

2.5.9.9.3. Método *TCP Half Open*;

2.5.9.9.4. TCP SSL;

2.5.9.9.5. Métodos HTTP e HTTPS;

2.5.9.9.5.1. Nos testes de disponibilidade HTTP e HTTPS, permitir a indicação de:

2.5.9.9.5.1.1. URL exata a ser testada;

2.5.9.9.5.1.2. Método HEAD, GET e POST;

2.5.9.9.5.1.3. Nome do campo HTTP "host" a ser testado;

2.5.9.10. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de:

2.5.9.10.1. Host;

2.5.9.10.2. URL;

2.5.9.10.3. Parâmetro HTTP;

2.5.9.10.4. Referer;

2.5.9.10.5. Endereço IP de origem;

2.5.9.10.6. Cabeçalho;

2.5.9.10.7. *Cookie*;

2.5.9.10.8. Campo do Certificado X509.

2.5.9.11. Implementar cache de conteúdo para HTTP, permitindo que objetos sejam armazenados e requisições HTTP sejam respondidas diretamente pela solução.

2.5.9.12. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por:

2.5.9.12.1. Endereço IP de origem;

2.5.9.12.2. Parâmetro do cabeçalho HTTP;

2.5.9.12.3. URL acessada;

2.5.9.12.4. *Cookie* – método *cookie* insert e *cookie rewrite*;

2.5.9.12.5. *Embedded cookie* (*cookie* original mais porção randômica);

2.5.9.12.6. Reescrita de *cookie*;

2.5.9.12.7. Cookie persistente;

2.5.9.12.8. ASP *session* ID;

2.5.9.12.9. PHP *Session* ID;

2.5.9.12.10. JSP *Session* ID;

2.5.9.12.11. Sessão SSL.

2.6. Serviços de Instalação e Configuração:

2.6.1. Os requisitos aqui definidos aplicam-se aos serviços de instalação e configuração de quaisquer equipamentos ofertados;

2.6.2. Correrá por conta da CONTRATADA toda e qualquer despesa, independentemente da sua natureza, decorrente dos serviços de instalação aqui mencionados;

2.6.3. Os serviços serão prestados em Palmas-TO.

2.6.4. Planejamento:

2.6.4.1. Após o recebimento dos equipamentos, a equipe técnica do Contratante deverá definir juntamente com a CONTRATADA o cronograma de instalação dos mesmos, contendo informações de data, hora, local e atividades a serem realizadas;

2.6.4.2. Durante o processo de implantação a CONTRATADA deverá assegurar a continuidade das aplicações e serviços do Contratante em regime de produção. Em caso de necessidade de interrupção a CONTRATADA deverá informar ao CONTRATANTE antecipadamente, de modo a constar tal observação nas atividades do cronograma;

2.6.4.3. No cronograma de instalação poderão ser definidos períodos fora do horário comercial, assim como fins de semana e feriados;

2.6.5. A CONTRATADA deverá realizar a instalação física assistida de todos os componentes de hardware e software com acompanhamento da equipe técnica do CONTRATANTE;

2.6.6. A CONTRATADA deverá providenciar a aplicação de todas as correções e upgrades de hardware e software, liberados até a data da instalação;

2.6.7. O processo de implantação será considerado concluído assim que todos os requisitos aqui definidos sejam atendidos.

2.6.8. As atividades técnicas deverão estar de acordo com as melhores práticas do fabricante da solução, como otimização de regras, melhoria de controles e topologias de segurança recomendadas.

2.6.9. O técnico designado pela CONTRATADA para executar a implantação deve ser certificado pelo fabricante na respectiva linha de equipamentos.

2.6.10. Após a conclusão dos serviços de instalação, o técnico da CONTRATADA irá realizar monitoramento local da solução por pelo menos 3 (três) dias úteis com acompanhamento da equipe do CONTRATANTE, a fim de identificar e sanar eventuais inconsistências.

