TRIBUNAL REGIONAL FEDERAL 5ª REGIÃO

TERMO DE REFERÊNCIA

1. DEFINIÇÃO DO OBJETO

Pregão com registro de preços, com validade da ata de 1(um) ano, para aquisição de Solução de NGFW com licenças e garantias para 48 meses.

Lote	Item	Descrição	TRF5	JFPE	JFAL	JFPB	JFRN	Total Registrado
1	1	Solução de NGFW Tipo 01	2	2	0	0	0	4
	2	Solução de NGFW Tipo 02	0	0	2	2	2	6
	3	Serviço de Instalação, Configuração e Migração Tipo 1	2	2	0	0	0	4
	4	Serviço de Instalação, Configuração e Migração Tipo 2	0	0	2	2	2	6
	5	Treinamento Técnico Oficial Tipo 1	1	1	0	0	0	2
	6	Treinamento Técnico Oficial Tipo 2	0	0	1	1	1	3
	7	Horas de Consultoria	200	200	200	200	200	1000

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1 JUSTIFICATIVA

Nos últimos anos, é notável o crescimento da infraestrutura de informática do Tribunal. Dezenas de novos sistemas e aplicações estão fazendo parte da rotina diária dos clientes internos e externos da DITI. PJes (Processo Judicial Eletrônico versões 1 e 2), Esparta, SEI, SGC, Jurisprudência, Diário Eletrônico, são exemplos destes sistemas, dentre tantos outros.

Além disso, cada vez mais é necessária a garantia de disponibilidade destes sistemas, devido às suas criticidades. Como exemplo disto, temos o caso dos Processos Judiciais Eletrônicos - PJes, que devido a suas

características de atendimento aos usuários, deve ter o mínimo de inatividade.
Portanto, o TRF da 5a Região possui um parque de recursos tecnológicos que necessitam de proteção constante. O Núcleo de Gestão da Segurança da Informação adota, dentre outros, o método de proteção em camadas para o ambiente de TI.
O método de proteção em camadas consiste em criar várias camadas de proteção distintas e complementares, sendo cada camada atuando de forma especializada em algum componente de segurança. Uma das camadas de proteção é realizada pelo firewall.
O firewall é um sistema, configurado pelos administradores, que permite liberar ou bloquear o tráfego passante entre redes. As regras de liberação e bloqueio são necessárias para se bloquear acessos indevidos a sistemas e redes e, devem sempre seguir o princípio do privilégio mínimo.
Atualmente, o TRF5 possui como firewall a solução da Palo Alto (PA 3220), que atende satisfatoriamente às suas necessidades de segurança e disponibilidade. Entretanto, o hardware dessa estrutura não é de domínio do Tribunal, que possui apenas o licenciamento para operar o produto, cedido em regime de comodato.
Dessa forma, com o vencimento desse licenciamento e visando adquirir um produto completo e de maior capacidade para operar na nuvem privada da JF5 faz-se necessário um novo processo de contratação, incluindo outras unidades da 5ª Região a fim de possibilitar uma gerência única, caso seja necessário, além da padronização dos equipamentos adquiridos
Diante do exposto, faz-se necessária a renovação, por parte do TRF5, de garantia e licenças da solução de firewall atual do TRF5.
Ingressa como participante deste pregão para registro de preços, além do TRF5, a JFPE, a JFAL, a JFPB e a JFRN.
Enfatizando que os itens foram agrupados no mesmo lote pois existe uma dependência entre estes itens para o correto funcionamento da solução, que deverá ter a possibilidade de gerência unificada a partir de um mesmo site da Justiça Federal da 5ª Região. Também visa uniformizar e padronizar as aquisições da JF5, garantindo maior economicidade, eficiência e disponibilidade dos serviços oferecidos.

2.3 MOTIVAÇÃO

Os seguintes fatores motivaram essa contratação:
• Reforço da segurança cibernética do TRF5 e Seções Judiciárias;
• Aumento da quantidade de ataques maliciosos às aplicações oferecidas pelo TRF5 e Seções Judiciárias;
• Aumento nos sistemas informatizados e processos digitais;

2.4 ALINHAMENTO ESTRATÉGICO

O elevado grau de automação dos processos operacionais e administrativos leva as Organizações a confiar e depender cada vez mais de sua infraestrutura tecnológica para viabilizar aplicações de missão crítica e implementar rapidamente novas soluções que aumentem a agilidade, a capacidade de adaptação, a otimização de custos e a melhoria dos serviços prestados, de forma continuada, aos seus clientes e usuários. Atender a essa demanda por alta qualidade e eficiência com economia, confiabilidade, flexibilidade, agilidade e racionalização de fluxos de trabalho, é preocupação constante da alta direção dos órgãos, o que tornou a Tecnologia da Informação e Comunicação ferramenta estratégica que deve estar alinhada com as áreas de negócios da Instituição. O serviço objeto de contratação encontra-se alinhado com o Plano Diretor de TI do TRF5ª Região através do objetivo estratégico: assegurar atuação sistêmica da TI na Justiça Federal. Iniciativa PDTI: I.13 (Manutenção e Evolução de Soluções de Segurança da Informação). Plano de ação: ID 44.
- Meta: Atingir, até 2026, 85% de satisfação dos clientes internos
Face ao exposto e em conformidade com os princípios constitucionais de legalidade, impessoalidade, moralidade, publicidade e, em especial, de eficiência, a solução para o suporte aos usuários e às operações de TI descrita neste termo de referência e seus anexos constitui-se em objeto de contratação estratégico para o alcance das metas e propósitos perseguidos pela Justiça Federal

2.5 RESULTADOS A SEREM ALCANÇADOS

I. Disponibilidade de sistemas e aplicações do TRF5 (PJe, PJe 2.0, Esparta, Portais, SGC, SEI, Diário Eletrônico, etc);
II. Reforço da estrutura de Segurança da Informação, principalmente em virtude do aumento massivo de ataques cibernéticos à órgãos governamentais.
III. Minimizar o risco de continuidade do negócio por ataques à infraestrutura de TI.
IV. Melhoria no nível de segurança de dados da Justiça Federal da 5ª Região;

2.6 JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

Cenário 01 – Não adquirir nenhuma solução.
Não é recomendável devido ao aumento exponencial de ataques maliciosos direcionados às aplicações. Um reforço na segurança cibernética é extremamente indicado com um equipamento de nova geração, com atualização e suporte do fabricante.
Cenário 02 – Utilizar solução gratuita.
Não é recomendável devido, entre outras coisas, a demora na atualização de vacinas para bloqueio de tentativas de invasão e falta de suporte a apoio de fabricante.
Cenário 03 – Realizar licitação para adquirir solução moderna e eficiente.
A aquisição de uma solução moderna e eficiente trará ao Tribunal um reforço na Segurança de TI, com as melhores especificações e o menor custo a ser determinado em licitação.
Obviamente, por existir a possibilidade de uma solução nova, há de se considerar os custos com treinamento, instalação, configuração e banco de horas de suporte.
É a solução escolhida, pois trará ao Tribunal um reforço na Segurança de TI, com as melhores especificações e o menor custo a ser determinado em licitação.

3. ESPECIFICAÇÃO TÉCNICA

3.1 Lote 1 – Itens 1 e 2 - Solução de NGFW - Tipo 01/02:
3.1.1 Solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança da informação perimetral que inclui, filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares “Zero Day”, filtro de URL, bem como controle de transmissão de dados e acesso à Internet compondo uma plataforma de segurança integrada e robusta;
3.1.2 Por plataforma de segurança entende-se hardware e software integrados do tipo appliance.
3.1.3 Capacidade e quantidades
3.1.3.1 A plataforma de segurança deve possuir a capacidade e as características abaixo, por equipamento:
3.1.3.1.1 Para o item 1, throughput de, no mínimo, 15 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;
3.1.3.1.2 Para o item 2, throughput de, no mínimo, 5,5 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;
3.1.3.1.3 Para o item 1, throughput de, no mínimo, 9.5 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Anti-spyware.
3.1.3.1.4 Para o item 2, throughput de 3.0 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
3.1.3.1.5 Os throughputs devem ser comprovados por documento de domínio público do fabricante;
3.1.3.1.6 Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend);
3.1.3.1.7 Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4;
3.1.3.1.8 Para o item 1, suporte a, no mínimo, 4.000.000 de conexões simultâneas;
3.1.3.1.9 Para o item 2, suporte a, no mínimo, 2.000.000 de conexões simultâneas;
3.1.3.1.10 Para o item 1, suporte a, no mínimo, 165.000 novas conexões HTTP por segundo;
3.1.3.1.11 Para o item 2, suporte a, no mínimo, 60.000 novas conexões HTTP por segundo;
3.1.3.1.12 Fonte 120/240 AC, redundante e hot-swappble;
3.1.3.1.13 Cooler hot-swappable;
3.1.3.1.14 Disco Solid State Drive (SSD) redundante de, no mínimo, 240 GB;
3.1.3.1.15 Apenas para o item 1, disco de, no mínimo, 2 TB em RAID 1 para armazenamento de logs interno ou externo a solução de firewall;
3.1.3.1.16 Interfaces para o tipo 1:
3.1.3.1.16.1 No mínimo, 04 (quatro) interfaces de rede 1 Gbps em portas cobre;
3.1.3.1.16.2 No mínimo, 04(quatro) interfaces de rede 1 Gbps SFP;
3.1.3.1.16.3 No mínimo, 04 (quatro) interfaces de rede 10 Gbps SFP+;
3.1.3.1.16.4 No mínimo, 02 (quatro) interfaces de rede 40 Gbps QSFP+;
3.1.3.1.16.5 2 (duas) interfaces dedicadas para alta disponibilidade;
3.1.3.1.16.6 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;

