TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE INFRAESTRUTURA
SEÇÃO DE SUPORTE ÀS REDES LOCAIS

TERMO DE REFERÊNCIA

I - Objeto (Art. 6º, Inciso XXIII, Alínea "a" da Lei 14.133/2021)

I.1 Aquisição de solução de Firewall de rede (NGFW) *Next Generation Firewall* de Borda em Cluster e Endpoint do fabricante Check Point Software Technologies Ltd, subscrição de licenças, com fornecimento de appliances, licenciamento, software de gerenciamento, serviços de instalação e configuração, suporte técnico e treinamento para a solução ofertada, de acordo com as especificações técnicas e quantidades constantes neste Termo de Referência.

I.2. O objeto desta contratação é classificado como bem comum e não se enquadra como sendo bem de luxo, conforme Portaria da Presidência nº 30, de 20 de junho de 2022.

GRUPO	ITEM	DESCRIÇÃO	DETALHAMENTO	CATMAT/CATSER	QUANTIDADES
1	1	Firewall Principal	Equipamento Firewall do tipo Applaince que operam em cluster	609340	2
	2	Licenças do Firewall I	Licenças do Firewall definido do item 1	26972	2
	3	Firewall Secundário	Equipamento Firewall do tipo Applaince para eventos	609340	10
	4	Licenças do Firewall II	Licenças do Firewall definido do item 3	26972	10
	5	Instalação e configuração	Instalação e configuração dos Firewalls	27120	1
	6	Suporte □técnico para a Solução	Assistência técnica - hardware e Software da solução	27740	1
	7	Treinamento	Treinamento da solução	21172	1
	8	Transceivers	TIPO: Transceivers 1000BASE-T RJ45	13991	8

Planilha1

II - FUNDAMENTAÇÃO DA CONTRATAÇÃO (Art. 6º, Inciso XXIII, Alínea "b" da Lei 14.133/2021)

A fundamentação da contratação está contida no Estudo Técnico Preliminar (ETP) 3997811, presente no Processo Administrativo SEI TRE-RJ nº 2024.0.000009795-4, aprovado em 23 de setembro de 2024, pelo Secretário de Tecnologia da Informação, Michel Marchetti Kovacs.

III - DESCRIÇÃO PORMENORIZADA DA SOLUÇÃO (Art. 6º, Inciso XXIII, Alínea "c", da Lei 14.133/2021)

III.1. - ITEM 1 - EQUIPAMENTO Firewall Principal

Quantidade: 2 (dois)

III.1.1 Características Gerais

III.1.1.1 A solução deverá ser composta de hardware e software licenciado, do mesmo fabricante;

III.1.1.2 A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

III.1.1.3 Na data da proposta, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale;

III.1.1.4 Todos os componentes devem ser próprios para montagem em rack "19" e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário;

III.1.1.5 Os gateways de segurança, bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3;

III.1.1.6 Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

III.1.2 Capacidade e quantidades

III.1.2.1 Solução em Appliance de segurança de perímetro de próxima geração

III.1.2.1.1 Throughput de, no mínimo, 20 (vinte) Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, Anti-Bot e prevenção de ameaças avançadas de dia zero;

III.1.2.1.2 Suporte a, no mínimo, 20M (vinte milhões) de conexões simultâneas;

III.1.2.1.3 Suporte a, no mínimo, 700.000 (setecentos mil) novas conexões por segundo;

III.1.2.1.4 Throughput de, no mínimo, 70 (setenta) Gbps, no mínimo, para conexões VPN;

III.1.2.1.5 Deve suportar a performance considerando as funcionalidades de Next Generation firewall (NGFW) de 65 (sessenta e cinco) Gbps;

III.1.2.1.6 Suportar e estar licenciado para acesso remoto Client-to-site ilimitado ou com a licença de maior capacidade;

III.1.2.1.7 Fonte de alimentação redundante e hot-swappable;

III.1.2.1.8 Througupt de no mínimo, 72 (setenta e dois) Gbps de IPS;

III.1.2.1.9 No mínimo, 04 (quatro) interfaces de rede 10Gbps SFP+;

III.1.2.1.10 No mínimo, 04 (quatro) interfaces de rede 10/100/1000 base-T;

III.1.2.1.11 No mínimo, 04 (quatro) interfaces de rede 25 Gbps SFP28;

III.1.2.1.12 Suportar atualização para no mínimo 02 (duas) interfaces de rede 100/40Gbps QSFP+ ou QSFP28;

III.1.2.1.13 Possuir 1 (uma) interface de rede dedicada para sincronismo;

III.1.2.1.14 Possuir 1 (uma) interface de rede dedicada ao gerenciamento, não sendo permitido utilizar qualquer outra interface para exercer a função de gerenciamento do equipamento;

III.1.2.1.15 Possuir 1 (uma) interface do tipo console ou similar;

III.1.2.1.16 Possuir interface dedicada e fisica para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responde. Caso o equipamento não possua essa interface fisica/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração via software ou uso da interface dedicada de gerenciamento.

III.1.2.1.17 Os equipamentos devem possuir arquitetura modular de interfaces de rede, permitindo a substituição de interfaces por outras com tipo de conexão e velocidades diferentes;

III.1.2.1.18 Cada um dos appliances da plataforma de proteção de rede deve possuir discos Solid State Drive (SSD) redundantes com no mínimo 900 GB de capacidade de armazenamento para o Sistema Operacional.

III.1.2.1.19 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

III.1.2.1.20 Suporte a RFC 4291 de Arquitetura de endereçamento IPv6.

III.1.2.1.21 Solução de suportar Dual stack ipv4/ipv6 e NAT64.

III.1.2.1.22 Deve suportar NAT64 e NAT46;

III.1.2.1.23 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

III.1.2.1.24 Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP v4 e v6 sem duplicação da base de objetos e regras;

III.1.2.1.25 Deve suportar operar em cluster ativo-passivo ou ativo-ativo sem a necessidade de licenças adicionais;

III.1.2.1.26 O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

III.1.2.1.27 Os valores de capacidade são considerados para cada equipamento, não sendo permitido a soma dos valores dos membros do cluster;

III.1.2.1.28 Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização;

III.1.3 Funcionalidade de Firewall

III.1.3.1 A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

III.1.3.2 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;

III.1.3.3 O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

III.1.3.4 A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

III.1.3.5 Realizar upgrade via SCP, SFTP e https via interface WEB

III.1.3.6 Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

III.1.3.6.1 Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;

III.1.3.6.2 Deverá suportar VXLAN;

III.1.3.7 Deve suportar os seguintes tipos de NAT:

III.1.3.7.1 Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino é suportar NAT de Origem e NAT de Destino simultaneamente;

III.1.3.8 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

III.1.3.9 As regras de NAT devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra;

III.1.3.10 Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizados de forma dinâmica, por exemplo: Office 365, AWS, Azure e outros. Objetos dinâmicos que não se caracterizam como FQDN.

III.1.3.11 Enviar logs para sistemas de monitoração externos, simultaneamente;

III.1.3.12 Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

III.1.3.13 Deve realizar roteamentos unicast e multicast simultaneamente em uma única instância(contexto) de firewall.

III.1.3.14 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

III.1.3.15 Suportar OSPF graceful restart;

III.1.3.16 Deve suportar roteamento ECMP (equal cost multi-path);

III.1.3.17 Para o ECMP, a solução deve suportar o balanceamento do roteamento de forma simultânea usando os seguintes parâmetros Origem, Destino, Porta de Origem, Porta de Destino e Protocolo;

III.1.3.18 Autenticação integrada via Kerberos.

III.1.3.19 A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções / ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problemas. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, acesso WEB, alterações de política, comunicação SNMP.

III.1.3.20 As regras Firewall devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra;

III.1.3.21 Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;

III.1.3.22 A solução deve ter a capacidade de operar através de uma única instância de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);

III.1.3.23 A solução deve permitir salvar as configurações das políticas para serem aplicadas em horarios pré-definidos;

III.1.3.24 Deve possuir mecanismo de ativação de validade da regra com período customizado;

III.1.3.25 Deverá suportar redundância e balanceamento de links, tendo capacidade de no mínimo 3 links de internet.

III.1.3.26 Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento.

III.1.3.27 Deve permitir a configuração do tempo de checagem para cada um dos links.

III.1.4 Funcionalidade de Filtro de Conteúdo WEB

III.1.4.1 Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

III.1.4.2 Controle de políticas por usuários, grupos de usuários, IPs e redes;

III.1.4.3 Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3

III.1.4.4 Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

III.1.4.5 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

III.1.4.5.1 Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

III.1.4.5.2 Reconhecer pelo menos 6.000 (seis mil) aplicações diferentes, incluindo, mas não limitado: a 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;

III.1.4.6 A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

III.1.4.7 Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE)

III.1.4.8 Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

III.1.4.9 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

III.1.4.10 A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 150 categorias de aplicações WEB pré-definidas pelo fabricante;

III.1.4.11 Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer.);

III.1.4.12 Possui mecanismo de controle de aplicação web e URL que possui configuração de bloqueio e liberação da aplicação principal e/ou as suas subcategorias. Quando o administrador da solução desejar bloquear apenas as subcategorias do facebook, como facebook chat, video, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser bloqueada toda a categoria como “Facebook” ou "Redes sociais" que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter , YouTube, etc. A solução precisa ser baseada em bloqueio de aplicações WEB que a própria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote.

III.1.4.13A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

III.1.4.14 Atualizar a base de assinaturas de aplicações automaticamente;

III.1.4.15 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

III.1.4.16 Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas entre elas usuários, IP, grupos de usuários do sistema do Active Directory;

III.1.4.17 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

III.1.4.18 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 órgão;

III.1.4.19 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

III.1.4.20 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

III.1.4.20.1 Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

III.1.4.20.2 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

III.1.4.20.3 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 Active Directory e base de dados local;

III.1.4.20.4 Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

III.1.4.20.5 Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;

III.1.4.20.6 Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;

III.1.4.20.7 Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

III.1.4.20.8 Suportar a criação de categorias de URLs customizadas;

III.1.4.20.9 Suportar a exclusão de URLs do bloqueio, por categoria;

III.1.4.20.10 Permitir a customização de página de bloqueio;

III.1.4.21 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, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

III.1.4.22 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API's ou Syslog, para a identificação de endereços IP e usuários;

III.1.4.23 Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

III.1.5 Funcionalidade de filtro de dados

III.1.5.1 A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de arquivos:

III.1.5.1.1 PCI - credit card numbers

III.1.5.1.2 HIPAA - Medical Records Number - MRN

III.1.5.1.3 International Bank Account Numbers - IBAN

III.1.5.1.4 Source Code - JAVA

III.1.5.1.5 U.S. Social Security Numbers - According to SSA

III.1.5.1.6 Salary Survey Terms

III.1.5.1.7 Viewer File - PDF

III.1.5.1.8 Executable file

III.1.5.1.9 Database file

III.1.5.1.10 Document file

III.1.5.1.11 Presentation file

III.1.5.1.12 Spreadsheet file

III.1.5.2 A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload".

III.1.5.3 A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

III.1.5.3 A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes estejam sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

III.1.6 Funcionalidades de Prevenção de Ameaças

III.1.6.1 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 equipamento de firewall;

III.1.6.2 Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

III.1.6.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/passivo;

III.1.6.4 Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

III.1.6.5 A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

III.1.6.6 Deverá possuir os seguintes mecanismos de inspeção de IPS:

III.1.6.6.1 Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

III.1.6.7 Detectar e bloquear a origem de port scans;

III.1.6.8 Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

III.1.6.9 Possuir assinaturas para bloqueio de ataques de buffer overflow;

III.1.6.10 Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

III.1.6.11 Suportar bloqueio de arquivos por tipo;

III.1.6.12 Identificar e bloquear comunicação com botnets;

III.1.6.13 Deve suportar referência cruzada com CVE;

III.1.6.14 Em cada proteção de segurança, deve estar incluso informações como:

III.1.6.14.1 Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro código de referência;

III.1.6.14.2 Severidade;

III.1.6.14.3 Tipo de ação a ser executada.