2.6.11. Serviços de instalação e configuração – firewall, análise de logs e gerência:

2.6.11.1. Os serviços deverão cobrir os seguintes quantitativos mínimos de equipamentos:

2.6.11.1.1. 1 (um) equipamento firewall tipo 1;

2.6.11.1.2. 1 (um) equipamento firewall tipo 2;

2.6.11.1.3. 2 (dois) equipamentos firewall tipo 3;

2.6.11.1.4. 2 (dois) equipamentos de análise de logs e gerência.

2.6.12. Serviços de instalação e configuração – mail gateway:

2.6.12.1. Os serviços deverão cobrir os seguintes quantitativos mínimos de equipamentos:

2.6.12.1.1. 2 (dois) equipamentos mail gateway;

2.6.13. Serviços de instalação e configuração – web application firewall:

2.6.13.1. Os serviços deverão cobrir os seguintes quantitativos mínimos de equipamentos:

2.6.13.1.1. 2 (dois) equipamentos web application firewall;

2.7. Serviços de treinamento básico e avançado:

2.7.1. Os requisitos aqui definidos aplicam-se aos serviços de treinamento básico e avançado de quaisquer equipamentos ofertados;

2.7.2. A CONTRATADA deverá oferecer capacitação a pelo menos 8 (oito) técnicos designados do CONTRATANTE;

2.7.3. A capacitação será na modalidade presencial nas dependências do CONTRATANTE e ministrada por técnico(s) especialista(s) na solução objeto deste Instrumento e do Termo de Referência;

2.7.4. Deverá cobrir a administração dos componentes da solução, todos os recursos de *hardware* e *software* do ambiente, abrangendo no mínimo os seguintes tópicos:

2.7.4.1. Instalação;

2.7.4.2. Configuração básica e avançada;

2.7.4.3. Operação básica e avançada;

2.7.4.4. Gerenciamento;

2.7.4.5. Solução de problemas (*troubleshooting*);

2.7.4.6. Laboratório prático baseado na solução adquirida.

2.7.5. O material didático e os certificados de conclusão deverão ser disponibilizados pelo fabricante dos equipamentos e não será admitido o uso de material fotocopiado ou qualquer outro que não seja adquirido diretamente do fabricante dos equipamentos;

2.7.6. A capacitação deverá ser direcionada com base nos equipamentos e serviços de instalação ofertados, com ênfase nas configurações realizadas no ambiente do CONTRATANTE;

2.7.7. Serviços de treinamento básico e avançado – firewall, análise de logs e gerência:

2.7.7.1. A carga horária mínima será de 16 (dezesseis) horas, sendo 4 (quatro) horas diárias.

2.7.8. Serviços de treinamento básico e avançado – mail gateway;

2.7.8.1. A carga horária mínima será de 8 (oito) horas, sendo 4 (quatro) horas diárias;

2.7.9. Serviços de treinamento básico e avançado – web application firewal;

2.7.9.1. A carga horária mínima será de 8 (oito) horas, sendo 4 (quatro) horas diárias.

CLÁUSULA TERCEIRA – DA GARANTIA E SUPORTE TÉCNICO:

3.1. Suporte técnico e garantia:

3.1.1. Os equipamentos ofertados deverão ser fornecidos com garantia mínima de 60 (sessenta) meses contados a partir do termo de recebimento definitivo.

3.1.2. Durante a vigência da garantia a CONTRATADA irá atender chamados enviados pelo CONTRATANTE sem ônus adicional, oferecendo no mínimo os seguintes serviços:

3.1.2.1. Direito a atualizações e *upgrades* da solução;

3.1.2.2. Direito de abertura de chamados para atendimento sem limites;

3.1.2.3. Atendimento 24x7 (vinte e quatro horas por dia, nos 7 dias da semana) via telefone 0800 ou *web*.

3.1.3. Os chamados serão resolvidos preferencialmente por meio de assistência remota e caso haja necessidade de ação *on-site*, como envio/recolhimento de equipamentos ou troca de peças, o serviço deverá ser realizado em Palmas/TO.