3.1.3.1.16.7 1 (uma) interface do tipo console ou similar;
3.1.3.1.17 Interfaces para o tipo 2:
3.1.3.1.17.1 8 (oito) interfaces de rede 1 Gbps 10/100/1000 base-TX ou SFP;
3.1.3.1.17.2 8 (oito) interfaces de rede 10 Gbps SFP+;
3.1.3.1.17.3 2 (duas) interfaces dedicadas para alta disponibilidade;
3.1.3.1.17.4 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;
3.1.3.1.17.5 1 (uma) interface do tipo console ou similar;
3.1.3.1.18 Para o tipo 1, suporte a, no mínimo, 60 (sessenta) zonas de segurança;
3.1.3.1.19 Para o tipo 2, suporte a, no mínimo, 60 (sessenta) zonas de segurança;
3.1.3.1.20 Para o tipo 1, estar licenciada para ou suportar sem o uso de licença, no mínimo, 10.000 (dez mil) clientes de VPN SSL simultâneos;
3.1.3.1.21 Para o tipo 2, estar licenciada para ou suportar sem o uso de licença, no mínimo, 2.000 (dois mil) clientes de VPN SSL simultâneos;
3.1.3.1.22 Para o tipo 1, estar licenciada para suportar 3.000 (três mil) túneis de VPN IPSEC simultâneos;
3.1.3.1.23 Para o tipo 2, estar licenciada para suportar 3.000 (três mil) túneis de VPN IPSEC simultâneos;
3.1.3.1.24 Para o tipo 1, deve suportar, no mínimo, 10 sistemas virtuais lógicos (Contextos) no firewall Físico;
3.1.3.1.25 Para o tipo 1, deve permitir expansão futura a até 20 sistemas virtuais lógicos (Contextos) no firewall Físico;
3.1.3.1.26 Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-spyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;
3.1.3.1.27 Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;
3.1.3.1.28 Por console de gerência e monitoração, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;
3.1.3.1.29 A console de gerência e monitoração podem residir no mesmo appliance de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função;
3.1.3.1.30 Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
3.1.3.1.31 A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
3.1.3.1.32 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
3.1.3.1.33 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;
3.1.3.1.34 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
3.1.3.1.35 O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
3.1.3.1.36 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
3.1.3.1.37 O software deverá ser fornecido em sua versão mais atualizada;
3.1.3.1.38 Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
3.1.3.1.38.1 Agregação de links 802.3ad e LACP;
3.1.3.1.38.2 Policy based routing ou policy based forwarding;
3.1.3.1.38.3 Roteamento multicast (PIM-SM);
3.1.3.1.38.4 DHCP Relay;
3.1.3.1.38.5 DHCP Server;
3.1.3.1.38.6 Jumbo Frames;
3.1.3.1.38.7 Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
3.1.3.1.38.8 Suportar sub-interfaces ethernet logicas;
3.1.3.1.39 Deve suportar os seguintes tipos de NAT:
3.1.3.1.39.1 NAT dinâmico (Many-to-1);

3.1.3.1.39.2 NAT dinâmico (Many-to-Many);
3.1.3.1.39.3 NAT estático (1-to-1);
3.1.3.1.39.4 NAT estático (Many-to-Many);
3.1.3.1.39.5 NAT estático bidirecional 1-to-1;
3.1.3.1.39.6 Tradução de porta (PAT);
3.1.3.1.39.7 Suportar NAT de Origem e NAT de Destino simultaneamente;
3.1.3.1.40 Deve implementar o protocolo ECMP;
3.1.3.1.41 Deve implementar balanceamento de link através do método round-robin;
3.1.3.1.42 Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quatro links;
3.1.3.1.43 Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;
3.1.3.1.44 Deve implementar balanceamento de link através de políticas por aplicação ou porta de destino;
3.1.3.1.45 Deve implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;
3.1.3.1.46 Enviar log para sistemas de monitoração externos, simultaneamente;
3.1.3.1.47 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
3.1.3.1.48 Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
3.1.3.1.49 Proteção contra anti-spoofing;
3.1.3.1.50 Deve permitir bloquear sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
3.1.3.1.51 Deve permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;
3.1.3.1.52 Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;
3.1.3.1.53 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
3.1.3.1.54 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
3.1.3.1.55 Suportar a OSPF graceful restart;
3.1.3.1.56 Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;
3.1.3.1.57 Suportar no mínimo as seguintes funcionalidades em IPv6:
3.1.3.1.57.1 SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação;
3.1.3.1.58 Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);
3.1.3.1.59 Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
3.1.3.1.60 Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
3.1.3.1.61 Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
3.1.3.1.62 Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
3.1.3.1.63 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
3.1.3.1.63.1 Em modo transparente;
3.1.3.1.63.2 Em layer 3;
3.1.3.1.64 A configuração em alta disponibilidade deve sincronizar:
3.1.3.1.64.1 Sessões;
3.1.3.1.64.2 Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de

rede;
3.1.3.1.64.3 Certificados de-criptografados;
3.1.3.1.64.4 Associações de Segurança das VPNs;
3.1.3.1.64.5 Tabelas FIB;
3.1.3.1.65 O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
3.1.3.1.66 As funcionalidades de VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

3.1.4 Controle por política de Firewall
3.1.4.1.1 Deverá suportar controles por zona de segurança;
3.1.4.1.2 Controles de políticas por porta e protocolo;
3.1.4.1.3 Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
3.1.4.1.4 Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
3.1.4.1.5 Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;
3.1.4.1.6 Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;
3.1.4.1.7 Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;
3.1.4.1.8 Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);
3.1.4.1.9 Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);
3.1.4.1.10 Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com HTTP/2, TLS 1.2 e 1.3;
3.1.4.1.11 Controle de inspeção e de-criptografia de SSH por política;
3.1.4.1.12 A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;
3.1.4.1.13 A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);
3.1.4.1.14 É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise;
3.1.4.1.15 Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;
3.1.4.1.16 Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);
3.1.4.1.17 QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;
3.1.4.1.18 Suporte a objetos e regras IPV6;
3.1.4.1.19 Suporte a objetos e regras multicast;
3.1.4.1.20 Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall:
3.1.4.1.20.1 Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
3.1.5 Controle de Aplicações
3.1.5.1.1 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
3.1.5.1.1.1 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
3.1.5.1.1.2 Reconhecer pelo menos 1700 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;
3.1.5.1.1.3 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;
3.1.5.1.1.4 Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões

regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;
3.1.5.1.1.5 Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
3.1.5.1.1.6 Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443;
3.1.5.1.1.7 Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
3.1.5.1.1.8 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. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro da mesma. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementada
3.1.5.1.1.9 Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos especificados apenas para alguns usuários;
3.1.5.1.1.10 Identificar o uso de táticas evasivas via comunicações criptografadas;
3.1.5.1.1.11 Atualizar a base de assinaturas de aplicações automaticamente;
3.1.5.1.1.12 Reconhecer aplicações em IPv6;
3.1.5.1.1.13 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;
3.1.5.1.1.14 Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
3.1.5.1.1.15 Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
3.1.5.1.1.16 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;
3.1.5.1.1.17 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
3.1.5.1.1.18 Permitir nativamente a criação de assinaturas personalizadas ou a importação da assinatura na própria interface para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
3.1.5.1.1.19 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
3.1.5.1.1.20 Deve alertar o usuário quando uma aplicação for bloqueada;
3.1.5.1.1.21 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
3.1.5.1.2 Deve permitir criar filtro na tabela de regras de segurança para exibir somente:
3.1.5.1.2.1 Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;
3.1.5.1.2.2 Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;
3.1.5.1.2.3 Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;
3.1.5.1.2.4 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;
3.1.5.1.2.5 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos;
3.1.5.1.2.6 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;
3.1.5.1.2.7 Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo

granularidade de controle/políticas para os mesmos;
3.1.5.1.3 Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:
3.1.5.1.3.1 Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc);
3.1.5.1.3.2 Nível de risco da aplicação;
3.1.5.1.3.3 Categoria e sub-categoria de aplicações;
3.1.5.1.3.4 Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.;
3.1.5.1.3.5 Deve proteger as aplicações contra movimentos laterais através da implementação de múltiplos fatores de autenticação;

3.1.6 Prevenção de Ameaças
3.1.6.1.1 Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante;
3.1.6.1.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-spyware);
3.1.6.1.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
3.1.6.1.4 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e Antispyware: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
3.1.6.1.5 Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2;
3.1.6.1.6 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
3.1.6.1.7 Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;
3.1.6.1.8 Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware , possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
3.1.6.1.9 Deve permitir o bloqueio de vulnerabilidades;
3.1.6.1.10 Deve permitir o bloqueio de exploits conhecidos;
3.1.6.1.11 Deve incluir proteção contra ataques de negação de serviços;
3.1.6.1.12 Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE;
3.1.6.1.13 Deverá possuir os seguintes mecanismos de inspeção de IPS:
3.1.6.1.13.1 Análise de padrões de estado de conexões;
3.1.6.1.13.2 Análise de decodificação de protocolo;
3.1.6.1.13.3 Análise para detecção de anomalias de protocolo;
3.1.6.1.13.4 Análise heurística;
3.1.6.1.13.5 IP Defragmentation;
3.1.6.1.13.6 Remontagem de pacotes de TCP;
3.1.6.1.13.7 Bloqueio de pacotes malformados;
3.1.6.1.14 Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc;
3.1.6.1.15 Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;
3.1.6.1.16 Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
3.1.6.1.17 Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
3.1.6.1.18 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
3.1.6.1.19 Possuir assinaturas para bloqueio de ataques de buffer overflow;
3.1.6.1.20 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
3.1.6.1.21 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
3.1.6.1.22 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