III.1.6.15 O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

III.1.6.16 O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

III.1.6.17 O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.

III.1.6.18 O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)

III.1.6.19 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

III.1.6.19.1 O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

III.1.6.20 Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

III.1.6.21 Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual;

III.1.6.22 A solução de IPS, deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção devem ser alteradas para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.

III.1.6.23 O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

III.1.6.24 A solução deverá possuir pelo menos dois perfis pré configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

III.1.6.25 A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.

III.1.6.26 Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

III.1.6.27 Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados;

III.1.6.28 O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;

III.1.6.29 A solução de IPS deve possuir engine onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;

III.1.6.30 O antivírus deve oferecer suporte à verificação de links dentro de emails.

III.1.6.31 A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso

III.1.6.32 A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;

III.1.6.33 Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;

III.1.6.34A solução deve permitir a criação de White list baseado no MD5 do arquivo;

III.1.6.35 Os eventos devem identificar o país de onde partiu a ameaça;

III.1.6.36 A funcionalidade de IPS e anti-bot, deve possuir capacidade de correlacionar em seus logs a visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de técnicas de acordo com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

III.1.6.37 Suportar rastreamento de vírus em arquivos pdf;

III.1.6.38 Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

III.1.6.39 Possuir a capacidade de prevenção de ameaças não conhecidas;

III.1.6.40 Em caso de falha no mecanismo de inspeção do Anti-Virus, deve ser possível configurar se as conexões serão permitidas ou bloqueada

III.1.6.41 A solução de Antivírus e Anti-Malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

III.1.6.42 A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;

III.1.6.43 Suportar a criação de políticas por Geolocalização, permitindo que o tráfego de determinado País/Países seja bloqueado;

III.1.6.44 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

III.1.6.45 Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

III.1.6.46 A solução de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

III.1.6.47 A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (command & Control);

III.1.6.48 A solução Antivírus deverá suportar a análise de links no corpo de emails.

III.1.7 Funcionalidades de Controle de Qualidade de Serviço

III.1.7.1 Suportar a criação de políticas de QoS por:

III.1.7.1.1 Endereço de origem, endereço de destino e por porta;

III.1.7.2 O QoS deve possibilitar a definição de classes por:

III.1.7.2.1 Banda garantida, banda máxima e fila de prioridade;

III.1.7.2.2 Disponibilizar estatísticas em tempo real para classes de QoS;

III.1.8 Funcionalidade de VPN

III.1.8.1 Suportar VPN Site-to-Site e Cliente-To-Site;

III.1.8.2 Suportar IPSec VPN;

III.1.8.3 A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);

III.1.8.4 Suportar SSL VPN;

III.1.8.5 A VPN IPSEc deve suportar:

III.1.8.5.1 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard), SHA-512 e Autenticação via certificado IKE PKI;

III.1.8.5.2 A solução deve possuir checagem de conformidade e verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus, firewall no host, chaves de registros e processos ativos;

III.1.8.5.3 A solução deve permitir bloquear o acesso dos usuários aos recursos via VPN caso o usuario não esteja em conformidade com a verificação dos parâmetros configurados.

III.1.8.6 A VPN SSL deve suportar:

III.1.8.6.1 permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

III.1.8.6.2 As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

III.1.8.6.3 Suportar configuração de conformidade para acesso do usuário via portal SSL ou cliente na máquina do usuário;

III.1.8.6.4 Atribuição de endereço IP nos clientes remotos de VPN;

III.1.8.6.5 Atribuição de DNS nos clientes remotos de VPN;

III.1.8.6.6 Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

III.1.8.6.7 Suportar autenticação via AD/LDAP, certificado e base de usuários local;

III.1.8.6.8 Suportar leitura e verificação de CRL (certificate revocation list);

III.1.8.6.9A tecnologia de VPN Client to Server deverá ser instalada na plataforma: iOS 10 ou superior e Android;

III.1.8.6.10 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8 e MacOS X;

III.1.9 Solução Para Proteção Contra Ameaças Avançadas – ZERO DAY

III.1.9.1 A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

III.1.9.2 A solução deverá ser composta por hardware e software específicos (appliance) com sistema operacional especializado em sua versão mais atualizada ou nuvem do próprio fabricante que possui o conceito de sandboxing para prevenção de ataques zero-day.

III.1.9.3 Não será aceito soluções que dependa da estrutura de hypervisor do contratante para a análise de ameaças de dia zero, como Vmware ESXi, Microsoft HyperV, entre outros;

III.1.9.4 A solução deverá operar em modo MTA (Mail Transfer Agent) para proteção de malware desconhecido de dia zero.

III.1.9.5 Caso a solução atue em modo MTA, será permitido composição com soluções de mercado, nao sendo elas soluções abertas “Software Livre”.

III.1.9.6 Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS), FTP e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

III.1.9.7 A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

III.1.9.8 Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL´s conhecidas;

III.1.9.9 A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP, Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

III.1.9.10 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 antes de entregar este arquivo para o cliente;

III.1.9.11 O conteúdo enviado para a solução de Sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado;

III.1.9.12 Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

III.1.9.13 Toda análise dos arquivos deverá ser realizada em ambiente controlado Sandboxing em nuvem. Não serão aceitas soluções em servidores ou software livre;

III.1.9.14 A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

III.1.9.15 Implementar detecção e bloqueio imediato de malwares que utilizam mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF acima de 10 Mb;

III.1.9.16 Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL;

III.1.9.17 Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos java (.jar e class);

III.1.9.18 A solução deve suportar inspeção para o protocolo SMBv3;

III.1.9.19 O relatório das emulações deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

III.1.9.20 A solução deve possuir engine de inspeção a nível de CPU para detectar técnicas ROP (Return Of Operation) além de outras técnicas de exploração de vulnerabilidade monitorando o fluxo de CPU;

III.1.9.21 Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

III.1.9.22 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

III.1.9.23 Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm e gz;

III.1.9.24 Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato, não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

III.1.9.25 Possibilitar remoção de conteúdo ativo dinamicos como macros, URL's, Java scripts e outros dos arquivos baixados, permitindo o download do arquivo original caso ele não seja malicioso;

III.1.9.26 A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

III.1.9.27 Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

III.1.9.27.1 Número de arquivos emulados;

III.1.9.27.2 Número de arquivos com malware.

III.1.9.28 A solução de prevenção de ameaças avançada, deve possuir capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detecada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

III.1.9.29 A solução deve prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

III.1.9.29.1O tamanho máximo do arquivo emulado seja excedido;

III.1.9.29.2O tempo máximo de emulação seja excedido.

III.1.10 Módulo de Gerência

III.1.10.1 A solução de gerência deverá ser separada dos gateways de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste documento;

III.1.10.2 Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada;

III.1.10.3 Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

III.1.10.4 Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede do mesmo fabricante desde que não sejam software livre;

III.1.10.5 O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;

III.1.10.6 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

III.1.10.7 Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

III.1.10.8 O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

III.1.10.9 Todos os logs da solução devem ser indexados e seu licenciamento deve ser o de maior capacidade.

III.1.10.10 O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;

III.1.10.11 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

III.1.10.12 Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

III.1.10.13 Suportar backup das configurações e rollback de configuração para a última configuração salva;

III.1.10.14 Suportar validação de regras antes da aplicação;

III.1.10.15 Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

III.1.10.16 Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;

III.1.10.17 Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

III.1.10.18 Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

III.1.10.19 Permitir a criação de certificados digitais para autenticação de usuários;

III.1.10.20 O relatório deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos GW's de segurança, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware e Sandboxing);

III.1.10.21 A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

III.1.10.22 A solução deve possuir logs, correlação de eventos e relatórios de auditoria dos administradores da solução;

III.1.10.23 Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados;

III.1.10.24 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;

III.1.10.25 Deve ser possível exportar os logs em CSV ou TXT;

III.1.10.26 Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

III.1.10.27 A solução deve ser capaz de segmentar a base de regras em uma estrutura em camadas;

III.1.10.28 A solução deve ser capaz de aplicar proteções relacionadas a ameaças e regras de acesso separadamente;

III.1.10.29 A solução deve combinar configuração de políticas e análise de logs em um único painel, para evitar erros alcançando maior confiabilidade na alteração de políticas;

III.1.10.30 O visualizador de log deve ter um recurso de pesquisa de texto livre;

III.1.10.31 Possibilitar rotação do log;

III.1.10.32 Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

III.1.10.32.1 Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e 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;

III.1.10.33 Deve permitir a criação de relatórios personalizados;

III.1.10.34 O gerenciamento centralizado deverá ser entregue como appliance virtual e dever ser compatível/homologado com/para VMWare ESX (vSphere 5.1, 5.5 ou 6;

III.1.10.35 A solução de gerenciamento deve possui a capacidade de gerenciar outros Firewalls de segurança do mesmo fabricante mesmo estão em ambientes virtualizados e nuvens públicas (AWS e Azure) e nuvens privadas (VmWare NSX ou Cisco ACI);

III.1.10.36 Possuir capacidade de integração com soluções de terceiros via API e também suportar configuração através de RestAPI.

III.1.10.37 Deve consolidar logs e relatórios de todos os dispositivos administrados;

III.1.10.38 Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

III.1.10.39 Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

III.1.10.40 Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

III.1.10.41 A gerência centralizada deve possuir módulo de solução para validação de conformidade de acordo com normas de mercado conforme exemplo.

III.1.10.41.1 ISO 27001 e ISO 27002;

III.1.10.41.2 PCI-DSS;

III.1.10.41.3 NIST 800-41

III.1.10.41.4 GDPR (base da norma LGPD);

III.1.10.42 Caso a solução não possua tal módulo, será permitido composição com soluções de mercado, não sendo elas soluções abertas “Software Livre”.

III.1.10.43 Simular o impacto de segurança das alterações de configuração antes da instalação de acordo com a aderência aos padrões regulatórios apresentados no item anterior;

III.1.10.44 Permitir a customização do padrão regulatório da própria instituição;

III.1.10.45 Permitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança;

III.1.10.46 Monitorar constantemente o status de conformidade da solução aos padrões regulatórios informados;

III.1.10.47 Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados à gestão de conformidade manual;

III.1.10.48 Gerar alertas de conformidade notificando os usuários sobre o impacto de suas decisões de segurança trazendo as considerações regulatórias na gestão de segurança;

III.1.10.49 Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação;

III.1.10.50 Possuir alertas de políticas e as potenciais violações de conformidade;

III.1.10.51 Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança;

III.1.10.52 Gerar relatórios regulamentares com base nas configurações de segurança em tempo real;

III.1.10.53 Permitir que os relatórios possam ser salvos, enviados e impressos;

III.1.10.54 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, nome do ataque, o país de origem e destino, etc;

III.1.10.55 A solução deve prover, no mínimo, as seguintes funcionalidade para análise avançada dos incidentes:

III.1.10.55.1 Visualizar quantidade de tráfego utilizado de aplicações e navegação;

III.1.10.55.2 Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

III.1.10.56 A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

III.1.10.57 A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credenciais;

III.1.10.58 Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

III.1.10.59 Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;

III.1.10.60 Criar certificados digitais para acesso dos usuários VPN;

III.1.10.61 Criar certificados digitais para VPNs Site-to-Site;

III.1.10.62 Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada;

III.1.10.63 Permitir criações de políticas de acesso de usuários autenticar no Active Directory, de forma que reconheça os usuários de forma transparente;

III.1.10.64 Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição.