3.1.4. Os atendimentos poderão ser relativos a substituições de *hardware* ou componente defeituoso; atualizações corretivas e evolutivas de firmware e *software*; ajustes e configurações conforme manuais e normas técnicas do fabricante; demais procedimentos destinados a recolocar a solução em perfeito estado de funcionamento, fornecimento de informações e esclarecimento de dúvidas sobre administração, configuração, otimização, *troubleshooting* ou utilização;

3.1.5. A garantia oferecida deverá incluir peças de reposição, mão de obra, atualizações *firmware* e *software* dos equipamentos fornecidos, com a disponibilização de novas versões por necessidade de correção de problemas ou implementação de novas funcionalidades;

3.1.6. A garantia deverá cobrir a reparação de eventuais falhas dos equipamentos, mediante a substituição de peças e componentes que se apresentem defeituosos, de acordo com os manuais e normas técnicas específicas para os equipamentos, a fim de sanar todos os vícios e defeitos da solução;

3.1.7. A CONTRATADA deverá garantir assistência técnica do próprio fabricante dos equipamentos;

3.1.8. A CONTRATADA, no caso da atualização de equipamento para corrigir falhas apresentadas, deve se responsabilizar pelos custos envolvidos, inclusive eventuais trocas de *hardware* ou substituição do equipamento, cabendo ao CONTRATANTE a emissão de documento fiscal ou equivalente necessário ao transporte do equipamento, quando for o caso.

3.1.9. A assistência técnica utilizará apenas peças e componentes originais salvo nos casos fundamentados por escrito e aceitos por técnicos do CONTRATANTE;

3.1.10. A assistência técnica deverá marcar com antecedência o horário de atendimento do chamado técnico;

3.1.11. Os chamados serão classificados em níveis de severidade, conforme descrito na tabela 2, a contar do momento da abertura do chamado:

Tabela 2 - Níveis de severidade

Severidade	Descrição
1	Equipamento inoperante, causando indisponibilidade total ou intermitente de serviços.
2	Equipamento parcialmente inoperante, causando degradação de desempenho ou ocorrência de mau funcionamento
3	Equipamento operante com ocorrência de alarmes; consultas gerais sobre administração, configuração, otimização, *troubleshooting* ou utilização.

3.1.12. Os chamados deverão ser resolvidos respeitando os prazos descritos na tabela 3, conforme os níveis de severidade e equipamentos envolvidos:

Tabela 3 – Prazos de resolução de chamados

Equipamento	Severidade	Prazo de resolução

Equipamento *firewall* tipo 3 Equipamento *mail gateway* Equipamento *web application firewall*	1	Até 06 (seis) horas
	2	Até 08 (oito) horas
	3	Até 24 (vinte e quatro) horas
Equipamento fir*ewall* tipo 1 Equipamento *firewall* tipo 2 Equipamento de análise de *logs* e gerência	1	Até 72 (setenta e duas) horas
	2	Até 96 (noventa e seis) horas
	3	Até 120 (cento e vinte) horas

CLÁUSULA QUARTA – DA DINÂMICA DE EXECUÇÃO:

4.1. A CONTRATADA alocará um coordenador de projeto, com capacitação técnica na solução oferecida, que atuará como interface entre a equipe do CONTRATANTE e a equipe da CONTRATADA.

4.2. O objeto deve ser entregue na Divisão de Administração e Segurança de Rede, localizada na Sede do CONTRATANTE, Palácio da Justiça Rio Tocantins, Praça dos Girassóis, s/n, Centro, Palmas/TO, CEP 77015-007.

4.3. A CONTRATADA deverá entregar os equipamentos em até 45 (quarenta e cinco) dias subsequentes a contar do recebimento da nota de empenho.

4.4. A CONTRATADA deverá iniciar os serviços de capacitação de técnicos do CONTRATANTE e implantação da solução em até 15 (quinze) dias subsequentes, a contar das respectivas emissões de ordem de serviço.