3.1.6.1.23 É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;
3.1.6.1.24 Suportar bloqueio de arquivos por tipo;
3.1.6.1.25 Identificar e bloquear comunicação com botnets;
3.1.6.1.26 Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);
3.1.6.1.27 Deve suportar referência cruzada com CVE;
3.1.6.1.28 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
3.1.6.1.28.1 O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
3.1.6.1.29 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Anti-spyware;
3.1.6.1.30 Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;
3.1.6.1.31 Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
3.1.6.1.32 Os eventos devem identificar o país de onde partiu a ameaça;
3.1.6.1.33 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
3.1.6.1.34 Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos;
3.1.6.1.35 Rastreamento de vírus em pdf;
3.1.6.1.36 Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);
3.1.6.1.37 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança etc., ou seja, cada regra de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
3.1.6.1.38 Deve Permitir a importação, criação e edição de regras SNORT.
3.1.6.1.39 A solução deve mostrar nos logs as seguintes informações sobre domínios DGA:
3.1.6.1.39.1 Domínio suspeito identificado;
3.1.6.1.39.2 ID de assinatura de detecção;
3.1.6.1.39.3 Usuário logado na estação/servidor que originou o tráfego;
3.1.6.1.39.4 Aplicação;
3.1.6.1.39.5 Porta de destino;
3.1.6.1.39.6 IP de origem;
3.1.6.1.39.7 IP de destino;
3.1.6.1.39.8 Horário;
3.1.6.1.39.9 Ação do firewall;
3.1.6.1.39.10 Severidade;
3.1.6.1.40 A solução deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;
3.1.6.1.41 A análise automática deve incluir, no mínimo, as seguintes características:
3.1.6.1.41.1 Padrões de consulta;
3.1.6.1.41.2 Entropia;
3.1.6.1.41.3 Análise de frequência n-gram de domínios;
3.1.6.1.41.4 Taxa de consultas.
3.1.7 Análise de Malwares Modernos
3.1.7.1 Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;
3.1.7.2 O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;
3.1.7.3 Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;
3.1.7.4 Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;

3.1.7.5 Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 e Windows 10;
3.1.7.6 Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;
3.1.7.7 A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;
3.1.7.8 A análise de links em sand-box deve deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;
3.1.7.9 Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;
3.1.7.10 O sistema de análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);
3.1.7.11 O sistema automático de análise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;
3.1.7.12 Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;
3.1.7.13 Deve permitir o download dos malwares identificados a partir da própria interface de gerência;
3.1.7.14 Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;
3.1.7.15 Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia zero a partir da própria interface de gerência;
3.1.7.16 Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 28 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;
3.1.7.17 Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;
3.1.7.18 Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
3.1.7.19 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar), MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;
3.1.7.20 Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box;
3.1.7.21 Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API;
3.1.7.22 Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução;
3.1.7.23 A solução deve analisar os arquivos do tipo malware em bare metal para evitar técnicas de evasão. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executem esta função;
3.1.7.24 Deve prevenir contra ataques em arquivo buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: Powershell e Javascript.
3.1.8 Filtro de URL
3.1.8.1 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
3.1.8.1.1 Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
3.1.8.1.2 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;
3.1.8.1.3 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 ldap, Active Directory, E-directory e base de dados local;
3.1.8.1.4 Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
3.1.8.1.5 Possui pelo menos 60 categorias de URLs;

3.1.8.1.6 Deve classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;
3.1.8.1.7 Deve possuir categoria específica para classificar domínios recém registrados (com menos de 32 dias);
3.1.8.1.8 A solução deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;
3.1.8.1.9 A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;
3.1.8.1.10 Suporta a criação categorias de URLs customizadas;
3.1.8.1.11 Suporta a exclusão de URLs do bloqueio, por categoria;
3.1.8.1.12 Permite a customização de página de bloqueio;
3.1.8.1.13 Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;
3.1.8.1.14 Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;
3.1.8.1.15 Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);
3.1.8.1.16 Suporta a inclusão nos logs do produto de informações das atividades dos usuários;
3.1.8.1.17 Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;
3.1.9 Identificação de Usuários
3.1.9.1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;
3.1.9.2 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
3.1.9.3 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
3.1.9.4 Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
3.1.9.5 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;
3.1.9.6 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
3.1.9.7 Suporte a autenticação Kerberos;
3.1.9.8 Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, Captive Portal e usuário de VPN SSL;
3.1.9.9 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
3.1.9.10 Deve identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;
3.1.9.11 Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-fowarded-for;
3.1.9.12 O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos a organização;
3.1.9.13 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
3.1.9.14 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.
3.1.10 QOS
3.1.10.1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de

largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.
3.1.10.2 Suportar a criação de políticas de QoS por:
3.1.10.2.1 Endereço de origem;
3.1.10.2.2 Endereço de destino;
3.1.10.2.3 Por usuário e grupo do LDAP/AD;
3.1.10.2.4 Por porta.
3.1.10.3 O QoS deve possibilitar a definição de classes por:
3.1.10.3.1 Banda Garantida;
3.1.10.3.2 Banda Máxima;
3.1.10.3.3 Fila de Prioridade.
3.1.10.4 Suportar marcação de pacotes Diffserv, inclusive por aplicação;
3.1.10.5 Deve implementar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);
3.1.10.6 Deve suportar QOS (traffic-shapping), em interface agregadas;
3.1.10.7 Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.
3.1.11 Filtro de Dados
3.1.11.1 Permite a criação de filtros para arquivos e dados pré-definidos;
3.1.11.2 Os arquivos devem ser identificados por extensão e assinaturas;
3.1.11.3 Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);
3.1.11.4 Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
3.1.11.5 Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
3.1.11.6 Permitir listar o número de aplicações suportadas para controle de dados;
3.1.11.7 Permitir listar o número de tipos de arquivos suportados para controle de dados.
3.1.12 Geolocalização
3.1.12.1 Suportar a criação de políticas por Geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados.
3.1.12.2 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.
3.1.12.3 Deve permitir visualizar nos logs e criar políticas para liberar e bloquear tráfego de países por: tipo de arquivo, aplicação e categoria de URL;
3.1.12.4 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.
3.1.13 VPN
3.1.13.1 Suportar VPN Site-to-Site e Cliente-To-Site;
3.1.13.2 Suportar IPSec VPN;
3.1.13.3 Suportar SSL VPN;
3.1.13.4 A VPN IPSEc deve suportar:
3.1.13.4.1 3DES;
3.1.13.4.2 Autenticação MD5 e SHA-1;
3.1.13.4.3 Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;
3.1.13.4.4 Algoritmo Internet Key Exchange (IKEv1 e v2);
3.1.13.4.5 AES 128 e 256 (Advanced Encryption Standard);
3.1.13.4.6 Autenticação via certificado IKE PKI.
3.1.13.5 Deve possuir interoperabilidade com os seguintes fabricantes:
3.1.13.5.1 Cisco;
3.1.13.5.2 Checkpoint;
3.1.13.5.3 Juniper;
3.1.13.5.4 Palo Alto Networks;
3.1.13.5.5 Fortinet;
3.1.13.5.6 Sonic Wall.
3.1.13.6 Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

3.1.13.7 A VPN SSL deve suportar:
3.1.13.7.1 O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
3.1.13.7.2 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
3.1.13.7.3 Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;
3.1.13.7.4 Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;
3.1.13.7.5 Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
3.1.13.7.6 Atribuição de DNS nos clientes remotos de VPN;
3.1.13.7.7 A solução de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;
3.1.13.7.8 Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;
3.1.13.7.9 Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
3.1.13.7.10 Suportar autenticação via AD/LDAP ou OTP (One Time Password), certificado ou base de usuários local;
3.1.13.7.11 Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;
3.1.13.7.12 Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
3.1.13.7.13 Suporta leitura e verificação de CRL (certificate revocation list);
3.1.13.7.14 Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
3.1.13.7.15 O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
3.1.13.7.16 O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário.
3.1.13.8 Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:
3.1.13.8.1 Antes do usuário autenticar na estação;
3.1.13.8.2 Após autenticação do usuário na estação;
3.1.13.8.3 Sob demanda do usuário;
3.1.13.8.4 Deve Manter uma conexão segura com o portal durante a sessão.
3.1.13.9 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OSx e Chrome OS;
3.1.13.10 O cliente de VPN SSL cliente-to-site também deve suportar dispositivos móveis (IOS e ANDROID) e sistemas operacionais Linux;
3.1.13.11 Deve possuir mecanismos de checagem de conformidade do dispositivo remoto;
3.1.13.12 A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: antivírus, firewall no host;
3.1.13.13 O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;
3.1.14 Console de Gerência e Monitoração
3.1.14.1 Caso a solução de gerenciamento possua licenciamento relacionado a armazenamento, este deve ser entregue com a maior capacidade suportada ou ilimitada sem a necessidade de licenciamento adicional;
3.1.14.2 Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos;
3.1.14.3 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;
3.1.14.4 Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções;
3.1.14.5 O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance fisíco deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em appliance virtual dever ser compatível com VMware ESXi 6.5 ou superior;