III.1.10.65 A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma única tela, como por exemplo pesquisar logs de Antivírus e navegação web simultaneamente na mesma query de pesquisa.

III.1.10.66 O relatório das emulações (sandboxing) deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

III.1.10.67 A plataforma de gerência centralizada e monitoração deve possibilitar a procura por IPs e redes, sendo que os resultados mostram estes Pps e redes nos campos de origem e destino do logs na mesma tela de pesquisa.

III.1.10.68 Possuir mecanismo para que logs antigos sejam removidos automaticamente;

III.1.10.69 Possuir a capacidade de personalização de gráficos como barra, linha e tabela;

III.1.10.70 Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

III.1.10.71 Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

III.1.10.72 A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

III.1.10.73 A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

III.1.10.74 A solução deve ser capaz de personalizar e criar regras de correlação;

III.1.10.75 A solução deve fornecer uma interface gráfica para criação das regras citadas no item anterior;

III.1.10.76 A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

III.2 ITEM 2- LICENÇAS do Firewall Principal

Quantidade: 2 (dois)

III.2.1 Licenças para Firewalls modelo 9.800:

III.2.1.1 FIREWALL

III.2.1.2 IPSEC VPN,

III.2.1.3 IPS

III.2.1.4 Application Control,

III.2.1.5 URL Filtering,

III.2.1.6 Content Awareness,

III.2.1.7 Anti-Virus

III.2.1.8 Anti-Bot

III.2.1.9 Mobile Acess

III.3. ITEM 3 - EQUIPAMENTO Firewall Secundário

Quantidade: 10 (dez)

III.3.1 Características Gerais

III.3.1.1 A solução deverá ser composta de hardware e software licenciado, do mesmo fabricante;

III.3.1.2 A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

III.3.1.3 Na data da proposta, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale;

III.3.1.4 Todos os componentes devem ser próprios para montagem em rack “19” e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário;

III.3.1.5 Os gateways de segurança, bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3;

III.3.1.6 Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

III.3.2 Capacidade e Quantidades

III.3.2.1 Solução em Appliance de Segurança de Perímetro da Próxima Geração

III.3.2.1.1 Throughput de, no mínimo, 340 Mbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, Anti-Bot e prevenção de ameaças avançadas de dia zero;

III.3.2.1.2 Suporte a, no mínimo, 1.000.000 de conexões simultâneas;

III.3.2.1.3 Suporte a, no mínimo, 10.000 novas conexões por segundo;

III.3.2.1.4 Throughput de, no mínimo, 970 Mbps, no mínimo, para conexões VPN;

III.3.2.1.5 Deve suportar a performance considerando as funcionalidades de Next Generation firewall de 600 Mbps;

III.3.2.1.6 Througupt de no mínimo, 670 Mbps de IPS;

III.3.2.1.7 No mínimo, 6 interfaces de rede 10/100/1000 base-T;

III.3.2.1.8 Possuir 1 (uma) interface do tipo console ou similar;

III.3.2.1.9 Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP v4 e v6 sem duplicação da base de objetos e regras;

III.3.2.1.10 Deve suportar operar em cluster ativo-passivo ou ativo-ativo sem a necessidade de licenças adicionais;

III.3.2.1.11 O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

III.3.2.1.12 Os valores de capacidade são considerados para cada equipamento, não sendo permitido a soma dos valores dos membros do cluster;

III.3.2.1.13 Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização;

III.3.3 Funcionalidade de Firewall

III.3.3.1 A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

III.3.3.2 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;

III.3.3.3 O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

III.3.3.4 A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

III.3.3.5 Realizar upgrade via SCP, SFTP e https via interface WEB

III.3.3.6 Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

III.3.3.6.1 Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server;

III.3.3.7 Deve suportar os seguintes tipos de NAT:

III.3.3.7.1 Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

III.3.3.8 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

III.3.3.9 Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizavéis de forma dinâmica, por exemplo: Office 365, AWS, Azure e outros. Objetos dinâmicos que não se caracterizam como FQDN.

III.3.3.10 Enviar logs para sistemas de monitoração externos, simultaneamente;

III.3.3.11 Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

III.3.3.12 Deve realizar roteamentos unicast e multicast simultaneamente em uma única instância(contexto) de firewall.

III.3.3.13 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

III.3.3.14 Autenticação integrada via Kerberos.

III.3.3.15 Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;

III.3.3.16 A solução deve ter a capacidade de operar através de uma unica instancia de Firewall de forma simultânea mediante o uso das suas interfaces fisicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o trafego de rede), camada 2 (L2) e camada 3 (L3);

III.3.3.17 A solução deve permitir salvar as configurações das politicas para serem aplicadas em horarios pré-definidos;

III.3.3.18 Deve possuir mecanismo de ativação de validada da regra com período customizado;

III.3.3.19 Deverá suportar redundância e balancemento de links, tendo capacidade a no minimo 3 links de internet.

III.3.3.20 Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento.

III.3.3.21 Deve permitir a configuração do tempo de checagem para cada um dos links.

III.3.4 Funcionalidade de Filtro de Conteúdo WEB

III.3.4.1 Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

III.3.4.2 Controle de políticas por usuários, grupos de usuários, IPs e redes;

III.3.4.3 Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3

III.3.4.4 Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

III.3.4.5 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

III.3.4.5.1 Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

III.3.4.5.2 Reconhecer pelo menos 6.000 (seis mil) aplicações diferentes, incluindo, mas não limitado: a 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;

III.3.4.6 A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

III.3.4.7 Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE)**.**

III.3.4.8 Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

III.3.4.9 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

III.3.4.10 A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 150 categorias de aplicações WEB pré-definidas pelo fabricante;

III.3.4.11 Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer.);

III.3.4.12 Possui mecanismo de controle de aplicação web e URL que possui configuração de bloqueio e liberação da aplicação principal e/ou as suas subcategorias. Quando o administrador da solução desejar bloquear apenas as subcategorias do facebook, como facebook, chat, video, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser bloqueada toda a categoria como “Facebook” ou "Redes sociais" que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter , YouTube, etc. A solução precisa ser baseada em bloqueio de aplicações WEB que a própria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote.

III.3.4.13 A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

III.3.4.14 Atualizar a base de assinaturas de aplicações automaticamente;

III.3.4.15 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

III.3.4.16 Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas entre elas usuários, IP, grupos de usuários do sistema do Active Directory;

III.3.4.17 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

III.3.4.18 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 órgão;

III.3.4.19 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

III.3.4.20 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

III.3.4.20.1 Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

III.3.4.20.2 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

III.3.4.20.3 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 Active Directory e base de dados local;

III.3.4.20.4 Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

III.3.4.20.5 Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;

III.3.4.20.6 Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;

III.3.4.20.7 Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

III.3.4.20.8 Suportar a criação de categorias de URLs customizadas;

III.3.4.20.9 Suportar a exclusão de URLs do bloqueio, por categoria;

III.3.4.20.10 Permitir a customização de página de bloqueio;

III.3.4.21 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, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

III.3.4.22 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API's ou Syslog, para a identificação de endereços IP e usuários;

III.3.4.23 Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

III.3.5 FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

III.3.5.1 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 equipamento de firewall;

III.3.5.2 Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

III.3.5.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/passivo;

III.3.5.4 Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

III.3.5.5 A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

III.3.5.6 Deverá possuir os seguintes mecanismos de inspeção de IPS:

III.3.5.6.1 Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

III.3.5.7 Detectar e bloquear a origem de portscans;

III.3.5.8 Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

III.3.5.9 Possuir assinaturas para bloqueio de ataques de buffer overflow;

III.3.5.10 Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

III.3.5.11 Suportar bloqueio de arquivos por tipo;

III.3.5.12 Identificar e bloquear comunicação com botnets;

III.3.5.13 Deve suportar referência cruzada com CVE;

III.3.5.14 Em cada proteção de segurança, deve estar incluso informações como:

III.3.5.14.1Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro codigo de referência;

III.3.5.14.2 Severidade;

III.3.5.14.3 Tipo de ação a ser executada.

III.3.5.15 O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

III.3.5.16 O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

III.3.5.17 O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.

III.3.5.18 O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)**.**

III.3.5.19 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

III.3.5.19.1 O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

III.3.5.20 Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual;

III.3.5.21 A solução de IPS, deve possuir mecanismo de analise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção devem ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.

III.3.5.22 O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

III.3.5.23 A solução deverá possuir pelo menos dois perfis pré configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

III.3.5.24 A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.

III.3.5.25 Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

III.3.5.26 Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados;

III.3.5.27 O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;

III.3.5.28 A solução de IPS deve possuir engine onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;

III.3.5.29 O antivírus deve oferecer suporte à verificação de links dentro de emails.

III.3.5.30 A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso

III.3.5.31 A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;

III.3.5.32 Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;

III.3.5.33 A solução deve permitir a criação de White list baseado no MD5 do arquivo;

III.3.5.34 Os eventos devem identificar o país de onde partiu a ameaça;

III.3.5.35 Suportar rastreamento de vírus em arquivos pdf;

III.3.5.36 Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

III.3.5.37 Possuir a capacidade de prevenção de ameaças não conhecidas;

III.3.5.38 Em caso de falha no mecanismo de inspeção do Anti-Vírus, deve ser possível configurar se as conexões serão permitidas ou bloqueada

III.3.5.39 A solução de Anti-virus e Anti-Malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

III.3.5.40 A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;

III.3.5.41 Suportar a criação de políticas por Geolocalização, permitindo que o tráfego de determinado País/Países seja bloqueado;

III.3.5.42 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

III.3.5.43 Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

III.3.5.44 A solução de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

III.3.5.45 A solução deve possuir funcionalidade de identificação de bloqueio de trafego malicioso comunicando com C&C (command & Control);

III.3.5.46 A solução Antivírus deverá suportar a análise de links no corpo de emails.

III.3.6 Funcionalidades de Controle de Qualidade de Serviço

III.3.6.1 Suportar a criação de políticas de QoS por:

III.3.6.1.1 Endereço de origem, endereço de destino e por porta;

I**II.3.6.2** O QoS deve possibilitar a definição de classes por:

III.3.6.2.1 Banda garantida, banda máxima e fila de prioridade;

III.3.6.2.2 Disponibilizar estatísticas em tempo real para classes de QoS;

III.3.7 Funcionalidades de VPN

III.3.7.1 Suportar VPN Site-to-Site e Cliente-To-Site;

III.3.7.2 Suportar IPSec VPN;

III.3.7.3 A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);

III.3.7.4 Suportar SSL VPN;

III.3.7.5 A VPN IPSEc deve suportar:

III.3.7.5.1 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard), SHA-512 e Autenticação via certificado IKE PKI;

III.3.7.5.2 A solução deve possuir checagem de conformidade e verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus, firewall no host, chaves de registros e processos ativos;

III.3.7.5.3 A solução deve permitir bloquear o acesso dos usuários aos recursos via VPN caso o usuário não esteja em conformidade com a verificação dos parâmetros configurados.

III.3.8 Solução para Proteção contra Ameaças Avançadas – ZERO DAY

III.3.8.1 A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

III.3.8.2 A solução deverá ser composta por hardware e software específicos (appliance) com sistema operacional especializado em sua versão mais atualizada ou nuvem do próprio fabricante que possui o conceito de sandboxing para prevenção de ataques zero-day.