4.5. Logística de implantação:

4.5.1. A CONTRATADA deverá implantar a solução descrita neste Instrumento e no Termo de Referência, a fim de garantir seu funcionamento em ambiente de produção;

4.5.2. O CONTRATANTE disponibilizará o espaço físico necessário em suas dependências para a realização dos serviços;

4.5.3. Caberá à CONTRATADA a execução de todas as atividades, bem como o fornecimento de todos os materiais necessários e suficientes para a instalação e configuração dos equipamentos fornecidos;

4.5.4. Todas as atividades referentes deverão ser agendadas junto à equipe técnica do CONTRATANTE.

CLÁUSULA QUINTA – DO RECEBIMENTO:

5.1. Dos bens permanentes:

5.1.1. Com fulcro nos artigos 25 e 26, da Portaria n° 145, de 2011, elaborada pelo CONTRATANTE, será criada uma Comissão de Recebimento Provisório e Definitivo, designada pelo Diretor Geral, ou por quem este delegar competência, para receber os objetos relativos aos bens permanentes Equipamento *Firewall* Tipo 1, 2 e 3, Equipamento de Análise de *Logs* e Gerência, Equipamento *Mail Gateway* e Equipamento *Web Application Firewall;*

5.1.2. O CONTRATANTE expedirá "Termo de Recebimento Provisório", o qual deverá ser assinado pelos membros da Comissão de Recebimento, conforme arts. 25 e 26 da Portaria n° 145, de 2011, do CONTRATANTE, para efeito de posterior verificação da conformidade dos objetos com as especificações constantes neste Instrumento e no Termo de Referência, nos termos do artigo 73, II, *"a",* da Lei n° 8.666, de 1993;

5.1.3. Após a verificação da qualidade e quantidade dos materiais e/ou equipamentos e consequente aceitação, nos termos do artigo 73, II, *"b",* da Lei n° 8.666, de 1993, o CONTRATANTE emitirá "Termo de Recebimento Definitivo", no prazo de 15 (quinze) dias úteis, o qual deverá ser assinado pelos membros da Comissão de Recebimento.

5.2. Dos serviços:

5.2.1. O CONTRATANTE expedirá "Termo de Recebimento Provisório", para os objetos relativos aos serviços de Instalação e Configuração – *Firewall*, Análise de *Logs* e Gerência, Treinamento Básico e Avançado – Firewall, Análise de *Logs* e Gerência, Instalação e Configuração – *Mail Gateway*, Treinamento Básico e Avançado – *Mail Gateway*, Instalação e Configuração – *Web Application Firewall*, Treinamento Básico e Avançado – *Web* Application *Firewall*, para efeito de posterior verificação da conformidade do objeto com as especificações constantes neste Instrumento e no Termo de Referência, mediante termo circunstanciado, assinado pelo Gestor em até 15 (quinze) dias úteis da comunicação escrita da CONTRATADA, nos termos do artigo 73, I*, "a",* da Lei n° 8.666, de 1993;

5.2.2. O CONTRATANTE emitirá "Termo de Recebimento Definitivo", mediante termo circunstanciado, assinado pelo Gestor, após o decurso do prazo de 15 (quinze) dias úteis de observação ou vistoria que comprove a adequação do objeto aos termos deste Instrumento e do Termo de Referência, nos termos do artigo 73, I, *"b",* da Lei n° 8.666, de 1993.

5.3. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança dos produtos/serviços fornecidos, nem ético-profissional, para perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou pelo contrato.

5.4. A CONTRATADA é obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.

CLÁUSULA SEXTA – DO VALOR:

6.1. O valor ordinário do presente Instrumento é de **R$ 1.015.706,67 (um milhão, quinze mil setecentos e seis reais e sessenta e sete centavos)** , compreendendo todas as despesas e custos diretos e indiretos necessários à perfeita execução deste Contrato.