3.1.14.6 Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;
3.1.14.7 Deve suportar organizar os dispositivos administrados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;
3.1.14.8 Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;
3.1.14.9 Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios;
3.1.14.10 Deve permitir a criação de objetos e políticas compartilhadas;
3.1.14.11 Deve consolidar logs e relatórios de todos os dispositivos administrados;
3.1.14.12 Deve permitir que exportar backup de configuração automaticamente via agendamento;
3.1.14.13 Deve permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;
3.1.14.14 Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;
3.1.14.15 Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;
3.1.14.16 O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
3.1.14.17 Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;
3.1.14.18 Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows ou Linux;
3.1.14.19 O gerenciamento deve permitir/possuir:
3.1.14.19.1 Criação e administração de políticas de firewall e controle de aplicação;
3.1.14.19.2 Criação e administração de políticas de IPS, Antivírus e Anti-spyware;
3.1.14.19.3 Criação e administração de políticas de Filtro de URL;
3.1.14.19.4 Monitoração de logs;
3.1.14.19.5 Ferramentas de investigação de logs;
3.1.14.19.6 Debugging;
3.1.14.19.7 Captura de pacotes.
3.1.14.19.8 Acesso concorrente de administradores;
3.1.14.19.8.1 Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;
3.1.14.20 Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI;
3.1.14.21 Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmos na configuração do dispositivo;
3.1.14.22 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
3.1.14.23 Deve permitir usar palavras chaves e cores para facilitar identificação de regras;
3.1.14.24 Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;
3.1.14.25 Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;
3.1.14.26 Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
3.1.14.27 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
3.1.14.28 Autenticação integrada ao Microsoft Active Directory e servidor Radius;
3.1.14.29 Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo

utilizados;
3.1.14.30 Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;
3.1.14.31 Criação de regras que fiquem ativas em horário definido;
3.1.14.32 Criação de regras com data de expiração;
3.1.14.33 Backup das configurações e rollback de configuração para a última configuração salva;
3.1.14.34 Suportar Rollback de Sistema Operacional para a última versão local;
3.1.14.35 Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
3.1.14.36 Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;
3.1.14.37 Validação de regras antes da aplicação;
3.1.14.38 Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.
3.1.14.39 É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.
3.1.14.40 Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
3.1.14.41 É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
3.1.14.42 Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.
3.1.14.43 Deve permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação a versão anterior;
3.1.14.44 Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)
3.1.14.45 Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
3.1.14.46 Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
3.1.14.47 Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
3.1.14.48 Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
3.1.14.49 Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day" detectados em sand-box e tráfego bloqueado;
3.1.14.50 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
3.1.14.51 Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela.
3.1.14.52 Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-spyware), etc;
3.1.14.53 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-spyware), e URLs que passaram pela solução;
3.1.14.54 Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;
3.1.14.55 Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
3.1.14.56 Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;
3.1.14.57 Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;
3.1.14.58 Deve ser possível exportar os logs em CSV;
3.1.14.59 Deverá ser possível acessar o equipamento a aplicar configurações durante momentos em que o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada;
3.1.14.60 Rotação do log;
3.1.14.61 Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em

que estão armazenados na solução, assim como no espaço em disco usado;
3.1.14.62 Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;
3.1.14.63 Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
3.1.14.63.1 Situação do dispositivo e do cluster;
3.1.14.63.2 Principais aplicações;
3.1.14.63.3 Principais aplicações por risco;
3.1.14.63.4 Administradores autenticados na gerência da plataforma de segurança;
3.1.14.63.5 Número de sessões simultâneas;
3.1.14.63.6 Status das interfaces;
3.1.14.63.7 Uso de CPU;
3.1.14.64 Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
3.1.14.64.1 Resumo gráfico de aplicações utilizadas;
3.1.14.64.2 Principais aplicações por utilização de largura de banda de entrada e saída;
3.1.14.64.3 Principais aplicações por taxa de transferência de bytes;
3.1.14.64.4 Principais hosts por número de ameaças identificadas;
3.1.14.64.5 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-spyware), de rede vinculadas a este tráfego;
3.1.14.64.6 Deve permitir a criação de relatórios personalizados;
3.1.14.64.7 Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP’s distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa.
3.1.14.65 Gerar alertas automáticos via:
3.1.14.65.1 Email;
3.1.14.65.2 SNMP;
3.1.14.65.3 Syslog;
3.2 Lote 1 - Itens 3 e 4 - Serviço de Instalação, configuração e migração:
3.2.1 Em todas as fases de planejamento instalação e configuração deverão ser realizadas com a presença de técnicos da CONTRATADA que deverão possuir capacidade técnica necessária à execução do serviço;
3.2.2 Para comprovação de capacidade, os técnicos deverão possuir certificação emitida pelo fabricante da solução para configuração dos Appliances.
3.2.3 A instalação, configuração e migração deverão ser planejadas e documentadas previamente pela CONTRATADA em conjunto com a equipe do Núcleo de Gestão de Segurança e Serviços do Tribunal, onde devem ser definidos todos os passos necessários para a migração, incluindo o cronograma e plano de testes;
3.2.4 O serviço de migração consiste na transferência das regras e demais configurações da solução atual para a solução adquirida;
3.2.5 A configuração deverá ser realizada de acordo com as recomendações do fabricante (recommended settings);
3.2.6 A instalação, configuração e migração dos appliances deverão ser iniciadas apenas após a conclusão do treinamento;
3.2.7 O prazo máximo para a instalação, configuração e migração dos appliances é de 30 (trinta) dias corridos após a conclusão do treinamento;
3.2.8 Depois de concluída a instalação, configuração e migração dos novos appliances, a CONTRATADA deverá fornecer documentação detalhada de todo o processo;
3.2.9 O TRF5 poderá solicitar à CONTRATADA a inclusão de elementos que ela achar pertinentes;
3.2.10 A CONTRATADA terá, no máximo, 10 (dez) dias corridos para efetuar as correções;
3.2.11 Toda documentação poderá ser fornecida na forma digital, não podendo estar protegida para edição.
3.3 Lote 1 – Itens 5 e 6 - Treinamento Técnico Oficial:
3.3.1 O(s) instrutor(es) deverá possuir certificação técnica comprovada, emitida pelo fabricante da solução, na configuração dos referidos appliances virtuais;
3.3.2 Para o item 5, treinamento para 6 (seis) pessoas (poderá ser online ou nas dependências do TRF);
3.3.3 Para o item 6, treinamento para 3 (seis) pessoas (poderá ser online ou nas dependências do TRF);
3.3.4 Deverá ser oficial do fabricante;
3.3.5 Deverá ser fornecido certificado de participação do treinamento aos participantes que frequentarem

pelo menos 70% do total de horas;
3.3.6 Deverá ser fornecido o material completo aos participantes do curso;
3.3.7 Após o término do curso, os integrantes do mesmo deverão responder a um questionário de avaliação informando quais assuntos foram ministrados e a avaliação do curso como um todo (péssimo, ruim, regular, bom, muito bom). Caso conste a falta de algum assunto a ser ministrado, o mesmo deverá ser realizado imediatamente. Caso a avaliação geral do curso seja regular ou ruim ou péssimo, o curso deverá ser repetido e refeito o questionário de avaliação, prosseguindo o procedimento de repetição do curso até que o conceito geral seja bom ou muito bom;
3.3.8 Deverá ter início em no máximo 15 (quinze) dias corridos após a entrega dos appliances, com as devidas licenças habilitadas.
3.3.9 O planejamento das datas e horários deverá ser combinado entre a CONTRATADA e a Subsecretaria de Informática;
3.3.10 A CONTRATADA poderá utilizar os equipamentos adquiridos pelo Tribunal e informar a necessidade de equipamentos adicionais para o treinamento (ex.: servidor Windows Server ou Linux, etc.);
3.3.11 Iniciado o treinamento, o mesmo deverá ser finalizado em um prazo máximo de 5 (cinco) dias úteis.
3.4 Lote 1 e 2 - Item 7 - Horas de Consultoria:
3.4.1 Deverá prover horas de serviços especializados para suporte a quaisquer demandas de administração, operação assistida, planejamento, tuning, reconfiguração, hardening e integração do produto ofertado com o ambiente atual. Os serviços poderão ser executados remotamente, desde que a ocorrência permita;
3.4.2 Horas para suporte de segundo nível na solução ofertada, abrangendo o apoio e execução nos procedimentos de administração, tais como:
3.4.2.1 Instalação, configuração, atualização e ajustes;
3.4.2.2 Suporte para resolução de problemas e dúvidas;
3.4.2.3 Análise, revisões, tuning e hardening da solução;
3.4.2.4 Configurações das funções avançadas quando aplicáveis;
3.4.3 Será contabilizado em termos de homem/horas de consultoria;
3.4.4 As horas deverão ser vigentes para uso durante o período de 12 meses, renováveis por mais 48 meses;
3.4.5 As horas serão consumidas sob demanda, de acordo com a necessidade da CONTRATANTE;
3.4.6 As contabilizações serão feitas individualmente para cada profissional alocado;
3.4.7 Será pago sob demanda, até o 10 dia de cada mês, as horas usadas no mês anterior;
3.4.8 O suporte técnico poderá ser prestado remotamente desde que a ocorrência permita;
3.4.9 Os serviços deverão ser realizados por profissionais capacitados e com certificação oficial do fabricante;
3.4.10 A responsabilidade pelo eventual pagamento de horas extras aos especialistas técnicos da CONTRATADA é de inteira responsabilidade desta. A CONTRATANTE não pagará nenhum valor adicional na hora contratada;
3.4.11 A CONTRATADA deverá possuir sistema de chamados via WEB que possibilite, no mínimo:
3.4.11.1 Abertura, acompanhamento, listagem e fechamento de chamados, a qualquer momento, 24 horas por dia, 7 dias por semana. Os chamados devem estar sempre atualizados ao final do dia;
3.4.11.2 Armazenar e gerar os relatórios das atividades executadas associadas ao chamado. Caso haja alguma indisponibilidade no sistema de abertura de chamados, deverão ser enviados relatórios dos chamados abertos, ao final do dia, com seus respectivos assentamentos;
3.4.11.3 Geração automatizada do número do protocolo no momento da abertura do chamado, pelo qual se referenciará cada atendimento/chamado;
3.4.11.4 Envio automatizado via e-mail para a CONTRATANTE de informações sobre todas as alterações nos status dos chamados, desde sua abertura até seu fechamento, referenciando o chamado através de seu número do protocolo;
3.4.12 A contratada deverá manter o mais absoluto sigilo sobre todas as informações nele imputadas, segregando-as inclusive de outros clientes que também mantenham contratos com a CONTRATADA e que por ventura também acessem o mesmo sistema;
3.4.13 Deverão ser fornecidas ao Gestor do Contrato do TRF5 e a um servidor responsável da Subsecretaria de Tecnologia da Informação, credenciais individuais para acesso ao sistema Web para abertura e acompanhamento dos chamados;
3.4.14 O sistema WEB será o método preferencial para abertura de chamados, porém, não eximindo a sua obrigatoriedade, para os casos de indisponibilidade deste, a CONTRATADA também deverá disponibilizar método alternativo para abertura de chamados, através de número telefônico;

