1. DEFINIÇÃO DO OBJETO

Trata-se da aquisição de uma solução de Next Generation Firewall para a implantação nos perímetros de usuário e de DataCenter, de modo a criar um perímetro de segurança completo capaz de proteger a rede do TJRJ de ataques advindos de todas as interfaces de contato externo.

A solução incluirá os equipamentos físicos, serviço de implantação/migração, treinamento, suporte técnico, suporte técnico especializado, bem como garantia de **36 (trinta e seis)** meses.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1 Demanda Prevista

2.1.1 Quantitativo a ser Contratado

2.1.1.1 01 (uma) solução de Next Generation Firewall

2.1.1.1.1 04 (quatro) appliances de Next Generation Firewall com conectores e cabeamento necessário à sua implantação;

2.1.1.2 01 (uma) solução de gerência centralizada;

2.1.1.2.1 02 (dois) appliances para solução de gerência Integrada de ativos de segurança com cabeamento necessário à sua implantação.

2.1.1.3 01 Uma solução para balanceamento dos appliances de Next Generation Firewall.

2.1.1.3.1 A solução de que trata o item 2.1.1.3, deverá ser composta de, no mínimo 02 (dois) appliances.

2.1.1.4 01 (um) serviço de implantação da solução.

2.1.1.5 01 (um) serviço de treinamento oficial da solução a ser ministrado para 4 (quatro) servidores do Poder Judiciário Estadual do Rio de Janeiro;

2.1.1.6 01 (um) serviço de suporte técnico;

2.1.1.7 01 (um) serviço de suporte técnico especializado;

2.1.1.8 01 (um) serviço de garantia.

2.2 Motivação

O TJERJ, possui hoje mais de um perímetro de comunicação com o mundo externo, como por exemplo, acesso direto à internet, acesso, via link direto, com diversos parceiros como PRODERJ, Defensoria Pública, Ministério Público, entre outros, Link com o Banco Bradesco, VPN

site-to-site com empresas prestadoras de serviço, VPN site-to-site com o CNJ, além de conexão com comarcas remotas.
Toda essa comunicação é consequência direta da integração tecnologia a serviço de uma justiça mais célere, o que permite, por exemplo, a execução de trabalho em home office, a realização de audiências remotas, etc.

Toda essa evolução, no entanto, torna a prestação jurisdicional mais suscetível a ataques vindos dos ambientes externos e internos, uma vez que amplia a quantidade de interfaces que podem ser exploradas pelos atacantes. Nesse sentido, um ataque feito a um parceiro, com conexão ao ambiente do TJERJ pode trazer graves consequências, desde tornar os serviços indisponíveis até mesmo ocasionar o furto ou perda de dados sensíveis.

Torna-se necessário, portanto, evoluir a infraestrutura de segurança de modo a abarcar todos os perímetros possíveis de comunicação com o exterior, dando a eles a quantidade de recursos de segurança compatível com o tráfego gerado, objetivando proteger os dados contra ataques internos e externos.

Outrossim, a presente contratação pretende substituir o atual contrato de prestação de serviços nº 003/0667/2019 (processo administrativo nº: 2018.031.255), com término em 15/10/2021em razão da necessidade de aumento da capacidade de processamento das transações realizadas em nossos sistemas.

2.3 Resultados a Serem Alcançados

TIPO	RESULTADO
Segurança	Ampliar a capacidade segurança a fim de evitar ataques cibernéticos advindos de diversos perímetros e capazes de tornar o ambiente indisponível ou ocasionar perda ou roubo de dados.
Eficiência / Agilidade	Modernizar o sistema de segurança, tornando-o capaz de suportar a quantidade de tráfego gerada atualmente e no futuro de modo a permitir a escalabilidade da solução.
Disponibilidade	Tornar o ambiente menos suscetível à indisponibilidade pela utilização de diversas formas atuais de prevenção, mitigação e eliminação de ameaças.
Proteção do Investimento	Proteger o investimento realizado ao se adotar uma solução escalável.

2.4 Justificativa da Solução Escolhida

Necessidade (definida no PETI)	Benefício	Tipo
CP1 – Contribuir com soluções de TI eficazes para agilizar os procedimentos administrativos e jurisdicionais.	Possibilitar a comunicação segura dos usuários externos e internos com os sistemas corporativos a fim de prover um serviço jurisdicional tecnologicamente estável e de qualidade.	Eficiência / Agilidade
CL1 – Assegurar a qualidade, disponibilidade e eficácia dos serviços de TI com foco na satisfação do cliente.	Tornar o ambiente disponível e menos suscetíveis a ataques internos e externos.	Eficiência / Agilidade
P1 – Garantir a integridade e disponibilidade de todos os serviços de TI do poder Judiciário.	Possibilitar que os serviços de TI atendam às necessidades e especificações com relação a níveis de integridade, disponibilidade e confidencialidade, esta última quando determinado, favorecendo e habilitando as operações de todas as áreas do PJERJ.	Disponibilidade / Integridade
R1 - Manter a infraestrutura de TI segura, apropriada e otimizada.	Manutenção do desempenho e dos recursos tecnológicos de modo a propiciar a máxima qualidade aos serviços oferecidos pelo TJERJ.	Disponibilidade / Eficiência

3. DESCRIÇÃO DA SOLUÇÃO DE TI

3.1 Descrição dos bens de serviços

Item	Descrição	Quantidade
1	Appliances Next Generation Firewall	4 unidades
2	Solução para balanceamento de appliances NG Firewall	2 unidades
3	Solução de Gerência Centralizada	2 unidades
4	Serviço de Implantação da Solução	1 Unidade

5	Serviço de suporte técnico	36 Meses
6	Serviço de suporte técnico especializado;	300 Horas (sob demanda)
7	Serviço de treinamento oficial da solução	4 Servidores
8	Serviço de garantia.	36 meses

3.2 Valor Estimado

****

4. ESPECIFICAÇÃO TÉCNICA

4.1 Requisitos Internos

4.1.1 Arquitetura da Solução

4.1.1.1 A solução de segurança deverá ser fornecida em appliances físicos (4 (quatro) appliances de Next Generation Firewall e 2 (dois) appliances para a solução de gerência integrada; orquestração e 2 (dois) appliances para a solução de balanceamento);

4.1.1.2 Será aceito que a solução de balanceamento e a solução de gerência estejam nos mesmos appliances, desde que isso não interfira no desempenho de cada uma;

4.1.1.3 Toda a solução, deverá vir acompanhada dos conectores e cabeamentos necessários à sua implantação e pleno funcionamento;

4.1.1.4 Não serão aceitas soluções com software e hardware de fabricantes distintos, ou mesmo soluções de uso geral como, Servidores, Estações de Trabalho ou Equipamentos como Blades, salvo no caso da Gerência Centralizada (item 2 da tabela 3.1), no caso de esta ser fornecida como máquina virtual.