CLÁUSULA SÉTIMA – DA DOTAÇÃO ORÇAMENTÁRIA:

7.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do CONTRATANTE deste exercício, na dotação abaixo discriminada:

Unidade Gestora: 06010 - Funjuris
Classificação Orçamentária: 06010.02.061.1145.3066
Natureza de Despesa: 44.90.52 / 33.90.40
Fonte de Recursos: 0240

7.2. As despesas inerentes à execução deste Contrato serão liquidadas por meio da Nota de Empenho que será emitida à conta da dotação orçamentária especificada nesta Cláusula.

7.3. A CONTRATADA emitirá Nota Fiscal em observância à unidade gestora emissora da nota de empenho que albergou a aquisição:

7.3.1. **Fundo Especial de Modernização e Aprimoramento do Poder Judiciário - Funjuris.**
CNPJ/MF: 03.173.154/0001-73
Praça dos Girassóis, S/Nº. - Centro
CEP: 77.015-007
Palmas/TO.

CLÁUSULA OITAVA – DO PAGAMENTO:

8.1. A CONTRATADA deverá apresentar nota fiscal, correspondente aos objetos efetivamente fornecidos.

8.2. A nota fiscal/fatura deverá indicar o número da conta corrente e agência bancária para emissão da respectiva Ordem Bancária, além do número da nota de empenho.

8.3. Caso tenha ocorrido o fornecimento de produtos importados, juntamente com a nota fiscal/fatura deverá ser apresentado documento que comprove a origem dos produtos e a quitação dos tributos de importação a eles referentes, se for o caso, sob pena de rescisão contratual e multa.

8.4. Sobre a fatura incidirão os tributos legalmente instituídos e as multas que eventualmente vierem a ser aplicadas. Sendo a CONTRATADA isenta ou beneficiária de redução de alíquota de qualquer imposto, taxa ou de contribuição social ou ainda optante pelo SIMPLES, deverá apresentar junto com a fatura, cópia do comprovante respectivo.

8.5. O CONTRATANTE reserva-se o direito de não realizar o atesto, se os dados estiverem em desacordo com os dados da CONTRATADA ou, ainda, se os objetos entregues não estiverem em conformidade com as especificações apresentadas neste Contrato e no Termo de Referência, ficando o pagamento suspenso até a regularização.

8.6. O atesto do gestor é condição indispensável para o pagamento.

8.7. Na ausência do gestor do contrato (férias, licença ou viagem por interesse do CONTRATANTE), o atesto será dado pelo gestor substituto.

8.8. O pagamento será efetuado em até 30 (trinta) dias corridos, contados a partir da data do protocolo de recebimento da nota fiscal (momento em que o credor está adimplente com a obrigação firmada perante o CONTRATANTE), sendo que, recaindo sobre dias não úteis, o termo final será prorrogado para o dia útil subseqüente.

8.9. O pagamento será realizado, no prazo previsto no subitem anterior, por meio de ordem bancária em conta corrente da CONTRATADA: **Banco do Brasil, Agência nº 3478-9, Conta Corrente 45733-8**, quando mantidas as mesmas condições iniciais de habilitação e caso não haja fato impeditivo para o qual não tenha concorrido.

8.10. O CNPJ constante da Nota Fiscal deverá ser o mesmo indicado na proposta e Nota de Empenho.

8.11. Fica a CONTRATADA ciente que por ocasião do pagamento será verificada a sua situação quanto à regularidade fiscal exigida na habilitação, as quais deverão ser mantidas durante toda a execução contratual.

8.12. As notas fiscais/faturas apresentadas em desacordo com o estabelecido neste Contrato e no Termo de Referência e na nota de empenho/contrato ou quando observada qualquer circunstância que desaconselhe o pagamento será devolvida à CONTRATADA e neste caso o prazo previsto nesta Cláusula será interrompido. A contagem do prazo previsto para pagamento será iniciada a partir da respectiva regularização.