3.4.15 O número telefônico designado pela CONTRATADA deverá permanecer disponível 24 horas por dia, 7 dias por semana, incluindo sábados, domingos e feriados, no qual um atendente deverá proceder a abertura do chamado e ativação da equipe técnica competente;
3.4.16 Este número telefônico deverá ser local, código de área 81, ou equivalente à chamada gratuita do tipo 0800;
3.4.17 Opcionalmente a CONTRATADA poderá disponibilizar mais de um número telefônico;
3.4.18 Excepcionalmente, como forma de agilizar a ciência a CONTRATADA nos chamados de maior criticidade, a CONTRATANTE poderá, independente da abertura do chamado via WEB, acionar a CONTRATADA via telefone;
3.4.19 A quantidade mínima de horas de um atendimento é de 1 (uma) hora;
3.4.20 Durante todo o período do contrato, 12 (doze) meses, deverá ser fornecido suporte técnico para instalação, configuração, dúvidas, otimização, troubleshooting, criação, remoção e modificação de relatórios, ajustes de funções, e demais auxílios necessários para o funcionamento da solução otimizado para o ambiente do contratante e de acordo com recomendações do fabricante para configuração otimizada e segura da solução;
3.4.21 Durante o período de suporte, deverá ser realizada a transferência de conhecimento para os técnicos do TRF5 das configurações e novas implementações realizadas;
3.4.22 O atendimento a quaisquer chamados deverá ser prestado por profissional certificado pelo fabricante;
3.4.23 Após a finalização de qualquer atendimento técnico, o profissional da contratada deverá elaborar relatório do mesmo que seja claro o suficiente para que os próprios técnicos do TRF5 possam segui-lo em caso de necessidade;
3.4.24 O relatório técnico deverá ser elaborado imediatamente após a conclusão do atendimento e deverá ser elaborado ainda nas dependências da Contratante;
3.4.25 Os chamados serão classificados em 03 (três) níveis de severidade, cada qual com seu respectivo tempo de atendimento pelos quais deverão ser priorizados, pela CONTRATANTE, de acordo com as especificações abaixo:

3.4.26 Severidade ALTA
3.4.26.1 Indicado para chamados com o maior nível de criticidade, cujo objetivo é resolver problemas que afetam de forma grave a produtividade, segurança ou desempenho da solução, pondo em risco a disponibilidade dos serviços;
3.4.26.2 Neste nível de severidade, o início do atendimento deverá ocorrer em um prazo máximo de 2 (duas) horas após a abertura do respectivo chamado;
3.4.26.3 O prazo máximo de solução deste tipo de atendimento é de 2 (dois) dias úteis contados a partir do que ocorrer primeiro entre a chegada do analista da CONTRATADA ou do prazo máximo previsto de início de atendimento após a abertura do respectivo chamado;
3.4.26.4 O atendimento deste nível de prioridade só poderá ser interrompido quando estabilizados os serviços e autorizado pelo TRF5;

3.4.27 Severidade MÉDIA
3.4.27.1 Indicado para chamados cujo objetivo é resolver problemas que afetam a produtividade, segurança ou desempenho da solução, mas que não põem diretamente em risco a sua disponibilidade;
3.4.27.2 Neste nível de severidade, o início do atendimento deverá ocorrer em um prazo máximo de 6 (seis) horas após a abertura do respectivo chamado;
3.4.27.3 O prazo de solução deste tipo de atendimento é de 3 (três) dias úteis contados, a partir do que ocorrer primeiro entre a chegada do analista da CONTRATADA ou do prazo máximo previsto de início de atendimento após a abertura do respectivo chamado;
3.4.27.4 O atendimento deste nível de prioridade poderá ser interrompido se autorizado pelo TRF5;

3.4.28 Severidade BAIXA
3.4.28.1 Indicado para chamados com menor nível de criticidade, cujo objetivo é sanar dúvidas, implementar/ajustar funções, geração de novos relatórios, apoiar em atividades administrativas/operacionais gerais da solução;
3.4.28.2 Neste nível de severidade, o início do atendimento deverá ocorrer até o próximo dia útil após a abertura do respectivo chamado;
3.4.28.3 O prazo de solução deste tipo de atendimento é de 4 (quatro) dias úteis contados, a partir do que

ocorrer primeiro entre a chegada do analista da CONTRATADA ou do prazo máximo previsto de início de atendimento após a abertura do respectivo chamado;
3.4.28.4 O atendimento deste nível de prioridade poderá ser interrompido ao final do expediente normal do TRF5, e retomado ao início do expediente do próximo dia útil de trabalho;

4. REQUISITOS DA SOLUÇÃO

4.1 REQUISITOS INTERNOS FUNCIONAIS

4.1.1 A Contratada deverá fornecer as licenças dos produtos e a documentação técnica, completa e atualizada, contendo manuais, guias de instalação e outros pertinentes, referente a procedimentos que a compõem, todos originais e redigidos em português ou inglês, não sendo aceitas cópias. A documentação técnica poderá ser entregue, também, por meio eletrônico.

4.2 REQUISITOS EXTERNOS

4.2.1 Requisitos de Qualidade dos Serviços
4.2.1.1 A CONTRATADA deverá executar fielmente o objeto contratado, de acordo com as normas legais, em conformidade com a proposta apresentada e com as orientações do CONTRATANTE, observando sempre os critérios de qualidade.
4.2.1.2 As tarefas deverão ser realizadas com base nas instruções normativas, processos e procedimentos internos ou nas boas práticas nacionais e internacionais voltadas para tecnologia da informação, tais como:
i. Para Gerenciamento de serviços de Tecnologia da Informação deve-se utilizar a biblioteca do ITIL (IT Infrastructure Library) e da NBR-ISO 20.000 – Gerenciamento de serviços de tecnologia da informação;
ii. Para gestão de governança e continuidade do negócio de Tecnologia da Informação deve-se utilizar o COBIT (Control Objectives for Information and related Technology);
iii. Para gerenciamento de projetos deve-se utilizar as boas práticas preconizadas pelo PMBOK (Project Management Base of Knowledge);
4.2.1.3 A CONTRATADA deverá fiscalizar regularmente os seus recursos técnicos designados para a prestação dos serviços verificando as condições em que as atividades estão sendo realizadas;
4.2.1.4 A CONTRATADA deverá substituir os recursos técnicos que não apresentem qualificação técnica compatível com a necessidade dos serviços, segundo as qualificações especificadas ou que apresentem conduta inadequada;
4.2.1.5 A CONTRATADA deverá refazer todos os serviços que, a juízo do representante do CONTRATANTE, não forem considerados satisfatórios, sem que caiba qualquer acréscimo no custo contratado, independentemente das penalidades previstas e Níveis de Qualidade fixados.

4.2.2 Requisitos Legais
4.2.2.1 O presente documento foi elaborado em conformidade com os seguintes ditames:

i. Lei Federal nº 8.666/1993: Institui normas para licitações e contratos da Administração Pública e dá outras providências;

ii. Lei 10.520/2002: Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências.

iii. Decreto nº 10.024/2019: Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal;

iv. Decreto nº 7.174/2010: Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal;

v. Acórdão nº 1099/2008 – TCU Plenário – Manifestou entendimento de que, havendo dependência entre os serviços que compõem o objeto licitado, a opção pelo não parcelamento mostra-se adequada, no mínimo do ponto de vista técnico;

vi. Nota Técnica nº 02/2008 – SEFTI/TCU – Estabelece o uso do pregão para aquisição de bens e serviços de tecnologia da informação;

vii. Instrução Normativa SLTI nº 01/2010: Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências;

viii. Instrução Normativa SLTI nº 04/2010: Dispõe sobre o processo de contratação de serviços de Tecnologia da Informação pela Administração Pública Federal direta, autárquica e fundacional;

ix. Resolução nº CF-RES-2012/00187: Dispõe sobre o Modelo de Contratação de Solução de Tecnologia da Informação da Justiça Federal – MCTI-JF no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus.

4.2.3 Requisitos de Política de Segurança da Informação
4.2.3.1 Manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas à política de segurança adotada pelo CONTRATANTE.