4.1.1.5 Nenhum dos componentes da solução (itens 1, 2 e 3 da tabela 3.1) poderá ter seu fim de venda (End-of-Sale) e fim de vida (End-of-Life) anunciado no momento do aceite definitivo de sua entrega. Caso seja essa a situação, o fornecedor deverá

entregar um modelo equivalente ou superior ao que entrou em Fim de Venda e/ou Fim de Vida.

4.1.1.6 Em caso de anúncio do Fim de Venda e/ou Fim de Vida ocorrer após o aceite definitivo da entrega da solução, o fim de suporte (End-of-Support) não poderá ocorrer nos próximos 60 (sessenta) meses a contar da emissão do Memorando de Início.

4.1.1.7 Todos os componentes da solução (hardwares e softwares) deverão ser fornecidos com todas as licenças necessárias ao seu pleno funcionamento de modo a realizar todas as funcionalidades descritas neste Termo de Referência.

4.1.1.8 Ao final do licenciamento, deverão permanecer plenamente funcionais, no mínimo, as funcionalidades de Firewall, as funcionalidades da Gerência, dos balanceadores além todos os recursos de Hardware de todos os appliances da solução.

4.1.1.9 Todos os appliances que compõem a solução devem possuir 2 (duas) fontes de alimentação independentes, do tipo hot-swappable, com alimentação de 100~120VAC e 210~240VAC e frequência de 50 ou 60 Hz ou auto-ranging. Os cabos de alimentação devem vir com, no mínimo, 1,80m e com plugue padrão ABNT NBR 14136 (três pinos);

4.1.1.10 Cada Appliance deverá possuir a altura máxima de 4 U (quatro rack units);

4.1.1.11 Deverá ser fornecido junto da solução de que trata o item 4.1.1.1, um Rack padrão de 19” (dezenove polegadas), para fixação dos equipamentos da solução, conforme os subitens abaixo:

4.1.1.11.1 O rack deverá possuir altura de 42 U (quarenta e dois rack units);

4.1.1.11.2 O rack deverá possuir rodinhas, a fim de facilitar sua movimentação em caso de necessidade;

4.1.1.11.3 Deverá possuir chave, a fim de que seja trancado;

4.1.1.11.4 Deverá possuir guia de cabos, tanto para rede quanto para elétrica;

4.1.1.11.5 Deverá possuir PDUs ou réguas que atendam toda a necessidades de alimentação de todos os equipamentos fornecidos na solução.

4.1.1.11.6 As tomadas devem seguir o padrão do DataCenter do TJERJ.

4.1.1.11.7 O Rack de que trata o item anterior deverá vir com a Régua de Energia Elétrica capaz de alimentar todo os equipamentos da solução.

4.1.1.12 Todos os appliances que compõem a solução devem vir acompanhados de todos os acessórios que são necessários para sua fixação em rack bastidor padrão com largura de 19” (dezenove polegadas).

4.1.2 Appliances Next Generation Firewall (item 1 da tabela 3.1)

4.1.2.1 **Características Gerais da Solução**

4.1.2.1.1 A solução deve possuir um throughput de tráfego real, por appliance, de no mínimo 9 Gbps (nove Gigabits por segundo) com todas as funcionalidades de proteção/inspeção descrita neste Termo de Referência ativadas simultaneamente.

4.1.2.1.2 Deve suportar, no mínimo, 5.000.000 (cinco milhões) de conexões simultâneas para cada applicance.

4.1.2.1.3 Deve suportar 150.000 (cento e cinquenta mil) novas conexões por segundo para cada appliance;

4.1.2.1.4 Cada appliance deverá ser fornecido com a sua capacidade máxima de memória e de processamento.

4.1.2.2 **Das Interfaces:**

4.1.2.2.1 Cada appliance deve possuir a seguinte quantidade de interfaces:

4.1.2.2.1.1 06 (seis) interfaces de rede 10/100/1000BaseT com portas de cobre, do tipo UTP (RJ-45);

4.1.2.2.1.2 04 (quatro) interfaces de rede 10GBase-SR do tipo SFP+ com os respectivos transceptores para fibra multimodo (LC-LC);

4.1.2.2.1.3 Mínimo de 01 (uma) porta do tipo console para configuração e gerenciamento via linha de comando (CLI).

4.1.2.2.1.3.1 Cada equipamento deverá vir acompanhado do respectivo cabo para conexão via console.

4.1.2.2.1.4 Deve possuir, pelo menos, 01 (uma) interface de rede 1GBps (padrão 10/100Base-T e/ou 1000Base-X, com transceptor multimodo incluído) dedicada ao gerenciamento do Appliance;

4.1.2.2.1.5 Deve possuir interface dedicada para interconexão com outro equipamento de modo a compor um cluster de pelo menos 4 (quatro equipamentos);

4.1.2.2.1.6 Deve possuir, pelo menos, 01 (uma) interface para gerência out-of-band, que não dependa do sistema operacional regular do equipamento, fornecendo assim um acesso a console via rede.

4.1.2.2.1.7 Deve ser fornecido com todas as suas portas de comunicação, interfaces de redes e afins habilitadas, operacionais e prontas para operação, juntamente com seus respectivos transceptores, sem custos adicionais;

4.1.2.3 **Das Funcionalidades Básicas dos Appliances NG Firewall.**

4.1.2.3.1 Os Appliances devem permitir acesso ao equipamento via interface de linha de comando (CLI), console, SSH além de interface web HTTPS;

4.1.2.3.2 Devem ser capazes de criptografar e autenticar a comunicação com a solução de gerenciamento centralizado e/ou de orquestração;

4.1.2.3.3 Devem possuir número ilimitado de máquinas e usuários protegidos;

4.1.2.3.4 Devem implementar os protocolos IPV4 e IPV6;

4.1.2.3.5 Devem permitir a utilização simultânea de políticas de segurança tanto para IPV4 quanto para IPV6;

4.1.2.3.6 Devem suportar os protocolos DHCP e DHCPv6;

4.1.2.3.7 Devem implementar DHCP Relay;

4.1.2.3.8 Devem implementar agregação de link (link aggregation) via padrão 802.3ad e LACP;

4.1.2.3.9 Devem implementar controle de fluxo segundo o padrão IEEE 802.3X;

4.1.2.3.10 Devem suportar o protocolo NTP;

4.1.2.3.11 Devem suportar os roteamentos estático para IPV4 e IPV6

4.1.2.3.12 Devem suportar os seguintes protocolos de roteamento RIP, OSPF v2, OSPF V3 E BGP v4;

4.1.2.3.13 Devem suportar os protocolos H.323, SIP, SCCP e MGCP, de modo a dar suporte;

4.1.2.3.14 Devem suportar os protocolos RTCP, RTMP, RTSP e RTP;

4.1.2.3.15 Devem implementar o mínimo de 1024 (mil e vinte e quatro) VLANs ativas, no padrão 802.1q;

4.1.2.3.16 Devem suportar os protocolos SNMP v2 e SNMP V3;

4.1.2.3.16.1 A MIB SNMP deve contemplar, no mínimo, os seguintes indicadores: Consumo de CPU, Consumo de Memória, Temperatura, além de possuir indicadores de desempenho do equipamento.