8.13. Ocorrendo atraso no pagamento, e desde que tal não tenha concorrido de alguma forma a CONTRATADA, haverá incidência de atualização monetária sobre o valor devido, pela variação acumulada do índice Geral de Preços – Disponibilidade Interna (IGP-DI), coluna 2, publicado pela FGV, ocorrida entre a data final prevista para o pagamento e a data de sua efetiva realização.

8.14. Todos os atos inerentes ao presente processo obedecerão às regras concernentes ao Sistema Eletrônico de Informações – SEI, do CONTRATANTE.

CLÁUSULA NONA – DO REAJUSTE E ALTERAÇÕES:

9.1. O valor contratado é fixo e irreajustável.

9.2. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATADA:

10.1. A CONTRATADA obriga-se a:

10.1.1. Observar as Leis, Decretos, Regulamentos, Portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis a este Contrato;

10.1.2. Atender prontamente às solicitações do CONTRATANTE no fornecimento dos objetos nas quantidades e especificações constantes neste Instrumento, no Termo de Referência de acordo com a necessidade do CONTRATANTE, a partir da solicitação do gestor do contrato;

10.1.3. Manter, durante a execução deste Contrato, todas as condições de habilitação e qualificação exigidas na licitação, em conformidade com art. 55, inciso XIII, da Lei nº 8.666, de 1993, incluindo a atualização de documentos de controle da arrecadação de tributos e contribuições federais e outras legalmente exigíveis;

10.1.4. Responsabilizar-se por todos os recursos e insumos necessários ao perfeito cumprimento do objeto contratado, devendo estar incluídas no preço proposto todas as despesas com materiais, insumos, seguros, impostos, taxas, encargos e demais despesas necessárias à perfeita execução do objeto;

10.1.5. Indicar, formalmente, preposto apto a representá-la junto ao CONTRATANTE, que deverá responder pela fiel execução deste Contrato;

10.1.6. Prestar todos os esclarecimentos técnicos que lhe forem solicitados pelo CONTRATANTE, relacionados com as características e funcionamento do objeto, inclusive em relação aos problemas detectados;

10.1.7. Comunicar, imediatamente, por escrito qualquer anormalidade, prestando ao CONTRATANTE os esclarecimentos julgados necessários;

10.1.8. Manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados; treinados e qualificados para prestação dos serviços.

10.1.9. Manter ficha de controle do serviço, na qual serão relatadas todas as ocorrências;

10.1.10. Assumir inteira responsabilidade técnica e operacional, não podendo, sob qualquer hipótese, transferir para outra empresa a responsabilidade por eventuais problemas na prestação do objeto;

10.1.11. Não transferir a outrem, no todo ou em parte, o objeto desta prestação;

10.1.12. Identificar qualquer equipamento de sua posse que venha a ser utilizado nas dependências do CONTRATANTE, afixando placas de controle patrimonial, selos de segurança etc;

10.1.13. Reparar quaisquer danos diretamente causados ao CONTRATANTE ou a terceiros, por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da presente relação contratual, não excluindo ou reduzindo essa responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pelo CONTRATANTE;

10.1.14. Manter sigilo sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa;

10.1.15. Cumprir integralmente as exigências do Acordo de Nível de Serviço, disposto no Anexo A, do Termo de Referência, Acordo de Nível de Serviço.

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DO CONTRATANTE:

11.1. O CONTRATANTE obriga-se a:

11.1.1. Observar as Leis, Decretos, Regulamentos, Portarias e demais normas legais, direta e indiretamente aplicáveis a este Contrato;

11.1.2. Responsabilizar-se pela lavratura do respectivo contrato, com base nas disposições da Lei;

11.1.3. Receber os objetos de acordo com as disposições constantes neste Contrato e no Termo de Referência;

11.1.4. Comunicar imediatamente a CONTRATADA qualquer incorreção apresentada com os objetos entregues;

11.1.5. Prestar quaisquer esclarecimentos que venham ser formalmente solicitados pela CONTRATADA e pertinente aos objetos, zelando pelo bom andamento desta aquisição, dirimindo quaisquer dúvidas que porventura existam;

11.1.6. Acompanhar e fiscalizar a execução do Contrato;

11.1.7. Assegurar os recursos orçamentários e financeiros para custear os objetos adquiridos e promover os pagamentos dentro dos prazos convencionados neste Contrato e no Termo de Referência;

11.1.8. Processar e liquidar a fatura correspondente aos valores, por meio de Ordem Bancária;

11.1.9. Zelar para que durante a vigência deste Contrato sejam cumpridas as obrigações assumidas por parte da CONTRATADA, bem como sejam mantidas todas as condições de habilitação e qualificação exigidas.