III.3.8.3 Não será aceito soluções que dependa da estrutura de hypervisor do contratante para a análise de ameaças de dia zero, como Vmware ESXi, Microsoft HyperV, entre outros;

III.3.8.4 Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e FTP via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

III.3.8.5 A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

III.3.8.6 Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL´s conhecidas;

III.3.8.7 A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP, Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

III.3.8.8 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 antes de entregar este arquivo para o cliente;

III.3.8.9 O conteúdo enviado para a solução de Sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado;

III.3.8.10 Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

III.3.8.11 Toda análise dos arquivos deverá ser realizada em ambiente controlado Sandboxing em nuvem. Não serão aceitas soluções em servidores ou software livre;

III.3.8.12 A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

III.3.8.13 Implementar detecção e bloqueio imediato de malwares que utilizam mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF acima de 10 Mb;

III.3.8.14 Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL;

III.3.8.15 Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos java (.jar e class);

III.3.8.16 A solução deve suportar inspeção para o protocolo SMBv3;

III.3.8.17 O relatório das emulações deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

III.3.8.18 A solução deve possuir engine de inspeção a nível de CPU para detectar técnicas ROP (Return Of Operation) além de outras técnicas de exploração de vulnerabilidade monitorando o fluxo de CPU;

III.3.8.19 Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

III.3.8.20 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, sub rede e endereço IP;

III.3.8.21 Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm e gz;

III.3.8.22 Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato, não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

III.3.8.23 Possibilitar remoção de conteúdo ativo dinâmicos como macros, URL's, Java scripts e outros dos arquivos baixados, permitindo o download do arquivo original caso ele não seja malicioso;

III.3.8.24 A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

III.3.8.25 Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

III.3.8.25.1 Número de arquivos emulados;

III.3.8.25.2 Número de arquivos com malware.

III.3.8.26 A solução de prevenção de ameaças avançada, deve possuir capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

III.3.8.27 A solução deve prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

III.3.8.27.1 O tamanho máximo do arquivo emulado seja excedido;

III.3.8.27.2 O tempo máximo de emulação seja excedido.

III.3.9 Módulo de Gerência

III.3.9.1 A solução de gerência deverá ser separada dos gateways de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste documento;

III.3.9.2 Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada;

III.3.9.3 Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

III.3.9.4 Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede do mesmo fabricante desde que não sejam software livre;

III.3.9.5 O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;

III.3.9.6 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

III.3.9.7 Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

III.3.9.8 O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

III.3.9.9 Todos os logs da solução devem ser indexados e seu licenciamento deve ser o de maior capacidade.

III.3.9.10 O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;

III.3.9.11 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

III.3.9.12 Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

III.3.9.13 Suportar backup das configurações e rollback de configuração para a última configuração salva;

III.3.9.14 Suportar validação de regras antes da aplicação;

III.3.9.15 Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

III.3.9.16 Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;

III.3.9.17 Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

III.3.9.18 Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

III.3.9.19 Permitir a criação de certificados digitais para autenticação de usuários;

III.3.9.20 O relatório deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos GW's de segurança, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware e Sandboxing);

III.3.9.21 A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

III.3.9.22 A solução deve possuir logs, correlação de eventos e relatórios de auditoria dos administradores da solução;

III.3.9.23 Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados;

III.3.9.24 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;

III.3.9.25 Deve ser possível exportar os logs em CSV ou TXT;

III.3.9.26 Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

III.3.9.27 A solução deve ser capaz de segmentar a base de regras em uma estrutura em camadas;

III.3.9.28 A solução deve ser capaz de aplicar proteções relacionadas a ameaças e regras de acesso separadamente;

III.3.9.29 A solução deve combinar configuração de políticas e análise de logs em um único painel, para evitar erros alcançando maior confiabilidade na alteração de politicas;

III.3.9.30 O visualizador de log deve ter um recurso de pesquisa de texto livre;

III.3.9.31 Possibilitar rotação do log;

III.3.9.32 Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

III.3.9.32.1 Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego;

III.3.9.33 Deve permitir a criação de relatórios personalizados;

III.3.9.34 O gerenciamento centralizado deverá ser entregue como appliance virtual e dever ser compatível/homologado com/para VMWare ESX (vSphere 5.1, 5.5 ou 6;

III.3.9.35 A solução de gerenciamento deve possui a capacidade de gerenciar outros Firewalls de segurança do mesmo fabricante mesmo estão em ambientes virtualizados e nuvens públicas (AWS e Azure) e nuvens privadas (VmWare NSX

ou Cisco ACI);

III.3.9.36 Possiu capacidade de integração com soluções de terceiros via API e também suportar configuração através de RestAPI.

III.3.9.37 Deve consolidar logs e relatórios de todos os dispositivos administrados;

III.3.9.38 Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

III.3.9.39 Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

III.3.9.40 Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

III.3.9.41 Permitir que os relatórios possam ser salvos, enviados e impressos;

III.3.9.42 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, nome do ataque, o país de origem e destino, etc;

III.3.9.43 A solução deve prover, no mínimo, as seguintes funcionalidade para análise avançada dos incidentes:

III.3.9.43.1 Visualizar quantidade de tráfego utilizado de aplicações e navegação;

III.3.9.43.2 Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

III.3.9.44 A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

III.3.9.45 A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credenciais;

III.3.9.46 Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

III.3.9.47 Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;

III.3.9.48 Criar certificados digitais para acesso dos usuários VPN;

III.3.9.49 Criar certificados digitais para VPNs Site-to-Site;

III.3.9.50 Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada;

III.3.9.51 Permitir criações de políticas de acesso de usuários autenticar no Active Directory, de forma que reconheça os usuários de forma transparente;

III.3.9.52 Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição.

III.3.9.53 A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma única tela, como por exemplo pesquisar logs de Antivírus e navegação web simultaneamente na mesma query de pesquisa.

III.3.9.54 O relatório das emulações (sandboxing) deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

III.3.9.55 A plataforma de gerência centralizada e monitoração deve possibilitar a procura por IPs e redes, sendo que os resultados mostram estes Pps e redes nos campos de origem e destino do logs na mesma tela de pesquisa.

III.3.9.56 Possuir mecanismo para que logs antigos sejam removidos automaticamente;

III.3.9.57 Possuir a capacidade de personalização de gráficos como barra, linha e tabela;

III.3.9.58 Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

III.3.9.59 Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

III.3.9.60 A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

III.3.9.61 A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

III.3.9.62 A solução deve ser capaz de personalizar e criar regras de correlação;

III.3.9.63 A solução deve fornecer uma interface gráfica para criação das regras citadas no item anterior;

III.3.9.64 A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

III.4. - ITEM 4- Licenças Firewall Secundário

Quantidade: 10 (dez)

III.4.1 Licenças para Firewalls modelo 1535:

III.4.1.1 FIREWALL

III.4.1.2 IPSEC VPN,

III.4.1.3 IPS

III.4.1.4 Application Control,

III.4.1.5 URL Filtering,

III.4.1.6 Content Awareness,

III.4.1.7 Anti-Virus

III.4.1.8 Anti-Bot

III.5. ITEM 5- Instalação e Configuração

III.5.1 Trata-se de serviço de instalação e configuração dos Firewalls principais e transceivers e secundários e suas licenças.

III.5.1.1 Para os 2 (dois) equipamentos Firewalls Principais instalados no Prédio Sede da Av. Presidente Wilson;

III.5.1.1.1 Instalação dos transceivers

III.5.1.2 Para todas as licenças dos 2 (dois) equipamentos Firewalls Principais.

III.5.1.3 Para 10 (dez) Firewalls secundários que serão utilizados em eventos ou emergencialmente nas unidades judiciárias do TRE-RJ.

III.5.1.4 Para todas as licenças dos 10 (dez) Firewalls secundários

III.5.1.5 Para as Licenças para Acesso Remoto (Mobile Access Blade Unlimited), que serão instaladas em 2 (dois) equipamentos Firewalls Principais na sede da Av. Presidente Wilson.

III.6. ITEM 6- Suporte técnico de toda a solução.

III.6.1 Trata-se de serviço de suporte técnico e garantia dos Firewalls Principais e Secundários, às licenças, os transceivers e os serviços desta aquisição:

III.6.1.1 Para os 2 (dois) equipamentos Firewalls Principais instalados no Prédio Sede da Av. Presidente Wilson;

III.6.1.2 Para todas as licenças dos 2 (dois) equipamentos Firewalls Principais.

III.6.1.3. Para 10 (dez) Firewalls secundários que serão utilizados em eventos ou emergencialmente nas unidades judiciárias do TRE-RJ.

III.6.1.4 Para todas as licenças dos 10 (dez) Firewalls secundários

III.6.1.5 Para as Licenças para Acesso Remoto (Mobile Access Blade Unlimited), que serão instaladas em 2 (dois) equipamentos Firewalls Principais na sede da Av. Presidente Wilson.

III.6.2 A empresa contratada deverá fornecer garantia para todos os itens fornecidos por um período mínimo de 36 (trinta e seis) meses, contados a partir da data do recebimento definitivo;

III.6.2.1 A garantia deverá atender a todos os componentes físicos (hardware) e lógicos (software) que fazem parte do objeto deste Termo de Referência;

III..6.2.2 Deverão estar cobertas pela garantia quaisquer atualizações de firmware e software disponibilizadas pelo fabricante.

III.6.2.3 A CONTRATADA deve providenciar a garantia dos equipamentos entregues junto ao fabricante dos mesmos;

III.6.2.4 O Termo de Recebimento Definitivo só será emitido após a comprovação, por parte da CONTRATADA, de que providenciou a garantia junto ao fabricante dos equipamentos;

III.6.3 Deve ser possível aos técnicos do TRE-RJ acessar, via internet, a base de conhecimentos do fabricante dos equipamentos;

III.6.4 A contratada deve possuir Central de Atendimento tipo 0800, ou telefone local, para abertura dos chamados de garantia e suporte, comprometendo-se a manter registros dos mesmos;

III.6.4.1 O período de disponibilidade para chamada de manutenção deverá ser de 24 (vinte e quatro) horas por dia, durante os 07 (sete) dias da semana;

III.6.5 Os chamados, no momento de sua abertura, serão identificados pela seguinte nomenclatura (ou equivalente), que estabelecerá seu grau de prioridade e os padrões exigidos para seu atendimento:

III.6.5.1 Chamados com prioridade “0” (solução inoperante):

III.6.5.1.1 São chamados para manutenção corretiva e reparação de eventuais falhas dos equipamentos, componentes ou periféricos que se encontram inoperantes ou com grave comprometimento de seu funcionamento;

III.6.5.1.2 O término do atendimento técnico não poderá ultrapassar o prazo de 4 (quatro) horas, contadas a partir da abertura do chamado;

III.6.5.1.3 Entende-se por término do atendimento técnico a hora em que a solução estiver novamente operacional e em perfeitas condições de funcionamento no local onde estiver instalada, estando condicionado à aprovação do TRE-RJ;

III.6.5.2 Chamados com prioridade “1” (solução com problema):

III.6.5.2.1 São chamados para correção de eventuais problemas dos equipamentos, componentes ou periféricos que não se encontrem inoperantes, mas que apresentem algum comprometimento de seu funcionamento, mediante a prestação de suporte telefônico ou, se necessário, atendimento “on site”;

III.6.5.2.2 O término do atendimento não poderá ultrapassar o prazo de 24 (vinte e quatro) horas, contadas a partir da abertura do chamado;

III.6.5.2.3 Entende-se por término do atendimento técnico a hora em que a solução for disponibilizada para uso em perfeitas condições de funcionamento, estando condicionado à aprovação do TRE-RJ;

III.6.6 Os serviços de reparo dos equipamentos defeituosos serão executados onde estes se encontrem (on site), salvo em caso de impossibilidade técnica devidamente justificada pela empresa contratada;

III.6.6.1 No caso de ser necessária a retirada do equipamento defeituoso das dependências do TRE-RJ, a empresa contratada deverá relatar por escrito a situação ao fiscal do contrato, que autorizará por escrito a saída do referido equipamento, após constatar tal necessidade;

III.6.6.1.1 A empresa contratada deverá providenciar imediatamente o empréstimo de um equipamento em perfeito estado de funcionamento e com características técnicas idênticas ou superiores às do equipamento retirado;

III.6.6.1.2 O equipamento colocado em substituição ficará instalado nas dependências do TRE-RJ até a devolução do equipamento consertado, que não poderá ultrapassar o prazo de 60 (sessenta) dias corridos;

III.6.7 A empresa contratada deverá enviar ao fiscal do contrato, no TRE-RJ, até o terceiro dia útil de cada mês, documento em que conste a identificação dos chamados, data e hora de início e término dos atendimentos, descrição dos serviços executados e indicação das peças ou componentes eventualmente substituídos no mês anterior;

III.6.8 Durante o prazo de garantia a substituição de qualquer parte ou peça defeituosa dos equipamentos deverá ocorrer sem ônus para o TRE-RJ;

III.6.8.1 No caso de troca de equipamento e/ou perda de configuração, a empresa contratada será responsável por prestar o auxílio necessário ao técnico ou analista do TRE-RJ, independentemente de onde o equipamento estiver;

III.6.9 Todos os custos relativos ao deslocamento de técnicos, eventual transporte de componentes e equipamentos, dentre outros, correrão exclusivamente por conta da empresa.