4.1.2.3.17 Devem implementar Sflow e/ou NetFlow;

4.1.2.3.18 Devem implementar políticas de roteamento baseado em endereço IP de origem, endereço IP de destino e porta de comunicação;

4.1.2.3.19 Devem suportar o funcionamento no modo “sniffer”, para inspeção de tráfego gerado por uma porta espelhada, para layer 2 e layer 3;

4.1.2.3.20 Devem possuir mecanismo de Backup/Restore de suas configurações e regras de segurança;

4.1.2.3.21 Devem possuir o agendamento automático de backups;

4.1.2.3.22 Devem armazenar os Backups internamente além de permitir, mesmo que através da gerência, que sejam transferidos para servidores externos;

4.1.2.3.23 Devem implementar regras de acesso por IPs de origem, IPs de destino, bem como agrupamentos de IPs de origem e/ou destino;

4.1.2.3.24 Devem implementar regras de acesso por sub-rede IP, tanto para origem quanto para destino;

4.1.2.3.25 Devem implementar regras de acesso a qualquer perímetro de segurança criada, relacionando-as a um usuário específico ou grupo de usuários do Active Directory/LDAP;

4.1.2.3.26 Devem implementar regras de acesso para qualquer perímetro, para máquinas do domínio;

4.1.2.3.27 Devem implementar regras de acesso à internet baseadas em domínio;

4.1.2.3.28 Devem implementar mecanismo de captura de pacotes;

4.1.2.3.29 Devem possuir mecanismo de *"anti-spoof";*

4.1.2.3.30 Os Appliances devem implementar alta disponibilidade podendo operar nos modos Ativo-Ativo e Ativo-Passivo com todo o m licenciamento habilitado para tal e sem perda de conexões;

4.1.2.3.31 No modo de operação de cluster, deverão ser sincronizadas, no mínimo, seções, configurações como regras de firewall, NAT, QoS, objetos de rede, certificados, associações de segurança de VPNs, tabelas FIB, entre outras;

4.1.2.3.32 Devem permitir o monitoramento de falha de link na operação em cluster;

4.1.2.3.33 Devem implementar o funcionamento em modo transparente, tipo "bridge";

4.1.2.3.34 Devem permitir o sincronismo de configurações entre equipamentos do *cluster* de forma automática ou por console de gerência centralizado;

4.1.2.3.35 Devem implementar a tradução de endereços "NAT", nos seguintes modos: um-para-um, N-para-um, um-para-N e N-para-N;

4.1.2.3.36 Devem permitir que um endereço tenha mais de um NAT associado, em função da origem, destino ou porta;

4.1.2.3.37 Devem implementar NAT de origem e NAT de destino simultaneamente na mesma política;

4.1.2.3.38 Devem permitir o registro de eventos de NAT no LOG, com as informações de endereço interno, endereço público, data e hora do evento além de portas de origem e destino;

4.1.2.3.39 Devem possibilitar o registro em LOG de informações de cada sessão, de modo a armazenar endereços de IP de origem e destino, traduções de NAT, portas, protocolos, identificação de usuário e ação sobre o pacote (permitido ou negado);

4.1.2.3.40 Devem permitir a configuração e envio simultâneo de LOG para mais de um servidor de LOG;

4.1.2.3.41 Devem suportar o balanceamento de, no mínimo, 2 (dois) links distintos;

4.1.2.3.42 Devem ser capazes de bloquear sessões TCP que utilizarem variações do 3-way handshake, como 4-way e 5-way split handshake, de modo a prevenir possíveis tráfegos maliciosos;

4.1.2.3.43 Devem permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;

4.1.2.3.44 Devem exibir nos logs do tráfego, o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver decripografia de SSL;

4.1.2.3.45 Devem permitir a consulta a fontes externas de domínios, URLs e endereços IP de modo a adicioná-los às políticas de firewall para bloqueio ou permissão;

4.1.2.3.46 Devem ser capazes de descriptografar, inspecionar e criptografar novamente o tráfego criptografado SSL, "*inbound*" e "*outbound*";

4.1.2.3.47 Devem permitir a criação de políticas de inspeção de tráfego para bloqueio dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg;

4.1.2.3.48 Devem suportar objetos IPV6 de modo a permitir a criação de regras com esses objetos;

4.1.2.3.49 Devem suportar agendamento de ativação de políticas, permitindo habilitar e desabilitar, automaticamente, políticas em horários predefinidos;

4.1.2.4 **Das características de Qualidade de Serviço.**

4.1.2.4.1 Deve prover funcionalidades para controle e gerenciamento do tráfego ("*Traffic Shaping"*/ QoS – "Quality of Service") de entrada e saída (tráfego *inbound* e *outbound*) da rede ou zona de segurança;

4.1.2.4.2 Deve possibilitar a configuração de políticas de *traffic shaping* por tipo de aplicação, incluindo, entre outras, aplicações de áudio/vídeo (exemplo: Skype, Youtube), aplicações de compartilhamento de arquivos do tipo *peer-to-peer,* aplicações de redes sociais, aplicações de comunicação, aplicações de armazenamento em nuvem (exemplos: Dropbox, OneDrive, Google Drive);

4.1.2.4.3 Deve possibilitar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP e SCCP;

4.1.2.5 **Das inspeções de tráfego criptografado.**

4.1.2.5.1 Os Appliances devem ser capazes de inspecionar tráfego criptografado SSL, TLS1.3 e HTTP/2 "inbound" e "outbound";

4.1.2.5.2 Devem permitir a configuração de regras para inspeção SSL, por interface ou zona de segurança, baseadas no IP de origem e de destino, tipo de domínio, usuário/grupo de usuários do LDAP/Active Directory, URL e categoria;