CLÁUSULA DÉCIMA SEGUNDA – DAS SANÇÕES ADMINISTRATIVAS:

12.1. A CONTRATADA que, convocada dentro do prazo de valida da sua proposta, não celebrar o contrato, deixar de entregar a documentação exigida ou apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedido de licitar e contratar com a Administração Pública do Estado do Tocantins e será descredenciada no Sistema de Cadastramento Unificado de Fornecedores (Sicaf), pelo prazo de 5 (cinco) anos, sem prejuízos de multas previstas em edital e no contrato e demais cominações legais.

12.2. Subsidiariamente, nos termos do art. 87 da Lei n° 8.666/93, pela inexecução total ou parcial das condições estabelecidas neste Instrumento, o CONTRATANTE poderá, garantida a prévia defesa da CONTRATADA, que deverá ser apresentada no prazo de 5 (cinco) dias úteis a contar da sua notificação, aplicar, sem prejuízo das responsabilidades penal e civil, as seguintes sanções:

a) Advertência, por escrito, quando a CONTRATADA deixar de atender quaisquer indicações aqui constantes;

b) Multa compensatória/indenizatória no percentual de 5% (cinco por cento) calculado sobre o valor contratado;

c) Suspensão temporária de participação em licitação e impedimento de contratar com o Poder Judiciário do Estado do Tocantins, pelo prazo de até 2 (dois) anos; e

d) 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 Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

12.3. Na hipótese de atraso no cumprimento de quaisquer obrigações assumidas pela CONTRATADA, a esta será aplicada multa moratória de 0,5% (zero vírgula cinco por cento) sobre o valor deste Contrato, por dia de atraso, limitada a 10% (dez por cento) do valor inadimplido.

12.4. O valor da multa aplicada, tanto compensatória quanto moratória, deverá ser recolhido ao Fundo Especial de Modernização e Aprimoramento do Poder Judiciário - Funjuris, dentro do prazo de 5 (cinco) dias úteis após a respectiva notificação.

12.5. Caso não seja paga no prazo previsto no subitem anterior, a multa será descontada por ocasião do pagamento posterior a ser efetuado pelo CONTRATANTE ou cobrada judicialmente.

12.6. Além das penalidades citadas, a CONTRATADA ficará sujeita, ainda, no que couber, às demais penalidades referidas no Capítulo IV da Lei n° 8.666/93.

CLÁUSULA DÉCIMA TERCEIRA – DA RESCISÃO:

13.1. O presente Instrumento poderá ser rescindido:

a) Por ato unilateral e escrito da Administração, nos casos enumerados nos incisos I a XII e XVII e XVIII do art. 78, da Lei 8.666/93;

b) Amigavelmente, por acordo entre as partes, reduzido a termo no respectivo procedimento administrativo, desde que haja conveniência para a Admi nistração; ou

c) Judicialmente, nos termos da Lei.

Parágrafo Único – No caso de rescisão amigável, a parte que pretender rescindir o Contrato comunicará sua intenção à outra, por escrito.

13.2. A CONTRATADA reconhece os direitos do CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993:

13.2.1. A inexecução total ou parcial deste Contrato ensejará a sua rescisão, com às consequências estabelecidas neste Instrumento e as previstas em lei.