III.6.10 Os serviços de suporte e garantia poderão ser prestados diretamente pelo fabricante dos itens fornecidos, desde que atendam a todas as exigências especificadas nos itens anteriores;

III.6.10.1 Caso o suporte ou a garantia sejam fornecidos pelos próprios fabricantes, a empresa contratada deverá fornecer todas as informações necessárias para abertura de chamados, como números telefônicos, nomes, e-mails e quaisquer outras informações relevantes.

III.6.11 A empresa contratada deverá substituir qualquer equipamento por outro novo e de primeiro uso, com padrão de qualidade e desempenho igual ou superior ao equipamento original, sempre que forem abertos 03 (três) ou mais chamados com prioridade “0” para o mesmo equipamento no prazo de 30 (trinta) dias corridos;

III.6.11.1 A substituição de que trata o item anterior será em caráter definitivo, devendo ser providenciada em até 30 (trinta) dias corridos após a empresa contratada ter sido notificada pelo TRE-RJ.

III.6.12 A contratada deverá substituir os firewalls, a qualquer tempo e às suas expensas, no prazo de 7 dias corridos após notificada, quando o equipamento apresentar irregularidade, defeito ou problema que impossibilite o seu uso na infraestrutura do TRE-RJ;

III.6.13 A contratada deverá atualizar qualquer atualização de firmware ou release dos Firewalls, durante o período de garantia no prazo de 7 dias corridos após notificada.

III.7. ITEM 7 - TREINAMENTO

III.7.1 Objetivo do Curso

Capacitar os participantes com conhecimentos fundamentais para a configuração, administração e uso da ferramenta de gerenciamento do Firewall Check Point. O curso é voltado para profissionais de TI que desejam iniciar ou aprimorar suas habilidades na administração de firewalls, com foco específico no Check Point.

Carga Horária: 40 horas

III.7.1.1 Módulo 1: Introdução ao Firewall Check Point

- Conceitos básicos de segurança de rede e firewall

- Visão geral da arquitetura Check Point

- Principais componentes do Check Point Security Management

- Licenciamento e versões disponíveis

III.7.1.2 Módulo 2: Instalação e Configuração Inicial

III.7.1.2.1 - Requisitos de sistema e planejamento de instalação

III.7.1.2.2- Instalação do Security Gateway e Security Management Server

III.7.1.2.3 - Configuração inicial do Security Gateway

III.7.1.2.4 - Configuração da comunicação entre Security Gateway e Management Server

III.7.1.3 Módulo 3: Políticas de Segurança

III.7.1.3.1 - Introdução às políticas de segurança

III.7.1.3.2- Criação e gerenciamento de regras de firewall

III.7.1.3.3- Tipos de objetos: Hosts, Networks, Serviços, etc.

III.7.1.3.4 - Verificação de políticas e troubleshoot básico

III.7.1.4 Módulo 4: NAT e VPN

III7.1.4.1- Configuração de NAT (Network Address Translation)

III.7.1.4.2 - Tipos de NAT: Source NAT e Destination NAT

III.7.1.4.3- Configuração básica de VPN Site-to-Site

III.7.1.4 .4 - Monitoramento e troubleshooting de VPN

III.7.1.5 Módulo 5: Gerenciamento de Logs e Relatórios

III.7.1.5.1- Configuração de logs e auditoria

III.7.1.5.2- Análise de logs e eventos

III.7.1.5.3 - Criação de relatórios personalizados

III.7.1.5.4 - Troubleshooting baseado em logs

III.7.1.6 Módulo 6: Ferramentas de Administração

III.7.1.6.1 - Introdução à ferramenta SmartConsole

III.7.1.6.2 - Navegação e principais funções da SmartDashboard

III.7.1.6.3 - Uso do SmartView Tracker para monitoramento

III.7.1.6.4 - Introdução ao SmartEvent para gerenciamento de eventos de segurança

III.7.1.7 -Módulo 7: Manutenção e Atualizações

III.7.1.7.1 - Backup e recuperação de configurações

III.7.1.7.2 - Procedimentos de atualização de software e patching

III.7.1.7.3 - Melhores práticas para manutenção e gerenciamento de patches

III.7.1.7.4 - Monitoramento de desempenho do firewall

III.7.1.8 -Módulo 8: Segurança Avançada e Práticas Recomendadas

III.7.1.8.1 - Introdução ao IPS (Intrusion Prevention System)

III.7.1.8.2 - Configuração básica de inspeções de tráfego

III.7.1.8.3 - Práticas recomendadas para políticas de segurança

III.7.1.8.4 - Estudos de caso e aplicação prática

III.7.2 O treinamento deverá ser oferecido com uma carga horária mínima que abranja todos os tópicos descritos para os subitens **III.7.1** e que não seja inferior a 40 (quarenta) horas, ressalvada que a carga horária diária máxima deverá ser de 4(quatro) horas.

III.7.2.1.Ao final do treinamento, ou de cada uma das etapas, deverá ser fornecido certificado de conclusão, onde deverá constar, obrigatoriamente:

a) Nome do participante.

b) Título do treinamento.

c) Carga horária total.

d) Data de início do treinamento.

e) Data do fim do treinamento.

f) Conteúdo programático abordado.

g) Razão social e CNPJ da empresa responsável pelo treinamento.

III.7.2.2 O treinamento poderá ser realizado no formato de ensino à distância sendo de responsabilidade da CONTRATADA o provimento de todos os recursos técnicos para a realização do mesmo.

III.7.2.3 É obrigatório o fornecimento pela CONTRATADA de material escrito (manuais, apostilas, livros) ou eletrônico (arquivo digital).

III.7.2.4 É obrigatória a disponibilização de uma plataforma de treinamento independente para cada aluno;

III.7.2.5 A data de início da capacitação será definida pela CONTRATANTE de acordo com suas necessidades.

III.7.2.6 A CONTRATANTE irá comunicar por mensagem eletrônica à CONTRATADA, com antecedência mínima de 30(trinta) dias, a data proposta para o início do treinamento.

III.7.2.7 O profissional que ministrar o treinamento deverá ser certificado/autorizado pelo fabricante.

III.7.2.8 A CONTRATADA deverá apresentar em até 30 (trinta) dias, contados a partir do primeiro dia útil subsequente à data de assinatura do Contrato, documento (s) que comprove(m) a certificação e/ou autorização, pelo fabricante da solução, do profissional que ministrará o curso.

III.7.2.9 A ementa do curso, a carga horária, o conteúdo programático da capacitação e os materiais didáticos deverão ser entregues à CONTRATANTE em até 30 (trinta) dias contados a partir do primeiro dia útil subsequente da comunicação à CONTRATADA a data proposta para o início do treinamento.

III.7.2.10 Caso a ementa do curso, a carga horária, o conteúdo programático, os materiais didáticos ou os instrutores do treinamento, não sejam aprovados, ou exista alguma pendência nos certificados e autorizações exigidos, a CONTRATADA deverá providenciar os ajustes e correções solicitados pelo CONTRATANTE, sem que isto venha a justificar qualquer dilação nos prazos, aumento dos custos previstos e alteração dos compromissos assumidos junto ao CONTRATANTE.

III.7.2.11 A CONTRATANTE avaliará, para fins de recebimento, a qualidade da prestação do serviço de treinamento junto aos participantes, devendo a CONTRATADA providenciar os ajustes e correções necessários, hipótese na qual poderá ser solicitado a refazer o treinamento, caso o objetivo do mesmo não tenha sido alcançado.

III.7.2.12 Todas as despesas com material, equipamentos, licenças de softwares, instrutores, deslocamento de instrutores e demais itens relacionados à oferta do treinamento em si, serão de responsabilidade da CONTRATADA.

III.7.2.13 A abordagem do treinamento deve ser eminentemente prática (hands on), utilizando exemplos e exercícios para ilustrar os conceitos e capacitar os participantes a empregar os recursos oferecidos.

III.7.2.14 A conclusão da capacitação será reconhecida pela CONTRATANTE somente se a avaliação da mesma for considerada satisfatória, pelos participantes.

III.7.2.15 Ao final dos treinamentos os participantes efetuarão uma avaliação, utilizando o formulário padrão de avaliação de treinamentos da Coordenadoria de Educação e Desenvolvimento do TRE-RJ, cujo modelo encontra-se no **ANEXO I.2 (4026441)** ,deste Termo de Referência. Será considerado aprovado o treinamento que obtiver avaliação superior a 7,5 (sete vírgula cinco) pontos.

III.7.2.15.1 Caso o Treinamento não seja aprovado pelos participantes, a Contratada terá até 15 dias corridos para informar outro calendário do treinamento, em concordância com a Contratante.

III.7.2.16 Serão avaliados os itens "1 - Resultados obtidos", "2 - Objetivos, conteúdo e material didático" e "3 - Atuação do expositor" e seus respectivos subitens.

III.7.2.17 Cada item será avaliado com os conceitos E - Excelente (10 pontos), B - Bom (7,5 pontos), R - Regular (5,0 pontos) e D - Deficiente (2,5 pontos).

III.7.2.18 Todos os treinamentos deverão ocorrer no prazo máximo de 10 (dez) meses, contados a partir do primeiro dia útil seguinte à assinatura do Contrato.

III.8 - ITEM 8 - TRANSCEIVERS

Quantidade: 8 (oito)

III.7.1 Conector: **RJ45;**

III.7.2 Protocolo: **1000BASE -T;**

III.7.3 Tipo de cabo suportado: **CAT 5**

III.7.4 Form Factor: **SFP +**

IV - REQUISITOS DA CONTRATAÇÃO (Art. 6º, Inciso XXIII, Alínea “d”, da Lei 14.133/2021)

IV. 1 Conformidade Técnica e Legal

IV.1.1 Resolução Nº 468 de 15/07/2022, Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ).

IV.1.2 Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação eComunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

IV.1.3 Resolução CNJ nº 370/2021, institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

IV.1.4 Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

IV.1.5 Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

IV.1.6 Resolução TSE Nº 23.644, de 1º de julho de 2021, Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.

IV.2. Das Obrigações do Contratante e da Contratada

IV.2.1. Obrigações da Contratada

IV.2.1.1 A CONTRATADA deverá executar os serviços de acordo com as orientações e especificações constantes neste Termo de Referência, utilizando-se de todos os recursos materiais e humanos necessários

IV.2.1.2 Trocar, às suas expensas, o material que for recusado pelo TRE-RJ, observando-se que o recebimento não caracteriza a aceitação do mesmo, que somente ocorrerá após o recebimento definitivo.