4.1.2.5.3 Devem permitir a configuração de regras de exceção para que o tráfego SSL não seja inspecionado, por interface ou zona de segurança, baseadas no IP de origem e de destino, tipo de domínio, usuário/grupo de usuários do LDAP/Active Directory, URL e categoria;

4.1.2.6 **Do controle das aplicações.**

4.1.2.6.1 O cluster de appliances deve implementar regras e políticas de segurança baseadas em aplicações, de modo a bloquear e/ou liberar aplicações (individuais ou em grupo) independentemente de porta ou protocolo que utilizem;

4.1.2.6.2 Deve implementar o controle para grupos estáticos e dinâmicos de aplicações, baseado em suas características e comportamentos;

4.1.2.6.3 O controle de aplicações deve poder ser implementado em todas as regras de segurança da solução;

4.1.2.6.4 Deve reconhecer no mínimo 3.300 (três mil e trezentas) aplicações diferentes, incluindo, entre outros, aplicações peer-to-peer, redes sociais, acesso remoto, protocolos de rede, update de software, voip, streeming de vídeo, áudio e vídeo, proxies, mensageiros instantâneos, compartilhamento de arquivos, email, etc.;

4.1.2.6.5 Deve reconhecer, no mínimo, as seguintes aplicações: http-proxy, http-tunnel, gnutella, youtube, facebook, facebook chat, twitter, linked-in, Skype, teamviewer, gmail, gmail chat, whatsapp, 4shared, onedrive, google drive, google docs, dropbox, db2, mysql, oracle, active directory, ldap, kerberos, radius, Citrix, ms-rdp, logmein, ftp, dhcp, itunes, dns, wins, msrpc, ntp, snmp, rpc over http webex, evernote, etc;

4.1.2.6.6 Deve ser capaz de visualizar e controlar as aplicações e os ataques que utilizam técnicas evasivas via comunicação criptografada, como Skype e ataques na porta 443;

4.1.2.6.7 Deve inspecionar o *payload* do pacote a fim de detectar assinaturas de aplicações conhecidas pelo fabricante independentemente de porta ou protocolo;

4.1.2.6.8 Deve ser capaz de determinar se uma aplicação está utilizando, ou não, a sua porta padrão;

4.1.2.6.9 Deve decriptografar o pacote SSL para possibilitar a leitura do *payload*, a fim de verificar as assinaturas de aplicações conhecidas pelo fabricante;

4.1.2.6.10 Deve permitir a utilização de quaisquer aplicativos a determinados grupos de usuários e negar a outros;

4.1.2.6.11 Deve permitir a utilização de aplicações em nuvem apenas no modo coorporativo e bloqueá-las ao serem utilizadas no modo pessoal, como por exemplo: Office 365, Skype, aplicativos do google, gmail, etc;

4.1.2.6.12 As atualizações da base de assinaturas de aplicações devem ser atualizadas automaticamente, a qual deve ficar registrada em LOG;

4.1.2.6.13 Deve ser capaz de reconhecer aplicações em IPV6;

4.1.2.6.14 Deve ser capaz de limitar a banda de download e upload usada por aplicações (“traffic shaping”), baseado no IP de origem, usuários e grupos de usuários do LDAP/Active Directory;

4.1.2.6.15 Deve suportar diversos métodos de identificação e classificação de aplicações como: Verificação de assinaturas, decodificação de protocolos e análise heurística;

4.1.2.6.16 Deve permitir a criação de assinaturas personalizadas sem intervenção do fabricante;

4.1.2.6.17 Deve implementar o controle sobre aplicações conhecidas e desconhecidas;

4.1.2.6.18 A solução deve permitir emitir alerta ao usuário quando a aplicação for bloqueada;

4.1.2.6.19 Deve permitir que o controle de portas seja aplicado a todas as aplicações;

4.1.2.6.20 Deve permitir a criação de grupos de aplicações personalizados a partir da base de aplicações existentes;

4.1.2.6.21 Deve implementar o controle de banda para aplicações, categorias e grupos de aplicações;

4.1.2.6.22 Deve implementar o bloqueio e desbloqueio de aplicativos, sites e categorias em faixas de tempo pré-determinadas;

4.1.2.6.23 A solução deve permitir a criação de usuários administrativos específicos para funcionalidades de controle de acesso a aplicações;

4.1.2.6.24 Para cada regra de controle de acesso às aplicações, a solução deve ser capaz de desabilitar o registro de log, habilitar o registro de log e registrar a quantidade de trafego enviado, recebido e o tempo de navegação.

4.1.2.7 **Das funções de Prevenção de Intrusão.**

4.1.2.7.1 Os appliances que compõem a solução devem possuir funcionalidades de IPS (*Intrusion Prevent System*) integrado;

4.1.2.7.2 Devem possuir base de assinaturas de IPS com, no mínimo, 10.000 (dez mil) ataques conhecidos;

4.1.2.7.3 A solução deve ser capaz de inspecionar integralmente todos os pacotes de dados, independentemente dos seus tamanhos;

4.1.2.7.4 Devem implementar a inspeção pelos mecanismos de análise de padrões de estado de conexões, de análise de decodificação de protocolo, de análise e detecção de anomalias de protocolo e de “IP fragmentation”;

4.1.2.7.5 Devem suportar análise e decodificação dos protocolos de rede de camada 2 até camada 7 do modelo OSI (*Open System Interconnection*);

4.1.2.7.6 Devem ser capazes de decodificar e analisar, no mínimo, 120 (cento e vinte) protocolos, entre os quais deverão constar: DHCP, DHCP versão 6, DNS, HTTP, HTTPS, FTP, FINGER, ICMP versão 4, ICMP versão 6, IMAP, H323, SIP, SCCP, MGCP, IP versão 4, IP versão 6, LDAP, NetBIOS, POP3, NFS, NTP, RADIUS, SNMP, SMTP, SSH, SSL, TLS, RPC, TELNET, TCP, UDP, FTP e TFTP;

4.1.2.7.7 A solução deve reconhecer pelo menos os seguintes protocolos: Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IPv4 encapsulation, IPv6 encapsulation, UDP, TCP, DNS, FTP, HTTP, HTTPS,IMAP, IMAPS, MGCP, MSRPC, NetBIOS Datagram, OPC UA Binary, OPC UA, Oracle, MySQL, POP3, POP3S, SIP, SRP, SSH, TELNET, WINS, X11, RTSP,

SMTP, SunRPC, NNTP, SCCP, SMB, SMB2, TFTP e demais protocolos constantes do item 4.1.2.3 e seus sub-itens;