CLÁUSULA DÉCIMA QUARTA - DA VINCULAÇÃO:

14.1. O presente Contrato fica vinculado aos autos 19.0.000023571-0 e 20.0.000016856-5.

CLÁUSULA DÉCIMA QUINTA – DA LEGISLAÇÃO E CASOS OMISSOS:

15.1. O presente Instrumento, inclusive os casos omissos, regula-se pela Lei nº 10.520/2002, pelo Decreto nº 10.024, de 20 de setembro de 2019 e, subsidiariamente, pela Lei nº 8.666/1993 e suas alterações posteriores.

CLÁUSULA DÉCIMA SEXTA – DAS VEDAÇÕES:

16.1. É vedado à CONTRATADA:

16.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

16.1.2. Subcontratar, no todo ou em parte, a execução do objeto deste Contrato;

16.1.3. Interromper a execução contratual sob alegação de inadimplemento por parte do CONTRATANTE, salvo nos casos previstos em lei.

CLÁUSULA DÉCIMA SÉTIMA – DA VIGÊNCIA:

17.1. Este Contrato terá inicio a partir da data de sua assinatura e vigência no seu respectivo crédito orçamentário, ressalvado o período de garantia dos objetos e /ou serviços.

CLÁUSULA DÉCIMA OITAVA – DA GESTÃO E FISCALIZAÇÃO:

18.1. Profissionais da CONTRATADA: equipe composta por técnicos da CONTRATADA, responsáveis pela execução e acompanhamento do objeto.

18.1.1. Técnico: funcionário da CONTRATADA, responsável pela execução técnica-operacional.

18.1.2. Preposto: funcionário representante da CONTRATADA, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto ao Gestor do Contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

18.2. Equipe de Gestão do Contrato: equipe composta pelo Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares.

18.2.1. Gestor do Contrato: servidor responsável pela gestão contratual, conforme Decreto Judiciário nº 291, de 2009 e Portaria nº 255, de 2009, do CONTRATANTE.

18.2.2. Fiscal Demandante: servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos funcionais da solução.

18.2.3. Fiscal Técnico: servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução.

18.2.4. Fiscal Administrativo: servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.

18.3. A atuação ou a eventual omissão da Fiscalização durante a realização dos trabalhos, não poderá ser invocada para eximir a CONTRATADA da responsabilidade no fornecimento dos produtos.

18.4. A fiscalização será sob o aspecto qualitativo e quantitativo, devendo ser anotado, em registro próprio as falhas detectadas, e comunicadas ao gestor do Contrato todas as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte da CONTRATADA.

18.5. A comunicação entre a fiscalização e a CONTRATADA será realizada por meio de correspondência oficial e anotações ou registros no mesmo processo que tratam da aquisição dos objetos.

18.6. Quando houver necessidade o gestor deverá emitir notificações para a CONTRATADA.

CLÁUSULA DÉCIMA NONA – DA PUBLICAÇÃO:

19.1. A publicação resumida do presente Contrato no Diário da Justiça Eletrônico - DJE, que é condição indispensável para sua eficácia, será providenciada pelo CONTRATANTE, nos termos do parágrafo único do artigo 61 de Lei nº 8.666/93.

CLÁUSULA VIGÉSIMA – DO FORO:

20.1. Para dirimir todas as questões oriundas do presente Contrato fica eleito o Foro de Palmas - TO, com renúncia expressa de qualquer outro, por mais privilegiado que seja.

E, para firmeza e como prova de assim haverem, entre si, ajustado e contratado, lavrou-se o presente Termo que, depois de lido e achado conforme, vai assinado pelas partes contratantes, por meio de assinatura eletrônica, utilizando-se do Sistema Eletrônico de Informações – SEI, para que produza seus efeitos.

Documento assinado eletronicamente por **Warlen Soares Brandão**, **Usuário Externo**, em 18/09/2020, às 16:06, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Desembargador Helvécio de Brito Maia Neto**, **Presidente**, em 21/09/2020, às 18:33, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.tjto.jus.br/verifica/ informando o código verificador **3328593** e o código CRC **D5C00999**.