IV.2.1.3 Substituir, reparar ou corrigir, às suas expensas, no prazo fixado no Termo de referência, o objeto fornecido com defeito, vícios ou incorreções.

IV.2.1.4 Informar no momento de envio da proposta, endereço eletrônico e contato telefônico para comunicação com o TRE/RJ, sendo de sua responsabilidade mantê-los atualizados durante toda a fase de execução da contratação.

IV.2.1.5 Manter, durante toda a execução do contrato, as condições de habilitação exigidas.

IV.2.1.6 Responder pelos danos causados diretamente à contratante ou aos seus bens, ou ainda a terceiros, decorrentes de sua culpa ou dolo na execução do contrato.

IV.2.1.7 Não transferir ou ceder a outrem, no todo ou em parte, o objeto do presente contrato.

IV.2.1.8 A contratada deverá treinar e orientar seus empregados sobre as disposições legais aplicáveis à proteção de dados pessoais, dando-lhes conhecimento formal das cláusulas, condições e obrigações relacionadas à Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais — LGPD, inclusive no tocante à Política Geral de Privacidade e Proteção de Dados Pessoais da Justiça Eleitoral, instituída pela Resolução TSE nº 23.650/2021.

IV.2.1.9 Para a formalização e execução do contrato, em atendimento ao disposto na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) e Resolução TSE nº 23.650/2021, a contratada autoriza à contratante o acesso aos dados pessoais/documentos de seus representantes tais como: número do CPF, endereço eletrônico e cópia do documento de identificação.

IV.2.1.10 Os dados pessoais dos representantes, prepostos e/ou colaboradores da contratada, obtidos em razão da execução contratual, poderão ser divulgados pela contratante, com a finalidade de cumprir mandamentos legais e jurisprudenciais relacionados à transparência.

IV.2.1.11 Sempre que solicitado pelo TRE-RJ, a contratada indicará representante para assuntos relacionados à LGPD, que poderá ser o mesmo colaborador qualificado como preposto para outros assuntos relacionados à execução do contrato, observada a necessária apresentação de termo de compromisso e responsabilidade pelo acesso aos dados.

IV.2.1.12 A contratada deverá prestar, no prazo fixado pela contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado, comprometendo-se, ainda, quando necessário e dentro das limitações pertinentes ao objeto do contrato, a auxiliar a contratante em relação à requisição dos titulares de dados pessoais, nos termos do art. 18 da LGPD.

IV.2.1.13 A contratada se declara ciente de que qualquer violação às disposições do LGPD é considerada uma violação do instrumento contratual pactuado pelas partes, sujeitando-se às penalidades cabíveis.

IV.2.1.14 Na hipótese de a contratação permitir a subcontratação, a contratada será responsável por assegurar que os subcontratados estejam vinculados por obrigações de confidencialidade, segurança e privacidade de dados, conforme estabelecido neste termo de referência.

IV.2.1.15 Comunicar ao Contratante, em até 24 horas, qualquer incidente de acesso não autorizado aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da LGPD.

IV.2.1.16 Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de que tomar conhecimento em razão da execução do contrato, respeitando todos os critérios de sigilo, segurança e inviolabilidade aplicáveis aos dados, informações, regras de negócio, documentos, entre outros.

IV.2.1.17 A CONTRATADA não deverá veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, do TRE-RJ.

IV.2.2. Obrigações da contratante

IV.2.2.1 Acompanhar e fiscalizar a execução do objeto, através de comissão/servidor especialmente designado.

IV.2.2.2 Receber provisória e definitivamente o objeto no prazo e condições estabelecidas neste Termo de Referência.

IV.2.2.3 Comunicar à contratada a ocorrência de quaisquer imperfeições verificadas no objeto fornecido, fixando prazo para que seja sanado o problema.

IV.2.2.4 Efetuar o pagamento à contratada, de acordo com as condições de preço e prazo estabelecidas neste Termo de Referência.

IV.2.2.5 A contratante tratará dados pessoais dos representantes, prepostos e/ou colaboradores da contratada para viabilizar o acesso às instalações físicas do Tribunal, a gestão contratual através de sistema de informação e o cumprimento do dever legal de fiscalização da execução do contrato.

IV.3 Das obrigações comuns às partes.

IV.3.1 As partes declaram que têm ciência da existência da Lei nº 13.709/2018 - Geral de Proteção de Dados Pessoais (LGPD) e Resolução TSE nº 23.650/2021 e se comprometem a adequar todos os procedimentos internos ao disposto na referida lei, com intuito de proteção dos dados pessoais repassados em virtude da execução contratual, sendo vedada a utilização de todo e qualquer dado pessoal repassado para finalidade distinta daquela contida no objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

IV.3.2 A contratante figura na qualidade de (controladora) de dados enquanto a contratada é definida como (operadora) de dados.

IV.3.3 A contratante e a contratada serão consideradas controladoras conjuntas quando eventualmente houver uma participação conjunta na determinação das finalidades e meios de tratamento dos dados pessoais.

IV.3.4 As partes comprometem-se a:

IV.3.4.1 Manter a integridade, o sigilo e a confidencialidade de todas as informações - em especial os dados pessoais e dados sensíveis - repassados em decorrência da execução contratual, em consonância com o disposto na Lei nº 13.709/2018 - Lei Geral de Proteção de Dados(LGPD) e Resolução TSE nº 23.650/2021, sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do Aviso de Dispensa Eletrônica/instrumento contratual;

IV.3.4.2 Manter registros precisos e atualizados das atividades de tratamento de dados pessoais, incluindo o acesso e a utilização dessas informações, para fins de auditoria e prestação de contas;

IV.3.4.3 Obter e apresentar à outra, sempre que necessário, e mediante solicitação prévia, os respectivos termos de ciência ou consentimento, quando for o caso, dos titulares para o tratamento dos dados pessoais dos quais forem controladoras, bem como os respectivos termos de compromisso e responsabilidade pelo acesso e tratamento de dados realizados por seus colaboradores, prepostos, prestadores de serviço, contratados terceirizados ou autônomos, sócios ou diretores a ela vinculados;

IV.3.4.4 Implementar todas as medidas técnicas e organizacionais cabíveis para prover um nível de segurança adequado frente aos riscos inerentes ao tratamento de dados pessoais objeto do contrato;

IV.3.4.5 Comunicar, em até 24 horas, a contar da ciência do ocorrido, qualquer incidente de acesso não autorizado aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da LGPD;

IV.3.4.6 Eliminar os dados pessoais que venham a ter acesso, após a satisfação da finalidade respectiva, encerramento do tratamento por decurso de prazo ou pelo término da execução contratual, ressalvados os casos em que a manutenção dos dados por período superior decorra de obrigação legal.

IV.3.5 A contratante poderá realizar auditorias nos processos da contratada para verificar a conformidade do tratamento dos dados pessoais pertinentes ao objeto do referido contrato, conforme determinado pela LGPD e pela Resolução TSE nº 23.650/2021.

IV.3.6 As partes responderão administrativa e judicialmente, em relação aos danos patrimoniais, morais, individual ou coletivo, comprovadamente causados aos titulares de dados pessoais, em decorrência da execução contratual por inobservância da LGPD e Resolução TSE nº 23.650/2021.

IV.4 - Da transferência de conhecimento

IV.4.1 Treinamento ministrado por um técnico certificado da Checkpoint para repasse de conhecimento técnico necessário para operacionalizar as soluções dentro do escopo atual do TRE-RJ

IV.4.2. A garantia de que toda informação gerada durante os processos de instalação e migração seja integralmente apresentada pela equipe da contratada, por meio de métodos expositivos, realização prática das atividades, apresentação de resumos, esquemas, relatórios ou qualquer outro documento que viabilize ou facilite a absorção da tecnologia do novo ambiente pela equipe da contratante.

IV.4.3 Outra forma se dará através dos acompanhamentos nos atendimentos técnicos especializados da contratada, sejam nas manutenções preventivas ou corretivas.

IV.5 REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

IV.5.1 Mesmo em se tratando de demanda por resultados focada em qualidade, em função das políticas de gestão de segurança implantada que definem os conceitos de utilização, monitoração, manutenção e segurança dos recursos de TI, é imprescindível que os recursos técnicos envolvidos na execução dos serviços estejam alocados em área interna exclusiva definida, sendo gerenciados exclusivamente pelo representante da empresa contratada. Esses recursos humanos deverão conhecer o funcionamento dos negócios internos da STI e executar os procedimentos de acordo com as regras de segurança, não sendo possível execução ou operacionalização remota. O mesmo ocorre com manutenções e monitorações que requeiram utilização de senhas privilegiadas ou que possam manipular ou ver informações de serviços críticos.

V - MODELO DE EXECUÇÃO DO CONTRATO (Art. 6º, Inciso XXIII, Alínea “e”, da Lei 14.133/2021)

V.1 As aquisições serão formalizadas através de termo de contrato, que deverá ser assinado pela empresa vencedora do certame no máximo em 3 dias úteis, contados da convocação deste Tribunal, sob pena de decair o direito à contratação, sujeito às sanções legais cabíveis.

V.2. Será verificado, por meio do SICAF e de outros meios, a manutenção das condições de habilitação exigidas no Edital.

V.3 A entrega dos equipamentos (itens 1, 3 e 8) e licenças (itens 2 e 4) deverão ser efetuada na SEREDE — Seção de Suporte às Redes Locais , localizada na Av. Presidente Wilson, 198 — 7º andar, Castelo, Rio de Janeiro, no horário de 10h00 as 17h00. Telefones: (21) 3436-8065/3436-8189/3436-8166/3436-8078.

V.4 Enquanto não expirado o prazo de entrega, a contratada poderá substituir os produtos recusados pelo Tribunal. Para isso, o prazo de entrega considerar-se-á suspenso durante a fase de análise, reiniciando-se a contagem do prazo restante a partir da data da comunicação da recusa à empresa. A suspensão só poderá ocorrer uma única vez.

V.5. Eventual solicitação de prorrogação do prazo de entrega, motivada por fato excepcional e estranho à vontade da contratada, somente será passível de apreciação caso remetida a este Tribunal ainda na vigência do prazo original de entrega, devidamente fundamentada, para o e-mail compras@tre-rj.jus.br, ressaltando-se que a confirmação de recebimento da solicitação não garante a dilação pleiteada, uma vez que a autorização da prorrogação fica a critério deste Tribunal.

V.6. A contratada ficará obrigada a trocar, às suas expensas, os equipamentos recusados pelo TRE-RJ, observando-se que o mero recebimento não caracteriza a aceitação do mesmo.

V.7 A contratada deverá, obrigatoriamente, entregar a totalidade do material solicitado, sob pena das sanções legais cabíveis.

V.8 O material deverá ser acondicionado conforme a praxe do fabricante, devendo garantir proteção durante transporte e estocagem, constar identificação do produto e demais informações exigidas na legislação em vigor.

V.9 Todos os equipamentos fornecidos deverão ser acondicionados e entregues em embalagens constituídas preferencialmente de materiais reciclados, recicláveis ou reutilizáveis, individualmente, com menor volume possível, de forma a garantir a máxima proteção durante o transporte e o armazenamento;

V.10 Os equipamentos deverão ser de primeiro uso, sendo aplicadas todas as normas e exigências do Código de Defesa do Consumidor.

V.11 Os serviços de instalação e configuração serão realizados pela equipe técnica especializada da CONTRATADA. Eles terão acesso a dados da rede IP do TRE-RJ, contudo será exigida a assinatura do Termo de compromisso de sigilo e confidencialidade responsáveis a ser firmado pela empresa e o TRE-RJ, conforme (**ANEXO I.3 - Id.4028332**) deste Termo.