4.1.2.7.8 Devem ser capazes de identificar ataques para todos os protocolos de rede independentemente das portas a que estejam relacionados para no mínimo os seguintes protocolos: FTP, HTTP, HTTPS, POP3, SMTP, IMAP, DNS, SNMP e RPC;

4.1.2.7.9 Devem ser capazes de realizar análise e inspeção *Statfull* (mantendo-se o estado da conexão) e análise e inspeção *Stateless;*

4.1.2.7.10 Devem suportar analise de tráfego na direção servidor-cliente, ou seja, ataques originados no ambiente externo e direcionados a usuários internos (*Client-side Attacks ou Drive-by Attacks*);

4.1.2.7.11 Devem ser capazes de detectar bloqueio de ataques direcionados a servidores de aplicação Web (Web Application), através de tecnologia heurística ou assinaturas próprias para a proteção contra este tipo de ataque em, no mínimo, sql-injection e buffer overflow;

4.1.2.7.12 Devem ser capazes de obter informações detalhadas sobre ataques para localização geográfica, reputação de aplicação e reputação de protocolo;

4.1.2.7.13 Devem implementar algoritmo de pontuação para a relevância de um ataque conforme padrão de mercado e definido por entidade independente (*Common Platform Enumeration*), CVE ID ou Bugtraq ID, ou suportar mecanismo próprio de pontuação de ataques, permitindo distinguir quando um ataque for permitido ou bloqueado;

4.1.2.7.14 A solução deve suportar a análise do nível de relevância de um ataque, permitindo uma demonstração de faixa de relevância para, no mínimo, 4 (quatro) níveis;

4.1.2.7.15 Devem suportar as categorias de ataques e tipos de ameaças, conforme padrões de mercado e definidos por entidades independentes, podendo estas serem importadas em padrão Snort;

4.1.2.7.16 Devem suportar a configuração e administração para, no mínimo, os seguintes itens:

4.1.2.7.16.1 Perfis de DoS (Denial-of-Service) e DDoS (Distributed Denial-of-Service);

4.1.2.7.16.2 Regras de ACL (Access Control List);

4.1.2.7.16.3 Contextos de administração (Virtual IPS) que devem ser configurados por VLAN (IEEE 802.1Q) e CIDR (Classless Inter-Domain Routing);

4.1.2.7.17 Devem ser capazes de detectar e bloquear ataques do tipo Denial-of-Service (DoS) e Distributed Denial-of-Service (DDos) de forma nativa para:

4.1.2.7.17.1 Detecção e bloqueio efetivo baseado em assinaturas de ataques às vulnerabilidades de DoS, conforme padrões de mercado e definidos por entidades independentes (*Computer Emergency Response Team e Common Vulnerability and Exposures*);

4.1.2.7.17.2 Detecção e bloqueio efetivo baseado em assinaturas de atividades de agentes zumbis) DDoS, conforme padrões de mercado e definidos por entidades independentes (*Computer Emergency Response Team e Common Vulnerability and Exposures*);

4.1.2.7.17.3 Detecção e bloqueio de ataque SYN, que permita limitar e controlar a quantidade de requisições de conexões;

4.1.2.7.18 Devem ser capazes de identificar e bloquear ataques de *Brute Force*;

4.1.2.7.19 Devem implementar a Detecção e bloqueio baseados em políticas, para no mínimo:

4.1.2.7.19.1 Filtros de origem e destino por: país, nome (DNS), endereço IP, porta, bloco de endereços, rede ou grupo de redes;

4.1.2.7.19.2 VLAN ID para, no mínimo, 1024 VLANs;

4.1.2.7.19.3 Filtros de controle de aplicação: aplicação, grupo de aplicações, porta de comunicação customizada, serviço ou grupo de serviços;

4.1.2.7.19.4 Filtro de resposta com, no mínimo os itens seguintes:

4.1.2.7.19.4.1 Bloqueio (*Drop*);

4.1.2.7.19.4.2 Negação (*Deny*);

4.1.2.7.19.4.3 Quarentena (Bloquear ou negar um IP por tempo determinado após atingir a quantidade de eventos relativos a uma regra);

4.1.2.7.19.4.4 Ignorar.

4.1.2.7.20 Devem ser capazes de detectar e bloquear o tráfego de aplicações Instant Messenger, P2P (peer-to-peer) além de Proxies Anônimos;

4.1.2.7.21 Devem suportar a detecção e bloqueio de ataques através de tuneis para IPv4-in-IPv4, IPv4-in-IPv6 e IPv6-in-IPv6;

4.1.2.7.22 Devem suportar a detecção e bloqueio de ataques através de VLANs;

4.1.2.7.23 A solução deve ser capaz de não interromper ou alterar segmentos monitorados com protocolos de roteamento e redundância de rotas, ainda que trafegados dentro do protocolo LACP (Link Aggregation Control Protocol);

4.1.2.7.24 Devem permitir a criação de novas assinaturas de ataques;

4.1.2.7.25 Devem permitir a configuração e administração de ACL em camada 3 com as seguintes regras:

4.1.2.7.25.1 Permitir: O tráfego é enviado Inline sem inspeção completa dos pacotes;

4.1.2.7.25.2 Permitir e Prevenir Ataques: O tráfego é enviado Inline para inspeção completa dos pacotes;

4.1.2.7.25.3 Descartar: O tráfego será descartado;

4.1.2.7.26 Devem suportar a detecção de bloqueio de ataques, pelo menos, nas seguintes modalidades:

4.1.2.7.26.1 Inspeção de tráfego Statefull: IP defragmentation e TCP stream reassembly;

4.1.2.7.26.2 Por assinaturas: Definidas pelo fabricante e definidas pelo usuário;

4.1.2.7.26.3 Anomalias;

4.1.2.7.26.4 Por protocolos de camada 7 do modelo OSI;

4.1.2.7.27 Devem possuir detecção e bloqueio de ataques, independente de sistema operacional alvo;

4.1.2.7.28 Devem suportar a detecção heurística e consulta de reputação de atividades de agentes (zumbis) internos que pertençam a uma Botnet;

4.1.2.7.29 Devem implementar o bloqueio de tráfego inbound e outbound baseado em, no mínimo, protocolo, porta e serviço;

4.1.2.7.30 Devem implementar proteção contra downloads automáticos de arquivos executáveis maliciosos através do protocolo HTTP;

4.1.2.7.31 Devem implementar criação de políticas para bloqueio de download de arquivos por extensão e tipos de arquivo;

4.1.2.7.32 A solução deve suportar, no mínimo as seguintes categorias e tipos de ataques:

4.1.2.7.32.1 Reconnaissance: Brute force, Host Sweep, OS Fingerprinting e Port Scan;

4.1.2.7.32.2 Exploits: Arbitrary Command Execution, Backdoor, Bot, Buffer Overflow, Denial of Service, DDoS Agent Activity, Code/Script Execution, Evasion Atempt, Privileged Access, Probe, remote Access, Trojan, Virus e Worms;