5. GESTÃO E FISCALIZAÇÃO DA CONTRATAÇÃO
5.1 PAPÉIS E RESPONSABILIDADES
5.1.1 Gestor do Contrato
5.1.1.1 Entidade: Núcleo de Gestão da Segurança da Informação NGSI/DITI/STI
5.1.1.2 Função: Servidor designado por meio de Portaria expedida pela Diretoria-Geral do TRF5, com atribuições gerenciais técnicas e operacionais relacionadas ao processo de gestão do contrato.
5.1.1.3 Responsabilidades

i. Adotar as providências necessárias ao fiel cumprimento do ajuste, tendo por parâmetro os resultados previstos neste Termo e no contrato. As decisões e providências que ultrapassarem a sua competência deverão ser encaminhadas, de imediato, aos seus superiores para a adoção das medidas pertinentes, que tomará as providências para que se apliquem as sanções previstas na lei e no contrato, sob pena de responsabilidade solidária pelos danos causados por sua omissão;

ii. Acompanhar e fiscalizar a execução dos serviços e anotar em registro próprio todas as ocorrências relacionadas com a execução, sob os aspectos quantitativos e qualitativos, comunicando ao preposto as ocorrências de quaisquer fatos que exijam medidas corretivas por parte da CONTRATADA;

iii. Alimentar o Sistema de Gestão Contratual relativo ao acompanhamento e fiscalização do contrato, especialmente, as ocorrências identificadas no exercício do seu mister;

iv. Controlar o prazo de vigência do instrumento contratual sob sua responsabilidade e solicitar à autoridade superior imediata, sempre que necessário, as medidas necessárias a não solução de continuidade da prestação do serviço;

v. Manter controle atualizado dos pagamentos efetuados, em ordem cronológica, observando para que o valor do contrato não seja ultrapassado;

vi. Receber, conferir e atestar as notas fiscais encaminhando-as à unidade competente para análise e posterior pagamento;

vii. Elaborar PAD - Pedido de Autorização de Despesa, ao constatar a necessidade de acréscimo, para verificação da disponibilidade orçamentária e autorização prévia;

viii. Comunicar à unidade técnica, formalmente, e em tempo hábil, irregularidades cometidas passíveis de penalidade, após os contatos prévios com a CONTRATADA;

ix. Solicitar à unidade competente esclarecimentos de dúvidas relativas ao contrato sob sua responsabilidade;

x. Informar à unidade de programação orçamentária e financeira, até 10 de dezembro de cada ano, as obrigações financeiras não liquidadas no exercício, visando à obtenção de reforço, cancelamento e/ou inscrição de saldos de empenho à conta de restos a pagar;

xi. Manter sob sua guarda cópias do Contrato em vigor e do respectivo Termo de Referência;

xii. Confrontar os preços e quantidades constantes da nota fiscal com os estabelecidos no contrato;

xiii. Fiscalizar o cumprimento das metas previamente estabelecidas neste Termo de Referência, acompanhando e avaliando a qualidade da execução dos serviços prestados, devendo comunicar à empresa por escrito o descumprimento das mesmas;

xiv. Comunicar à Administração o descumprimento dos prazos e metas previamente estabelecidos, para efeito de glosa e aplicação de penalidade, se for o caso.

5.2 DEVERES E RESPONSABILIDADES DO TRF5

5.2.1 Levar ao conhecimento da CONTRATADA, por escrito, qualquer fato extraordinário ou anormal que ocorrer na execução do objeto desta proposição, bem como imperfeições, falhas ou irregularidades constatadas no objeto pactuado, para que sejam adotadas as medidas corretivas necessárias.
5.2.2 Prestar as informações e os esclarecimentos que venham a ser solicitados pela FORNECEDORA.
5.2.3 Verificar e atestar as faturas da FORNECEDORA.
5.2.4 Efetuar o pagamento devido, no prazo estabelecido, desde que cumpridas todas as formalidades e exigências previstas neste Termo.

5.3 DEVERES E RESPONSABILIDADES DA FORNECEDORA

5.3.1 Responsabilizar-se integralmente pelo objeto adquirido, nas quantidades e padrões estabelecidos, sendo vedada a subcontratação, vindo a responder pelos danos causados diretamente ao TRF5 ou a terceiros, decorrentes de sua culpa ou dolo, nos termos da legislação vigente, não excluindo ou reduzindo essa responsabilidade a fiscalização ou acompanhamento pelo órgão interessado, conforme espeque no art. 70 da Lei nº 8.666/1993
5.3.2 Encaminhar à unidade fiscalizadora todas as faturas dos objetos.
5.3.3 Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes do fornecimento do objeto.
5.3.4 Reportar ao TRF5 imediatamente qualquer anormalidade, erro ou irregularidades que possa comprometer o bom andamento das atividades do Tribunal.
5.3.5 Guardar sigilo sobre dados e informações obtidos ou da relação mantida com o Tribunal.
5.3.6 Obedecer rigorosamente a todas as normas e procedimentos de segurança implementados no ambiente de TI e institucional do TRF5.
5.3.7 Responder, em prazo máximo de 48h (quarenta e oito) horas, a quaisquer solicitações/questionamentos do TRF5.
5.3.8 Comunicar formalmente e imediatamente ao TRF5 quaisquer mudanças de endereço de correspondência e contato telefônico.
5.3.9 Não empregar menores de 18 anos em trabalho noturno, perigoso ou insalubre, bem como a não empregar menores de 16 anos em qualquer trabalho, salvo na condição de aprendiz, a partir de 14 anos.

5.4 PRAZOS E CONDIÇÕES

5.4.1 Prazo para entrega dos itens 1 e 2: 90 (noventa) dias após a assinatura contratual;
5.4.2 Prazo para implantação, configuração e migração da Solução (itens 3 e 4): 30 dias corridos após a conclusão do treinamento;
5.4.3 Prazo para realização do treinamento (Itens 5 e 6): Até 15 dias corridos após a entrega dos equipamentos dos itens 1 e 2.
5.4.4 O contrato a ser celebrado deve ter a duração de 1 (um) ano, podendo, para o item 7, ser renovado por até 60 (sessenta) meses.

5.5 ACEITE, ALTERAÇÃO E CANCELAMENTO

5.5.1 Condição de Aceite
5.5.1.1 Observado o disposto nos artigos 73 a 76 da Lei 8.666/93, o recebimento do objeto desta aquisição será realizado da seguinte forma:
5.5.1.1.1 Provisoriamente, assim que efetuada a entrega, para efeito de posterior verificação da conformidade com as especificações;
5.5.1.1.2 Definitivamente, até 10 (dez) dias úteis da entrega, após verificação da qualidade e quantidade do bem e consequente aceitação.

5.5.1.2 No caso de consideradas insatisfatórias as condições do objeto recebido provisoriamente, será lavrado Termo de Recusa, no qual se consignarão as desconformidades, devendo o produto ser recolhido e substituído.
5.5.1.2.1 Após a notificação à Fornecedora, o prazo decorrido até então será desconsiderado, iniciando-se nova contagem tão logo sanada a situação.
5.5.1.3 O fornecedor terá prazo de 10 (dez) dias úteis para providenciar a substituição do objeto, a partir da comunicação oficial feita pelo TRF da 5ª Região, sem qualquer custo adicional para o TRF da 5ª Região.
5.5.1.4 O recebimento provisório e definitivo do objeto não exclui a responsabilidade civil a ele relativa, nem a ético-profissional, pela sua perfeita execução e dar-se-á se satisfeitas as seguintes condições:
5.5.1.4.1 Objeto de acordo com a especificação técnica contidas neste Termo de Referência e na Proposta Comercial vencedora;
5.5.1.4.2 Quantidades em conformidade com o estabelecido na Nota de Empenho;
5.5.1.4.3 Entrega no prazo, local e horários previsto neste Termo de Referência.

5.6 CONDIÇÕES PARA PAGAMENTO
5.6.1 Para efeitos de pagamento, a FORNECEDORA deverá apresentar documento de cobrança constando, de forma discriminada a efetiva realização do objeto adquirido, informando o nome e número do banco, a agência e o número da conta-corrente em que o crédito deverá ser efetuado.
5.6.2 A empresa contratada deverá apresentar juntamente com o documento de cobrança a comprovação de que cumpriu as seguintes exigências, cumulativamente:
5.6.2.1 Certidão de regularidade com a Seguridade Social;
5.6.2.2 Certidão de regularidade com o FGTS;
5.6.2.3 Certidão de regularidade com a Fazenda Federal;
5.6.2.4 Certidão Negativa de Débitos Trabalhistas;
5.6.2.5 Certidão de regularidade com a Fazenda Estadual.
5.6.2.6 Certidão de regularidade com a Fazenda Municipal.
5.6.3 Os documentos de cobrança deverão ser entregues pela empresa contratada, no Setor de Protocolo do TRF da 5ª Região, localizado térreo do edifício sede, situado na Avenida Cais do Apolo, s/n, Bairro do Recife, Recife / PE, CEP 500.30-908, CNPJ 24.130.072/0001-11.
5.6.4 Caso o objeto contratado seja faturado em desacordo com as disposições previstas no Edital e neste Termo de Referência ou sem a observância das formalidades legais pertinentes, a licitante vencedora deverá emitir e apresentar novo documento de cobrança, não configurando atraso no pagamento.
5.6.5 Após o atesto do documento de cobrança, que deverá ocorrer no prazo de até 05 (cinco) dias úteis contado do seu recebimento, o responsável deverá encaminhá-lo para pagamento.
5.6.6 O pagamento será efetuado:
5.6.6.1 Em parcela única mediante crédito em conta-corrente até o 5º (quinto) dia útil após o atesto do documento de cobrança e cumprimento da perfeita realização dos objetos e prévia verificação da regularidade fiscal da licitante vencedora.
5.6.6.2 Nos casos de eventuais atrasos de pagamento, desde que a FORNECEDORA não tenha concorrido de alguma forma para tanto, esta fará jus à taxa de atualização financeira devida pelo TRF5, entre a data acima referida e a correspondente ao efetivo adimplemento da parcela, condicionado ao requerimento da FORNECEDORA.
5.6.6.3 Na ocorrência da situação prevista no Subitem anterior, a taxa de atualização financeira terá a aplicação da seguinte fórmula:

EM = I x N x VP

onde:

EM = Encargos Moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga;
I = Índice de atualização financeira = 0,0001644, assim apurado:

I = (TX/100) □ I = (6/100) □ I = 0,0001644
366 365
TX = Percentual da taxa anual = 6%

5.7 SIGILO E RESTRIÇÕES

5.7.1 Condição de Manutenção de Sigilo

5.7.1.1 A FORNECEDORA deverá tratar como confidenciais e zelar pelo sigilo de todos os dados, informações ou documentos que tomar conhecimento em decorrência do objeto desta contratação, bem como deverá submeter-se às normas e políticas de segurança do TRF5, devendo orientar seus empregados e/ou prepostos nesse sentido, sob pena de responsabilidade civil, penal e administrativa;

5.7.1.2 A FORNECEDORA deverá assumir responsabilidade sobre todos os possíveis danos físicos e/ou materiais causados ao Órgão ou a terceiros, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança;

5.7.1.3 A FORNECEDORA estará sujeita às penalidades administrativas, civis e penais pelo descumprimento da obrigação assumida.