V.12. Cronograma de execução

O recebimento dos equipamentos e serviços obedecerão às etapas e eventos descritos nas tabelas abaixo.

Evento	Responsável	Prazo
Assinatura do contrato	TRE-RJ e Contratada	Após a emissão da nota de empenho
Prazo máximo para entrega de 02 (dois) Equipamentos Firewall Principais, os 8 (oito) transceivers. suas licenças, 10 Firewall secundários e suas licenças	Contratada	Em até 45 (quarenta e cinco) dias corridos contados a partir do início da vigência do contrato. Após o recebimento dos materiais, será emitido o Termo de Recebimento Provisório. Início do PFE – Período de Funcionamento Experimental
Fim do período para que as instalações e configurações deverá ser realizada no prazo de 10 dias, contados do recebimento provisório	TRE-RJ	Em até 55 (cinquenta e cinco) dias corridos e contados a partir do início da vigência do contrato pela contratada terá Finalização do PFE – Período de Funcionamento Experimental, e emissão do Termo de Recebimento Definitivo
Início do período relativo ao suporte técnico da solução (Firewalls principais e secundários e suas respectivas licenças e Acesso Remoto (Mobile Access Blade Unlimited).	TRE-RJ e Contratada	Na emissão do Termo de Recebimento Definitivo.
Fim do período relativo ao serviço de suporte.	Contratada	36 (trinta e seis) meses após emissão do Termo de Recebimento Definitivo.
Treinamento	Contratada	Deverá ocorrer no prazo máximo de 10 (dez) meses, contados a partir do primeiro dia útil seguinte à assinatura do Contrato

Tabela 1 – Etapas e eventos para recebimento dos Firewalls

V.13.1 A contagem dos prazos constantes na tabela de etapas e eventos para implantação da solução será em dias corridos.

V.13.2 Caso a conclusão de algum evento/etapa seja antecipada, os eventos/etapas subsequentes serão automaticamente antecipados.

V.14.14 Os empregados da CONTRATADA deverão assinar termo de sigilo e responsabilidade **(ANEXO I.4 - Id. 4028381)** antes de iniciar suas atividades junto ao TRE-RJ.

V.14.15 A CONTRATADA deverá promover o afastamento, no prazo máximo de 24 (vinte e quatro) horas, após o recebimento da notificação por e-mail, de qualquer dos seus recursos técnicos que não correspondam aos critérios de confiança ou que perturbem a ação da equipe de fiscalização do TRE-RJ.

V.14.16. A CONTRATADA deverá responsabilizar-se pelos materiais, produtos, ferramentas, instrumentos e equipamentos disponibilizados para a execução dos serviços, não cabendo ao TRE-RJ qualquer responsabilidade por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer.

V.14.17 Para que a CONTRATADA atenda aos requisitos exigidos com relação às normas de Controle de Acesso, deverá:

V.14.17.1 Responsabilizar-se pelo credenciamento e descredenciamento de acesso às dependências do TRE-RJ e suas unidades, assumindo quaisquer prejuízos porventura causados por dolo ou culpa de seus profissionais.

V.14.17.2 Fornecer aos seus colaboradores, sem qualquer ônus para o TRE-RJ, crachás de identificação com foto, nome, cargo e logo da empresa.

V.14.17.3 Solicitar, por escrito, o credenciamento e autorização de acesso para os recursos técnicos da CONTRATADA.

V14.17.4 Informar e solicitar ao FISCAL TÉCNICO do TRE-RJ, no prazo máximo de 24 (vinte e quatro) horas, o descredenciamento dos recursos desvinculados da prestação de serviços com o TRE-RJ.

V.14.17.5 Devolver todos os recursos e equipamentos utilizados pela CONTRATADA, como crachás, cartões certificadores, “pendrives” e outros, de propriedade do TRE-RJ, juntamente com a solicitação de descredenciamento.

V14.17.6 A CONTRATADA deverá manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas à:

V14.17.6.1 Políticas de segurança adotada pelo TRE-RJ e Órgãos de Controle, assim como as configurações de hardware e de softwares decorrentes;

V14.17.6.2 Processo de instalação, configuração e customização de produtos, ferramentas e equipamentos;

V.14.17.6.3 Quaisquer dados sensíveis dos quais a CONTRATADA venha a ter conhecimento em decorrência da presente contratação.

V.14.18 Os colaboradores da CONTRATADA, enquanto estiverem prestando serviços nas instalações do TRE-RJ, deverão estar em conformidade com seguintes normas:

V.14.18.1 Resolução TSE nº 20.882/01 - Normas para uso dos ambientes de redes internet e intranet e correio eletrônico, no âmbito da Justiça Eleitoral.(Alterada pela Res. TSE nº 23.266/10)

V.14.18.2 Resolução TSE nº 23.644/2021 - Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.

V.14.18.3 Resolução TRE-RJ nº 948/2016 - Institui o Código de Ética do Tribunal Regional Eleitoral do Rio de Janeiro. (Alterada pelas Res.TRE/RJ nº 1085/19 e 1278/2023)

V.14.18.4 Resolução TRE-RJ nº 1.222/2022 - Dispõe sobre a adoção da Política de Segurança da Informação da Justiça Eleitoral.

VI - MODELO DE GESTÃO DO CONTRATO (Art. 6º, Inciso XXIII, Alínea “f”, da Lei 14.133/2021)

VI.1. EQUIPE DE GESTÃO E FISCALIZAÇÃO DOS CONTRATOS

VI.1.1 Os gestores e fiscais de execução serão designados dentre os servidores da Serede e da Coinf.

VI.2 FORMA DE COMUNICAÇÃO ENTRE OS AGENTES

VI.2.1. O acompanhamento e a fiscalização da execução do contrato serão exercidos por representantes do TRE-RJ (gestor e fiscal do contrato) especialmente designados para este fim.

VI.2.2. Compete ao gestor dirimir eventuais dúvidas que surgirem no curso e sua execução e de tudo dar ciência à Contratada, para fiel execução contratual durante toda a vigência do contrato.

VI.2.3. Além da reunião de alinhamento e validação de expectativas da contratação, deverão ser realizadas, se necessárias, outras reuniões presenciais ou não entre o Gestor do Contrato e o Preposto da Contratada para avaliação do serviço(s) prestado(s) no período, e verificação do atendimento aos requisitos contratuais estabelecidos;

VI.2.4. Poderão ser realizados, alternativamente, e a critério do Gestor do Contrato, o controle e o acompanhamento da prestação de serviço mediante o uso de mensagens eletrônicas. Nesse caso, Gestor do Contrato deverá apresentar descritivo contendo situações merecedoras de avaliação por parte da Contratada;

VI.2.5. A contratada deverá substituir por outro profissional de qualificação igual ou superior qualquer um dos seus profissionais cuja qualificação, atuação, permanência ou comportamento decorrentes da execução do objeto forem julgados prejudiciais, inconvenientes ou insatisfatórios à disciplina do órgão ou ao interesse do serviço público, sempre que exigido pelo Gestor do Contrato,

VI.2.6. A contratada deverá prestar todos os esclarecimentos que lhe forem solicitados pelo contratante, atendendo prontamente a todas as reclamações, no prazo de 02 (dois) dias úteis.

VI.3. CRITÉRIOS E METODOLOGIA DE FISCALIZAÇÃO

VI.3.1 Do preposto

VI.3.1.1. Preposto: funcionário representante da empresa 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. Compete ao Preposto:

- O representante nomeado pela empresa Contratada deverá ter condições de coordenar a execução do Contrato e ter poderes expressos para representá-la em todos os atos do contrato, especialmente para ajustes obrigacionais registrados em atas de reuniões, termos de recebimento ou recusa de objeto a ser entregue, notificações, ofícios, e demais atos relacionados à execução do contrato;

- Esta designação será escrita, assinada pelo representante da empresa Contratada (outorgante) e pelo próprio preposto indicado, podendo ocorrer através de e-mail;

- No ato da designação, a empresa Contratada deverá apresentar todas as informações de contato do preposto escolhido (endereço, telefone, celular, WhatsApp, e-mail etc.), bem como os canais específicos para o registro de solicitações, consultas, intimações, etc.

- Havendo necessidade de realizar reuniões de planejamento e/ou ajuste da execução dos serviços, o gestor do contrato poderá convocar reuniões específicas, as quais o Preposto da empresa Contratada deverá comparecer.

- Reportar-se imediatamente ao gestor do contrato, por escrito, quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução do objeto prestando ao TRE-RJ os esclarecimentos necessários.

VI.3.1.2. O preposto da Contratada deve enviar os relatórios e as notas fiscais ao fiscal de execução e ao gestor do contrato.

VI.3.1.3. A Contratada deve informar os dados do novo Preposto, até o próximo dia útil, em caso de mudança do Preposto por iniciativa da contratada.

VI.3.1.4. A Contratada deve informar os dados do novo Preposto, em até 5 dias úteis, em caso de mudança do Preposto por solicitação do TRE-RJ.

VI.4 Competências dos agentes da administração

VI.4.1. Gestor do Contrato: servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão do contrato. Compete ao gestor do contrato:

- Planejar e orientar a contratação, especialmente para estabelecer diretrizes para a contratação e condução dos vínculos contratuais;
- Acompanhar e fiscalizar a execução do Contrato junto com o fiscal do contrato dirimindo eventuais dúvidas que surgirem no curso de sua execução e de tudo dar ciência à empresa Contratada, para fiel execução contratual durante toda a vigência do contrato.
- Além da reunião de alinhamento e validação de expectativas da contratação, deverão ser realizadas, se necessárias, outras reuniões presenciais ou não entre o Gestor do Contrato e o Preposto da empresa Contratada para avaliação do serviço(s) prestado(s) no período, e verificação do atendimento aos requisitos contratuais estabelecidos;
- Manter-se sempre informado de todos os cumprimentos e descumprimentos contratuais e repassar às autoridades pró-ativamente aquelas que interfiram no gerenciamento da Administração;
- Controlar e acompanhar a prestação dos serviços mediante o uso de mensagens eletrônicas, como também na operacionalização da garantia, podendo o Gestor do Contrato, ou o Fiscal Técnico, apresentar descritivo contendo situações merecedoras de avaliação por parte da Contratada.
- Paralisar a execução do contrato no caso de estar em desacordo com o pactuado ou diante de graves descumprimentos pelo fornecedor ou riscos para a Administração. Em caso de descumprimento das condições exigidas, o Gestor do Contrato deverá proceder à abertura de processo para apuração de responsabilidade, podendo resultar na rescisão do contrato (com aplicação de penalidade à contratada) e a necessidade de nova contratação.
- Solicitar os pertinentes ajustes no contrato.
- Conduzir o encerramento do contrato.
- Realizar o recebimento definitivo do objeto.

VI.4.2. Fiscal de Execução do Contrato: 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, bem como para atestar o recebimento provisório.