4.1.2.7.32.3 Volume DoS: Statistical Deviation e Over Threshold ou possuir mecanismo que permita detecção e contenção de ataques DoS;

4.1.2.7.32.4 Policy Violations: Audit, Command Shell, Covert Channel e Non-standard Port;

4.1.2.7.33 Suportar assinaturas para detecção e bloqueio de ataques através de vulnerabilidades DoS e DDoS;

4.1.2.7.34 Devem suportar assinaturas para detecção e bloqueio de atividades de agentes (zumbis) DDoS;

4.1.2.7.35 Devem suportar aplicação e remoção de quarentena:

4.1.2.7.35.1 Sob demanda do administrador, o qual deverá ter a opção de inserir e remover um endereço IP da quarentena através de interface administrativa sem a necessidade de reinicialização do equipamento ou reaplicação de política;

4.1.2.7.35.2 Por períodos programáveis pelo administrador, podendo ser esses (os períodos) diferentes em cada regra;

4.1.2.7.35.3 Por remoção explicita, após expiração de tempo pré-determinado.

4.1.2.7.36 A solução deve suportar ajuste de bloqueio inteligente, baseado em assinaturas recomendadas pelo fabricante para bloqueio;

4.1.2.7.37 Deverá permitir a visualização de bloqueios de pacotes e de conexões, independente do motivo pelos quais ocorreram.

4.1.2.8 **Das Detecções de Ameaças (*Malwares, Worms e Spyware).***

4.1.2.8.1 A Solução deve realizar a detecção e bloqueio de códigos maliciosos, ameaças malwares e malwares avançados, vírus, *worms* e *spyware* em tempo real, utilizando-se os seguintes mecanismos:

4.1.2.8.1.1 Mecanismo de lista local de arquivos confiáveis (lista branca), os quais não precisarão ser analisados por serem confiáveis;

4.1.2.8.1.2 Mecanismo de lista com valores Hash de arquivos que sejam códigos maliciosos e ameaças (malwares) conhecidas e armazenado em uma base de dados local (lista negra);

4.1.2.8.1.3 Mecanismos de detecção de códigos maliciosos e ameaças (malwares), que deve operar em tempo real, para no mínimo, arquivos PDF, objetos e arquivos Flash, arquivos executáveis, arquivos Microsoft Office, HTML, JavaScript, arquivos comprimidos (exemplo: zip, gzip, etc).

4.1.2.9 **Da Solução de Antibot.**

4.1.2.9.1 A solução prover proteção contra tráfego de “botnets” (identificar e bloquear comunicação com redes “botnet”);

4.1.2.9.2 Deve possuir mecanismos de detecção variados e que incluam pelo menos: verificação de endereço IP e descrição da comunicação;

4.1.2.10 **Da Resposta aos ataques.**

4.1.2.10.1 Deve implementar as seguintes ações de resposta: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar “tcp-reset”;

4.1.2.10.2 Deve implementar a atualização global de bloqueio para determinado ataque de modo a propagar e atualizar todas as políticas;

4.1.2.10.3 Deve suportar a captura de pacotes para análise de evidências em formato LIBPCAP (*Library for Packet Capture*);

4.1.2.10.4 Deve suportar o envio de Trap SNMP para SNMPv2 e SNMPv3;

4.1.2.10.5 Deve implementar o envio de e-mail;

4.1.2.11 **Das Funcionalidades de VPN (Virtual Private Network).**

4.1.2.11.1 A solução de appliances devem possuir funcionalidades de concentrador VPN conforme se segue;

4.1.2.11.2 Deve implementar VPN IPSEC;

4.1.2.11.2.1 A VPN IPSEC deve ser implementada nas modalidades “site-to-site” e “cliente-to-site”;

4.1.2.11.3 Deve implementar VPN SSL;

4.1.2.11.4 Deve implementar VPNs SSL utilizando certificados digitais;

4.1.2.11.5 A solução deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos Tuneis VPN SSL;

4.1.2.11.6 A VPN IPSEC deve ser implementada com as seguintes funcionalidades/algoritmos:

4.1.2.11.6.1 Suporte aos algoritmos de criptografia DES, 3DES, AES-128 e AES-256;

4.1.2.11.6.2 Suporte à autenticação MD5 e SHA-1;

4.1.2.11.6.3 Suporte a “Diffie-Hellman” Group 1, Grtoup 2, Group 5 e Group 14;

4.1.2.11.6.4 Suporte ao algoritmo “Internet Key Exchange” – IKE v1 e v2;

4.1.2.11.6.5 Suporte a autenticação via certificado IKE PKI;

4.1.2.11.7 Deve permitir a interoperabilidade de VPN site-to-site com, no mínimo, os seguintes fabricantes: Checkpoint, Cisco, Fortinet, Junjiper, Palo Alto, Sophos e Sonic Wall;

4.1.2.11.8 A VPN IPSEC deve ser implementada por meio de conexão via Web bem como por meio de conexão via cliente VPN instalado no computador do usuário;

4.1.2.11.9 A VPN SSL deve possibilitar o acesso à rede interna e/ou zona de segurança do contratante, de acordo com a política de segurança para esta finalidade;

4.1.2.11.10 A VPN SSL deve suportar autenticação via LDAP/Active Directory, certificado digital e também na base de usuários local;

4.1.2.11.11 A VPN SSL deve implementar o controle de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário/grupo de usuários do LDAP/Active Directory;

4.1.2.11.12 A VPN SSL deve permitir a atribuição de endereço IP dinâmico aos usuários remotos, de modo a permitir a configuração e utilização de faixa de endereços IP específica ou range de IPs específicos para clientes VPN;

4.1.2.11.13 A VPN SSL deve permitir a atribuição de endereço IP fixos aos clientes remotos;

4.1.2.11.14 A VPN SSL deve possibilitar configuração que direcione todo o tráfego dos usuários remotos de VPN para dentro do túnel de VPN, ou apenas o tráfego referente às rotas que o cliente recebe ao estabelecer a conexão VPN;

4.1.2.11.15 A VPN SSL deve possibilitar atribuição de DNS aos usuários remotos de VPN;

4.1.2.11.16 A solução de VPN SSL deve permitir a criação das seguintes de políticas de segurança para o tráfego dos seus usuários remotos: inspeção de tráfego SSL, controle de aplicações, IPS, antivírus, *antispyware* e filtro Web;