5.8 MECANISMOS FORMAIS DE COMUNICAÇÃO

5.8.1 Sempre que exigir-se, a comunicação entre o representante do TRF5 e a Fornecedora deverá ser formal, considerando-se como documentos formais, além de documentos do tipo Ofício, as comunicações por correio eletrônico.

5.9 Nos termos do artigo 67 da Lei n.º 8.666/93, a responsabilidade pela gestão e fiscalização desta contratação ficará a cargo da Subsecretaria de Tecnologia da Informação do Tribunal Regional Federal da 5ª Região e Núcleos de Tecnologia da Informação (Seções Judiciárias), através dos servidores designados, que também serão responsáveis pelo recebimento e atesto do documento de cobrança;

5.10 A gestão e fiscalização deste Contrato serão realizadas por servidores indicados pela Diretoria Geral;

5.11 As atribuições do gestor e do fiscal do contrato estão definidas na Instrução Normativa nº 03, de 28 de abril de 2014, da Diretoria Geral do TRF da 5ª Região, publicada no Diário Eletrônico Administrativo do TRF da 5ª Região nº 77.0/2014, do dia 29 de abril de 2014;

5.12 Ao tomarem conhecimento de qualquer irregularidade ou inadimplência por parte da CONTRATADA, os titulares da fiscalização deverão, de imediato, comunicar por escrito ao órgão de administração da CONTRATANTE, que tomará as providências para que se apliquem as sanções previstas na lei, no Edital, no Instrumento Contratual e no Termo de Referência, sob pena de responsabilidade solidária pelos danos causados por sua omissão:

5.13 A omissão, total ou parcial, da fiscalização não eximirá a CONTRATADA da integral responsabilidade pelos encargos ou serviços que são de sua competência.

5.14 Após a assinatura do Contrato respectivo, a Administração deverá fornecer ao gestor/fiscal designado todos os elementos necessários ao cumprimento de sua obrigação;

5.15 São de exclusiva responsabilidade da CONTRATADA, sem qualquer espécie de solidariedade por parte da CONTRATANTE, as obrigações de natureza fiscal, previdenciária, trabalhista e civil, em relação ao pessoal que a mesma utilizar para prestação dos serviços durante a execução do contrato.

6. ESTIMATIVA DE PREÇO

6.1 Para propiciar a avaliação do custo pela área requisitante, em atenção aos princípios da impessoalidade e da moralidade administrativa, em observância aos artigos 15, inciso V e 43, inciso IV da Lei nº 8.666/93 e aos Acórdãos 301/2005 – Plenário, 1544/2004 – 2ª Câmara e 1182/2004 – Plenário, do Tribunal de Contas da União, foi realizada pesquisa de preços junto a fornecedores, pregões e contratos com a Administração Pública.

6.2 O orçamento detalhado feito a partir das pesquisas aproxima-se do valor real a ser praticado na contratação, tendo em vista que o referido orçamento se baseia estritamente nos requisitos encaminhados aos possíveis licitantes.

6.3 Nos valores apresentados pelas empresas, estão incluídos, além do lucro, todas e quaisquer despesas de responsabilidade do Proponente que, direta ou indiretamente, decorram do fornecimento do objeto licitado;

7. GARANTIAS E SUPORTES

7.1 Contratada deverá comunicar ao TRF5 e as Seções sobre a descoberta de erros (bugs) na solução durante toda a vigência do contrato. A descrição destes erros e seus possíveis impactos devem ser divulgados para o TRF5 e as Seções;

7.2 A Contratada deverá comunicar ao TRF5 e as Seções cada lançamento de correção (patch) dos produtos. As correções lançadas deverão estar disponíveis para download, via Internet, no prazo máximo de 10 (dez)

dias, a contar da data do lançamento da correção, sem ônus adicional para o TRF5 e as Seções;
7.3 A Caberá ao TRF5 e as Seções a decisão por migrar ou permanecer em determinada versão da solução, sem qualquer ônus ou prejuízo ao TRF5 e as Seções;
7.4 Ao final do prazo contratual referente ao serviço de atualização e suporte técnico, o TRF5 e as Seções continuarão tendo as licenças de uso da solução na sua última versão disponível por tempo indeterminado;
7.5 O serviço envolverá, ainda, a realização das seguintes atividades, necessárias para garantir a operação contínua da solução:
7.5.1 Resolução de dúvidas e esclarecimentos relativos à utilização e configuração das funcionalidades do ambiente;
7.5.2 Resolução de problemas de desempenho do ambiente; e
7.5.3 Resolução de problemas que limitem ou impeçam o desenvolvimento e/ou execução das aplicações do TRF5 e as Seções que façam uso efetivo das suas funcionalidades;
7.6 O serviço deverá será prestado por meio da Internet e por telefone, utilizando o idioma português do Brasil;
7.7 O serviço deverá disponibilizar canais para abertura e acompanhamento de chamados em tempo integral (24 horas por dia, 7 dias por semana, todos os dias do ano, inclusive sábados, domingos e feriados), em ambas as modalidades;
7.8 O TRF5 e as Seções poderão efetuar um número ilimitado de chamados de suporte durante a vigência do contrato para suprir suas necessidades de utilização dos softwares;
7.9 A Contratada deverá disponibilizar documentação impressa ou em meio eletrônico informando o processo de abertura de chamado, incluindo um número de telefone que possibilite a realização de chamadas gratuitas para (tipo 0800) e o endereço eletrônico do suporte via web;
7.10 A Contratada deverá fornecer um conjunto de, no mínimo, 2 (dois) identificadores e respectivas senhas de acesso para pessoas autorizadas a abrir e acompanhar os chamados de suporte para os softwares;
7.11 A Contratada deverá disponibilizar documentação impressa ou em meio eletrônico informando o processo de abertura de chamado, incluindo um número de telefone que possibilite a realização de chamadas gratuitas para (tipo 0800) e o endereço eletrônico do suporte via web;
7.12 Sempre que possível, a Contratada deverá fornecer procedimento para evitar a reincidência do problema;
7.13 A finalização de cada atendimento só poderá ser efetuada com anuência formal do responsável técnico do TRF5 e Seções;
7.14 A prestação do serviço iniciará no momento seguinte após a solicitação do TRF5 e as Seções;

8. SANÇÕES APLICÁVEIS

8.1 Pela inexecução total ou parcial do objeto, pela execução em desacordo com o estabelecido, ou pelo descumprimento das obrigações, o Tribunal poderá, garantida a prévia defesa, e observada a gravidade da ocorrência, aplicar, inclusive de forma cumulativa, à FORNECEDORA as seguintes sanções, não necessariamente na mesma ordem que segue:

i. Advertência;

ii. Multa de 1% (um por cento) sobre o valor do item por dia de atraso, por não entregar o equipamento/software/licença nos prazos estabelecidos;

iii. Multa de 0,5% (zero vírgula cinco por cento), por ocorrência e por dia, calculada sobre o valor total, por deixar de cumprir determinação formal ou instrução do TRF5;

iv. Multa de 2% (dois por cento) incidente sobre o valor total, em caso de violação ao anonimato ou privacidade dos respondentes, por ocorrência;

v. Multa de 2% (dois por cento) incidente sobre o valor total por deixar de cumprir quaisquer das obrigações estabelecidas no edital e seus anexos, por ocorrência;

vi. Multa de 20% (vinte por cento) sobre o valor global, em caso de inexecução total da obrigação assumida;

vii. Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a dois anos;

viii. Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a autoridade que aplicou a penalidade, que será concedida sempre que a contratada ressarcir o Tribunal pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no item anterior;

8.2 A suspensão temporária do direito de contratar com a Administração é aplicável no caso de inexecução total, por culpa exclusiva da contratada. A declaração de inidoneidade para licitar ou contratar com a Administração Pública é aplicável no caso de fraude na execução do objeto.
8.3 As sanções de multa podem ser aplicadas à FORNECEDORA juntamente com a de advertência, suspensão temporária do direito de participar de licitação e impedimento de contratar com o Tribunal Regional Federal da 5a Região e declaração de inidoneidade para licitar ou contratar com a Administração Pública, descontando-a do pagamento a ser efetuado.
8.4 A multa aplicada em razão de atraso injustificado não impede que a Administração aplique outras sansões previstas em lei.
8.5 O disposto nos itens anteriores não prejudicará a aplicação de outras penalidades a que esteja sujeita a Contratada, nos termos dos artigos 87 e 88 da Lei nº 8.666/1993.
8.6 O valor da multa aplicada, após regular Procedimento administrativo, será descontado dos pagamentos eventualmente devidos pelo Contratante ou cobrado judicialmente.
8.7 Excepcionalmente, ad cautelam, o CONTRATANTE poderá efetuar a retenção do valor presumido da multa, calculado com base nos termos estabelecidos nos Subitens anteriores, antes da instauração do regular procedimento administrativo.
8.8 Além das penalidades citadas, à licitante vencedora ficará sujeita ainda ao cancelamento de sua inscrição no Cadastro de Fornecedores do TRF da 5ª Região, bem como será descredenciada do SICAF e, no que couberem, às demais penalidades referidas no Capítulo IV da lei 8.666/1993.
8.9 As penalidades aplicadas à licitante vencedora serão registradas no SICAF;
8.10 O rol das infrações descritas na tabela acima não é exaustivo, não excluindo, portanto, a aplicação de outras sanções previstas na Lei nº 8.666/93 e nas demais legislações específicas.

9. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR
9.1 LICITAÇÃO
9.1.1 Modalidade: Pregão Eletrônico

9.1.2 Tipo: Menor Preço por Lote

9.1.2.1 Justificativa: O objeto caracterizado pelo termo de referência teve padrão de qualidade e desempenho definidos objetivamente, além de tratar-se de objeto plenamente disponível no mercado. Desse modo, consoante previsão do art. 1º da Lei nº 10.520/02 c/c art. 2º do Dec. Fed. nº 10.024/2019, o pretendido certame licitatório deverá ser processado na modalidade pregão, na forma eletrônica e do tipo menor preço por lote.
O lote foi determinado de tal forma que existe uma dependência entre os itens para o correto funcionamento da solução, que deverá ter a possibilidade de gerência unificada a partir de um mesmo site da Justiça Federal da 5ª Região. Também visa uniformizar e padronizar as aquisições da JF5, garantindo maior economicidade, eficiência e disponibilidade dos serviços oferecidos.

9.1.3 Critério de Habilitação (Técnica Operacional)
9.1.3.1 Deverá ser apresentado atestado de capacidade técnica de fornecimento de solução de NGFW compatível com as especificações técnicas solicitadas, além da instalação e configuração de ferramenta similar à ofertada;
9.1.3.2 Todos os atestados apresentados na documentação de habilitação deverão conter, obrigatoriamente, a especificação da entrega/fornecimento executados, o nome e cargo do declarante.
9.1.3.3 Também deverá ser apresentado ponto a ponto comprovando as especificações solicitadas no item 3, juntamente com datasheets, links do fabricante, documentos oficiais, etc. a fim de checar a veracidade desta comprovação.
9.1.3.4 A Administração se resguarda no direito de diligenciar junto à pessoa jurídica emitente do Atestado/Declaração de Capacidade Técnica, visando a obter informações sobre o objeto e cópias dos respectivos contratos e aditivos e/ou outros documentos comprobatórios do conteúdo declarado.

9.1.3.5 Não será aceito pela Administração atestado/declaração emitido pela própria licitante, sob pena de infringência ao princípio da moralidade, posto que a licitante não possui a impessoalidade necessária para atestar sua própria capacitação técnica.

9.1.4 Critério de Aceitabilidade de Preços Unitários e Globais.
9.1.4.1 O preço mínimo será aquele ofertado pela empresa vencedora do pregão eletrônico, desde que atenda a todos os requisitos técnicos e administrativos exigidos neste Termo de Referência.
9.1.4.2 O preço máximo admitido pela Administração está definido no item 6 - ESTIMATIVA DE PREÇO, deste termo de referência, o qual espelha a pesquisa de mercado realizada (art. 40, X, da Lei nº 8.666/93).
9.1.5 Critério de Julgamento.
Menor Preço Global.

9.2 PLANILHA DE COMPOSIÇÃO DE PREÇOS
9.2.1 Para efeito de proposta, a licitante deverá apresentar planilha detalhada de composição de preços a fim de se auferir as quantidades, os valores unitários e totais necessários e que compõe os objetos ofertados;
9.2.2 O licitante deverá utilizar a planilha abaixo como modelo:

Lote	Item	Descrição	TRF5	JFPE	JFAL	JFPB	JFRN	Total Registrado	Preço Unitário	Preço Total
1	1	Solução de NGFW Tipo 01	2	2	0	0	0	4		
	2	Solução de NGFW Tipo 02	0	0	2	2	2	6		
	3	Serviço de Instalação, Configuração e Migração Tipo 1	2	2	0	0	0	4		
	4	Serviço de Instalação, Configuração e Migração Tipo 2	0	0	2	2	2	6		
	5	Treinamento Técnico Oficial Tipo 1	1	1	0	0	0	2		
	6	Treinamento Técnico Oficial Tipo 2	0	0	1	1	1	3		
	7	Horas de Consultoria	200	200	200	200	200	1000		

10. DO REAJUSTE DOS PREÇOS E DO EQUILÍBRIO ECONÔMICO-FINANCEIRO

10.1 O reajuste de preços poderá ser utilizado na presente contratação, desde que seja observado o interregno mínimo de 01 (um) ano da data-limite para apresentação das propostas constante do edital, em relação aos custos necessários à execução do objeto;

10.2 Será considerado índice inicial o da data da apresentação de proposta, com base na seguinte fórmula

(Decreto nº 1.054/94 e Lei nº 10.192/01):

R= V x I – Io
Io
Sendo:

R = Valor do reajuste procurado;

V = Valor contratual do serviço;

I = Índice relativo ao mês do reajuste;

Io = Índice inicial – refere-se ao índice de custos ou de preços correspondentes ao mês da entrega da proposta da licitação.

10.3 O índice a ser utilizado para o cálculo do reajustamento do contrato é o Índice Nacional de Preços ao Consumidor Amplo - IPCA divulgado pelo Instituto Brasileiro de Geografia e Estatística - IBGE, ou outro índice que venha a substituí-lo;
10.4 Caberá à contratada a iniciativa e o encargo da apresentação da memória de cálculo do reajuste a ser pleiteado, cuja aprovação do percentual de reajuste deverá ser negociada e aprovada pelo contratante, observando-se os valores praticados no mercado à época de sua concessão para serviços compatíveis com o objeto da contratação;
10.5 É vedada a inclusão, por ocasião do reajuste de itens de materiais e insumos não previstos na proposta inicial, exceto quando se tornarem obrigatórios por força de instrumento legal, sentença normativa, acordo coletivo ou convenção coletiva;
10.6 A decisão sobre o pedido de reajuste deve ser feita no prazo máximo de 60 (sessenta) dias corridos, contados a partir da solicitação e da entrega dos comprovantes de variação dos custos;
10.7 Os reajustes serão formalizados por meio de apostilamento e não poderão alterar o equilíbrio econômico-financeiro dos contratos;
10.8 O prazo referido no item 10.6 ficará suspenso enquanto a contratada não cumprir os atos ou deixar de apresentar a documentação solicitada pelo contratante para a comprovação da variação dos custos;
10.9 Os reajustes a que a contratada fizer jus e não forem solicitados durante a vigência do contrato serão objeto de preclusão com o encerramento do contrato;
10.10 Os novos valores contratuais decorrentes dos reajustes terão suas vigências iniciadas do interregno mínimo de 01 (um) ano da data de ocorrência do fato gerador que deu causa ao reajuste, ou seja, do aniversário da data-limite para apresentação das propostas constante deste edital, em relação aos custos com materiais e insumos necessários à execução do objeto contratado;
10.11 Os efeitos financeiros do reajuste ocorrerão exclusivamente para os itens que o motivaram, e apenas em relação à diferença porventura existente;
10.12 O reajuste não interfere no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico-financeiro dos contratos com base no disposto no art. 65 da Lei nº 8.666/93.

Documento assinado eletronicamente por **JOSÉ AUGUSTO LINS DE ARAÚJO NETO**, **DIRETOR(A) DE NÚCLEO**, em 09/03/2022, às 09:40, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **YURI GALINDO FRANCA DE OLIVEIRA**, **SUPERVISOR(A) DE SEÇÃO**, em 09/03/2022, às 10:10, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **KATIUSCIA DE AZEVEDO BARBOSA SANTOS**, **DIRETOR(A) DE SECRETARIA**, em 09/03/2022, às 10:43, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **VICENTE JULIAO MARQUES RODRIGUES BARROS**, **DIRETOR(A) DE SECRETARIA**, em 09/03/2022, às 12:11, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **SANDRA MARIA DA FONSECA**, **TÉCNICO JUDICIÁRIO/ APOIO ESPECIALIZADO (OPERAÇÃO DE COMPUTADOR)**, em 10/03/2022, às 11:08, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LENO PEREIRA FERREIRA**, **TÉCNICO JUDICIÁRIO/ APOIO ESPECIALIZADO (INFORMÁTICA)**, em 10/03/2022, às 11:26, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **DANIEL NUNES LIRA BARBOSA**, **ANALISTA JUDICIÁRIO/ APOIO ESPECIALIZADO (INFORMÁTICA (INFRAESTRUTURA))**, em 10/03/2022, às 12:21, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **FRANCISCO DALTON BARBOSA DIAS**, **ANALISTA JUDICIÁRIO/ APOIO ESPECIALIZADO (INFORMÁTICA)**, em 10/03/2022, às 13:54, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JOSE ALENCAR FEITOSA NETO**, **SUPERVISOR(A) DE SEÇÃO**, em 10/03/2022, às 15:46, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ABRAÃO RAFAEL BOLONHEZE**, **SUPERVISOR(A) ASSISTENTE**, em 16/03/2022, às 11:09, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.trf5.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2618215** e o código CRC **BB95775E**.