Compete ao Fiscal do Contrato:

- Avaliar o cumprimento das obrigações contratuais;
- Cobrar da Contratada o cumprimento do contrato;
- Manter contato com a Contratada de modo a promover todo o tipo de interlocução operacional em nome do Tribunal;
- Comunicar ao Gestor do contrato as ocorrências detectadas de cumprimento e de descumprimento contratual.
- As decisões e providências que ultrapassarem a competência da fiscalização deverão ser solicitadas a seus superiores em tempo hábil para adoção das medidas convenientes;
- O fiscal anotará as ocorrências relacionadas com a execução do Contrato, determinando o que for necessário à regularização das faltas ou defeitos observados, conforme Termo de Referência;
- Devolver para a empresa Contratada 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;
- A fiscalização será exercida no interesse exclusivo do TRE-RJ e não exclui nem reduz a responsabilidade da Contratada por qualquer inconsistência;

VI.5. Das situações de aplicação de multa:

GRAU	CORRESPONDÊNCIA % sobre ...(definir se os percentuais incidirão sobre o valor mensal ou sobre o valor total do contrato).
1	0,5% a 2%
2	3% a 5%
3	6% a 10%
4	20%
5	30%

VI.5.1. São situações passíveis de aplicação de multas por inexecução total ou parcial do objeto do contrato ou pelo descumprimento de obrigações contratuais:

Item	Descrição	Grau	Incidência
1	Deixar de executar objeto solicitado, sem motivo justificado.	5	Por ocorrência
2	Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequências letais nas dependências da Contratada.	1	Por ocorrência.
3	Deixar de cumprir quaisquer dos itens do contrato e seus anexos não previstos nesta tabela de multas	4	Por ocorrência
4	Deixar de manter a documentação de habilitação atualizada.	2	Por item e por ocorrência
5	Deixar de cumprir determinação formal ou instrução complementar da fiscalização.	2	Por ocorrência
6	Utilizar as dependências da CONTRATANTE para fins diversos do objeto do contrato	2	Por ocorrência
7	Inexecução total do contrato	5	Única

VI.5.2.São situações passíveis de aplicação de multas moratórias por atraso na execução do objeto ou no cumprimento de obrigação contratual

Item	Descrição	Grau	Incidência
1	Atraso injustificado na entrega dos equipamentos Firewalls ou serviços solicitados .	3	Por dia
2	Suspender ou interromper, salvo motivo força maior ou caso fortuito, os serviços contratuais.	3	Por dia
3	Atrasar na correção dos serviços considerados insatisfatórios, no prazo fixado pela Fiscalização.	3	Por ocorrência e por dia de atraso

VII - CRITÉRIOS PARA MEDIÇÃO DOS RESULTADOS E AFERIÇÃO DE QUALIDADE DOS SERVIÇOS PRESTADOS (Art. 6º, Inciso XXIII, Alínea “g”, da Lei 14.133/2021)

VII.1. O Instrumento de Medição de Resultados – IMR não se aplica na presente contratação.

VII.2. O processo de liquidação e pagamento seguirá as seguintes etapas e prazos:

Etapa	Procedimento de fiscalização	Prazo	Responsável
Recebimento provisório (itens 1 a 4 e 8)	Conferência da conformidade dos quantitativos entregues em relação à descrição no documento fiscal e neste Termo de Referência	Até 2 dias corridos a contar da entrega dos equipamentos	Fiscal de Execução do Contrato
Recebimento provisório (item 5)	Conferência da conformidade dos serviços prestados em relação às exigências técnicas previstas neste Termo de Referência	Até 2 dias corrido a contar da instalação e configuração	Fiscal de Contrato
Recebimento provisório (item 7)	Conferência da conformidade dos serviços prestados em relação às exigências técnicas previstas neste Termo de Referência	Até 1 (um) dia útil a contar do começo do treinamento	Fiscal do contrato
Recebimento definitivo (itens 1 a 4 e 8)	Conferência da conformidade das características dos materiais em relação à descrição constante neste Termo de Referência	Até 10 dias a contar da emissão do termo de recebimento provisório	Gestor de Contrato
Recebimento definitivo (item 5)	Conferência da conformidade dos serviços prestados em relação às exigências técnicas previstas neste Termo de Referência	Até 10 dias a contar da emissão do termo recebimento provisório	Gestor de Contrato
Recebimento definitivo (Item 7)	Conferência da conformidade do serviço prestado em relação às exigências técnicas previstas neste Termo de Referência	Até 5 dias a contar da Aprovação do Treinamento	Gestor de Contrato
Atesto da nota fiscal (para todos os itens)	Conferência da conformidade do documento fiscal	Até 1 dia útil a contar da emissão do termo de recebimento definitivo	Gestor de Contrato
Pagamento	Verificação da regularidade fiscal da contratada e demais condições de habilitação	Até 10 dias úteis a contar do atesto da nota fiscal	Secretaria de Orçamento e Finanças

VII.2.1. O recebimento do objeto da contratação não exclui a responsabilidade civil, nem a ético-profissional pela perfeita execução do Contrato, dentro dos limites estabelecidos pela lei.

VII.2.2. O pagamento será realizado por meio de ordem bancária, creditada na conta corrente da contratada.

VII.2.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

VII.2.4 Em caso de erro na nota fiscal, esta será devolvida à contratada, com a exposição dos motivos do não atesto e o prazo referido acima retornará à contagem inicial.

VII.2.4.1 Caso a nota fiscal apresente valor superior ao correto a faturar, a contratada poderá autorizar a glosa da diferença apurada ou a substituição da mesma, no prazo máximo de 3 dias úteis, a contar da comunicação deste Tribunal.

VII.2.5. Os prazos serão interrompidos sempre que se façam necessários a solução de pendências na execução do objeto, identificadas em qualquer etapa da liquidação da despesa ou do saneamento na inconsistência do documento fiscal apresentado pela contratada.

VII.2.6. Caso a contratada opte por efetuar o faturamento por meio de CNPJ (matriz ou filial) distinto daquele constante na proposta, a regularidade fiscal e trabalhista de ambos os estabelecimentos.

VII.2.7. No caso de atraso no pagamento provocado exclusivamente pela Administração, a contratada fará jus à atualização financeira, com juros de mora de 0,00016438% ao dia, alcançando-se 6% ao ano, multiplicados pelo número de dias de atraso entre a data do vencimento e o efetivo adimplemento da parcela.

VIII - FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR (Art. 6º, Inciso XXIII, Alínea “h”, da Lei 14.133/2021)

VIII.1. Modalidade de Licitação e Adjudicação do objeto

VIII.1.1 O fornecedor será selecionado por meio de licitação, na modalidade Pregão, sob a forma eletrônica, com a adoção do critério de julgamento pelo menor preço por grupo na forma da Lei 14.133/2021.

VIII.2. Condições de análise da proposta.

VIII 2.1 Certificado de que os equipamentos referentes aos itens 1 e 3 desta contratação, são fabricados com materiais que não agridam ao meio ambiente, comprovado mediante o atendimento à diretiva RoHs(Restriction of Hazardous Substances) a ser comprovado através de certificado ou autodeclaração do fabricante.

VIII.2.2.Carta de parceria ou referência no site oficial do fabricante Check Point Software Technologies Ltda. (endereço eletrônico), de forma a comprovar que é o fornecedor e parceiro oficial do fabricante Check Point;

VIII.3.2. Condições de Habilitação:

VIII.3.2.1.Declaração do licitante, indicando os profissionais responsáveis pela execução do objeto desta contratação, que deverão ser especializados na solução tecnológica implantada, devendo esta condição ser comprovada mediante certificados emitidos pelo fabricante.

VIII.3.2.1.1.A empresa se compromete durante a vigência do contrato, manter profissionais técnicos qualificados, garantindo a qualidade na prestação dos serviços.

VIII.3.2.2. Atestado de capacidade técnica, emitido por pessoas jurídicas de direito público ou privado, comprovando que a empresa já forneceu solução de natureza compatível com pelo menos, 2 firewalls principais e 5 secundários e que já prestou os serviços de suporte e assistência técnica por, pelo menos, 18 meses.

VIII.3.2.2.1 O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

VIII.3.2.3 A justificativa para as exigência de habilitação técnica se fundamentam nos comandos legais contidos na Lei 14.133/2021, na necessidade de aferição da experiência e da expertise da empresa em executar o objeto a ser contratado, desde que constatada a execução anterior satisfatória, de modo a minimizar riscos para a regular execução do objeto.

VIII.3.2.4 A habilitação econômico-financeira

VIII.3.2.4.1. Certidão negativa de falência expedida pelo distribuidor da sede do licitante.

VIII.3.2.4.2 Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos dois últimos exercícios sociais, que comprove:

VIII.3.2.4.2.1 Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um); ou alternativamente patrimônio líquido mínimo de 10% do valor total estimado do grupo.

Fórmula dos índices contábeis:

I - Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante);

II - Solvência Geral (SG)= (Ativo Total) / (Passivo Circulante +Passivo não Circulante); e

III - Liquidez Corrente (LC) = (Ativo Circulante) / (Passivo Circulante).

VIII.3.2.4.2.2 Deverá ser apresentada declaração assinada por profissional habilitado da área contábil, que ateste o atendimento pelo licitante dos índices acima exigidos.

VIII.3.2.5. Os requisitos de qualificação técnica e econômico-financeira definidos neste Termo de Referência visam verificar se a situação financeira do licitante é suficientemente boa para suportar a execução do contrato, diante da criticidade do objeto para o funcionamento das atividades deste Tribunal.

VIII.4. Da Vistoria

VIII.4.1. É facultado aos interessados a realização de vistoria no local onde será realizada a execução do presente objeto a fim de se obter os subsídios necessários à adequada elaboração das propostas comerciais.

VIII.4.2. A vistoria poderá ser realizada por um representante da licitante, acompanhada por um profissional técnico Seção de Suportes às Redes Locais - Serede, impreterivelmente até o dia anterior à data prevista para a realização da abertura da licitação, em data previamente marcada pelo telefone (21) 3436-8065 ou 3436-8166 ou 3436-8189 em dias úteis, no horário de 11h às 18h, ou e-mail serede@tre-rj.jus.br.

VIII.4.3. Ao término da vistoria será emitido, em 2 (duas) vias, o termo de Declaração de Vistoria, conforme modelo constante do (**ANEXO I.5 - Id. 4028452)** - Modelo De Declaração De Vistoria deste Termo de Referência.

VIII.4.4 A declaração de vistoria deverá ser assinada pela Serede e pelo Licitante, comprovando que a empresa realizou a vistoria técnica para conhecimento dos serviços necessários, dos ambientes de instalação e das condições técnicas para sua realização.

VIII.4.5 A forma do §3° do artigo 63 da Lei 14.133/21, caso o licitante abstenha-se de realizar a vistoria prevista no subitem VIII.2.1.1, deverá apresentar declaração, atestando que conhece o local e as condições de execução do objeto, conforme modelo do **ANEXO I.6 - Id. 4028454.**

VIII.4.6 A Licitante que optar pela não realização da vistoria estará se responsabilizando por todas as condições de fornecimento, não podendo em qualquer momento da execução contratual alegar desconhecimento ou impossibilidade para a prestação dos serviços.

IX - ADEQUAÇÃO ORÇAMENTÁRIA (Art. 6º, Inciso XXIII, Alínea “i” e “j”, da Lei 14.133/2021)

1. Unidade Gestora Responsável

COINF - COORDENADORIA DE INFRAESTRUTURA

2. Ação Orçamentária

Julgamento de Causas e Gestão Administrativa da JE

3. Código do Item Orçamentário

COI013

4. Código CNAE

7050

5. Valor estimado da despesa

O valor estimado da despesa constará de documento anexo a este Termo de Referência.

X - DECLARAÇÃO SOBRE SIGILO DO ORÇAMENTO DA CONTRATAÇÃO:

Não se aplica.

Rio de Janeiro, 01 de outubro de 2024

JOSE AMARO DOS SANTOS FILHO
CHEFE DA SEÇÃO DE SUPORTE ÀS REDES LOCAIS

Documento assinado eletronicamente em 03/10/2024, às 17:38, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

ALBERTO CARMO DE ARAUJO
COORDENADOR(A) DE INFRAESTRUTURA

Documento assinado eletronicamente em 03/10/2024, às 17:51, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

FELIPE DE MELLO SANTOS
CHEFE DA SEÇÃO DE INSTRUÇÃO DE COMPRAS

Documento assinado eletronicamente em 03/10/2024, às 18:20, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.