4.1.2.11.17 A VPN SSL deve permitir que seja identificado o sistema operacional (bem como a sua versão) utilizado pelo usuário;

4.1.2.11.18 A solução de VPN SSL deve possuir cliente VPN, próprio ou de terceiros, para, no mínimo, os sistemas operacionais Windows 7, Windows 8, Windows 10, Mac OS X, Apple IOS, Google Android e Linux;

4.1.2.11.19 A solução de VPN SSL deve possuir cliente, próprio ou de terceiros, para instalação em dispositivos móveis (sistemas operacionais Apple iOS e Google Android), em desktops (sistemas operacionais Windows e MAC OS X), e suportar conexões VPN "*clientless*" (VPN via browser) desses sistemas operacionais e também de Linux e Chrome OS;

4.1.2.11.20 A VPN deve suportar e estar licenciada para, no mínimo:

4.1.2.11.20.1 500 (quinhentos) clientes de VPN SSL simultâneos;

4.1.2.11.20.2 1000 (um mil) túneis de VPN IPSEC simultâneos;

4.1.2.11.20.3 2500 (dois mil e quinhentos) usuários simultâneos via conexão VPN “clientless” (VPN via browser);

4.1.2.11.20.4 500 (quinhentos) usuários simultâneos com conexões via cliente VPN e VNP site-to-site;

4.1.2.11.20.5 A solução deve permitir a arquitetura de VPN HUB e SPOKE.

4.1.2.11.20.6 A solução deve implementar NAT-T (NAT *Transversal*);

4.1.2.12 **Da Prevenção contra ameaças do tipo Zero-Day e ameaças novas.**

4.1.2.12.1 A solução dever prover proteção contra malwares não conhecidos (“zero-day” /sem assinatura registrada);

4.1.2.12.2 A análise de *malwares* modernos em *sandbox* deverá ser realizada de forma interna no *appliance* do próprio fabricante ou em nuvem (serviço acessado pela Internet) do próprio fabricante;

4.1.2.12.3 A solução deverá prover proteção contra *malwares* não conhecidos (*zero-day*) nos tráfegos de entrada e saída com filtro de ameaças avançadas e análise de execução em tempo real; e inspeção de tráfego de saída de *callbacks*;

4.1.2.12.4 A solução deverá prover inspeção, bloqueio e alerta de tráfego de saída do tipo “*callbacks*” (comunicação do malware com o servidor de comando e controle);

4.1.2.12.5 A solução deve ser capaz de enviar arquivos trafegados de forma automática para análise "in cloud" ou localmente, onde o arquivo será executado e simulado em ambiente controlado (*sandbox*);

4.1.2.12.6 Deve permitir selecionar de forma granular quais tipos de arquivos serão inspecionados;

4.1.2.12.7 Deve prover a análise de arquivos maliciosos em *sandbox*, no mínimo, no sistema operacional Microsoft-Windows XP, Microsoft Windows 7 e Microsoft Windows 10;

4.1.2.12.7.1 Caso sejam necessárias licenças de sistemas operacionais e softwares para execução de arquivos na *sandbox*, as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

4.1.2.12.8 Deve permitir selecionar através de regras granulares quais tipos de arquivos serão inspecionados incluindo, no mínimo, endereço IP de origem/destino, usuário/grupo do Active Directory/LDAP, porta, tipo de arquivo bem como compor esses critérios na mesma regra;

4.1.2.12.9 Deve possuir a capacidade de diferenciar os arquivos inspecionados com pelo menos três níveis de intensidade da ameaça;

4.1.2.12.10 Deve implementar análise em *sandbox*, detecção e bloqueio de *malwares* nos seguintes tipos de arquivos:

4.1.2.12.10.1 Trafegados na Internet (*downloads* e anexos de e-mail) por meio dos protocolos HTTPS, HTTP e SMTP;

4.1.2.12.10.2 Executáveis, DLLs, ZIP e criptografados em SSL;

4.1.2.12.10.3 Do pacote MS-Office (exemplo: .doc, .docx, .xls, .xlsx, .ppt, .pptx, etc.);

4.1.2.12.10.4 Java (.jar e class);

4.1.2.12.10.5 compactados (RAR, ZIP, 7-ZIP);

4.1.2.12.10.6 no formato PDF;

4.1.2.12.11 Deve possuir a capacidade de analisar em *sandbox* links (http e https) presentes no corpo de e-mails trafegados em SMTP. Caso a análise do link pela funcionalidade de *sandbox* o identifique como ameaça ou como site hospedeiro de exploits, deve ser gerado alerta/relatório e registrado em LOG;

4.1.2.12.12 A funcionalidade de análise de links deve ser capaz de classificar sites falsos na categoria de *phishing* e atualizar a base de filtro de URL da solução;

4.1.2.12.13 Para ameaças trafegadas em protocolo SMTP, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação do usuário vítima do ataque;

4.1.2.12.14 A solução deve possibilitar a criação de novas assinaturas e atualização automática da sua base de assinaturas para bloqueio dos *malwares* identificados em *sandbox*;

4.1.2.12.15 Deve permitir a criação de regras de exceção por Interfaces, zonas de segurança, sub-rede, endereço IP de destino ou origem, para que o tráfego não passe por esse tipo de inspeção;

4.1.2.12.16 A solução deve permitir visualizar a quantidade de arquivos enviados para análise em *sandbox*;

4.1.2.12.17 A solução deve prover mecanismo do tipo “painel de controle” e relatório onde seja possível a visualização de, no mínimo, as informações de sumário de detecção e proteção além de gráfico com as principais ameaças detectadas;

4.1.2.12.18 A solução deve prover relatório das análises em *sandbox* contendo detalhamento dos arquivos analisados (nome, extensão, tamanho, etc.), bem

como detalhamento das atividades identificadas na análise, como alterações em arquivos do sistema operacional, alterações nos registros, utilização da rede, manipulação de processos, etc.;

4.1.2.12.19 Com base nos resultados das análises em *sandbox* a solução deve gerar assinaturas de antivírus e *antispyware* automaticamente e integrá-las à sua base de assinaturas contra ameaças;

4.1.2.12.20 Com base nos resultados das análises em *sandbox* a solução deve prover informações, no mínimo o seu endereço IP, sobre o usuário infectado;

4.1.2.12.21 A solução deve permitir exportar o resultado das análises de *malwares* "*zero-day*" em PDF.

4.1.2.13 **Das Funcionalidades de filtro de URL.**

4.1.2.13.1 A solução deve prover o controle e proteção de acesso à Internet por meio do reconhecimento de aplicações, independente de porta e protocolo, e da classificação de URLs;

4.1.2.13.2 A solução deve permitir a criação de regras que possibilitem a permissão e bloqueio de acessos baseado no mínimo nos seguintes critérios:

4.1.2.13.2.1 Origem: grupos de domínio, serviços de diretório LDAP ou Active Directory e Aplicação;

4.1.2.13.2.2 Destino: categoria, domínio e url/lista;

4.1.2.13.2.3 Tipo de arquivo;

4.1.2.13.2.4 Protocolos HTTP, FTP, entre outros;

4.1.2.13.2.5 Horário, e período (dia, mês, ano, dia da semana) de modo a definir os períodos de funcionamento por regra;

4.1.2.13.3 A solução deve permitir a definição de largura e percentual de banda máxima para o acesso, de acordo com o estabelecido em regra, baseando-se em IP de origem, grupos de usuários, categoria do destino e/ou protocolo;

4.1.2.13.4 A solução deve ser capaz de atuar como "man in the middle" de modo a intermediar e repassar todas as requisições;

4.1.2.13.5 A solução deve suportar certificados on-box, de modo a importar certificados válidos ou gerar certificados auto-assinados;

4.1.2.13.6 Deve permitir a emissão de páginas customizáveis de erro também aos sites criptografados;

4.1.2.13.7 Deve permitir controle de acesso através do percentual de largura de banda disponível para determinadas categorias e, os limites de banda devem der definidos por:

4.1.2.13.7.1 Limite geral ou percentual de banda, de modo a definir um limite para todos os usuários e aplicações na rede, de modo a restringir a quantidade de tráfego gerado;

4.1.2.13.7.2 Limite de banda por usuário, de modo a definir um limite para um usuário específico ou uma categoria de usuários.

4.1.2.13.8 A Solução deve permitir a definição de quota de acesso, de modo que determinados destinos (categorias, URLs, domínios ou listas) possam ser acessados por um período limitado de tempo;

4.1.2.13.9 Deve possuir mecanismo de classificação em tempo real dos sites visitados ou sistema de filtro de reputação que permita estabelecer uma reputação para cada endereço IP dos servidores de destino;

4.1.2.13.10 A rede de reputação a que se refere o item anterior não deve somente ser baseada em informações de fluxo da própria base de appliances instalados, mas sim em correlações entre outros parâmetros: Listas negras de URL, listas Brancas de URL, listas de equipamentos comprometidos, volume global de trafego, histórico dos sites, dados de categorização de URLs e web crawlers;

4.1.2.13.11 A solução deve permitir atualização automática da lista de URLs categorizadas via internet por meio de base proprietária do fabricante do equipamento;

4.1.2.13.12 Deve possuir mecanismo segurança que analise em tempo real a presença de conteúdo malicioso nas páginas acessadas;

4.1.2.13.13 Deve possuir mecanismo que gere alertas via e-mail quando há uma tentativa excessiva a um site bloqueado. Este alerta será disparado quando atingido o

número de tentativas bloqueadas previamente pelo administrador para cada categoria;

4.1.2.13.14 Deve suportar o registro nos LOGs de informações das atividades dos usuários;

4.1.2.13.15 Deve suportar o registro/contabilização das atividades dos usuários que acessam a Internet. A solução deve possibilitar a geração de relatório gerencial por usuário contendo essas informações (URLs e aplicações acessadas, tempo utilizado no acesso por URL/aplicação);

4.1.2.13.16 Deve suportar métodos de manipulação de sites dinâmicos e sites web 2.0, ou seja, alterar seu comportamento de acordo com o conteúdo específico divulgado pelo site;

4.1.2.13.17 Deve permitir o armazenamento em cache, a fim de melhorar a performance do acesso à internet.

4.1.2.14 **Das funcionalidades de DLP (Data Loss Prevention).**

4.1.2.14.1 A solução deve prover funcionalidades para proteção contra perda e vazamento de informações sensíveis à organização, de modo a impedir a saída de arquivos e informações da rede interna, o qual deverá funcionar para redes ou zonas de segurança;

4.1.2.14.2 Deve permitir a criação de regras com filtros que identifiquem e bloqueiem a transferência de arquivos pelo seu tipo, incluindo, mas arquivos do MS-Office, PDF entre outros;

4.1.2.14.3 As regras de que trata o item anterior devem ser capazes de inspecionar os seguintes tipos de aplicação: *instant messaging*, SMB, entre outras;

4.1.2.14.4 As regras de que trata o item 4.1.2.14.2 devem ser capazes de inspecionar os seguintes tipos de protocolo: HTTP, SMTP e FTP;

4.1.2.14.5 As regras de que trata o item 4.1.2.14.2 devem ser capazes de inspecionar tráfego HTTPS;

4.1.2.14.6 A solução deve permitir a identificação e o bloqueio de informações sensíveis como número de cartão de crédito;

4.1.2.14.7 A solução deve permitir a criação de novos tipos de dados para monitoramento e eventual bloqueio da transferência;

4.1.2.14.8 Deve suportar a identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses arquivos;

4.1.2.14.9 Deve possibilitar a criação de políticas de DLP por usuário/grupos de usuários do LDAP/Active Directory;

4.1.2.14.10 A solução deve prover interface para visualização do número de incidentes de DLP ou Filtro de Dados;

4.1.2.14.11 Será permitido que a funcionalidade de Data Loss Prevention seja fornecida em appliance separado.

4.1.3 Da Solução para Balanceamento (item 2 da tabela 3.1)

4.1.3.1 A solução de a que se refere este item terá por finalidade prover o balanceamento entre os appliances de Next generation Firewall, de modo a permitir que seus throughputs, suas capacidades de análise, capacidades de inspeção bem como todas as funcionalidades pedidas no item 4.1.2 e seus subitens sejam somados;

4.1.3.2 A solução de balanceamento deve permitir que a solução de NG Firewall se torne escalável;

4.1.3.3 A solução deve suportar a orquestração entre appliances de modelos diferentes, do mesmo fabricante, de modo a prover a escalabilidade ao longo do tempo.

4.1.3.4 A solução de balanceamento deverá ser fornecida em appliances físicos;

4.1.3.4.1 Os appliances deverão vir acompanhados de todos os conectores, cabeamento e peças de fixação no Rack, necessários à sua instalação e funcionamento, conforme as especificações deste Termo de Referência.

4.1.3.5 A solução deverá ser provida de forma redundante, de modo que se houver a falha de uma delas, a outra possa assumir totalmente o controle, sem que haja perda do tráfego;

4.1.3.6 A solução deve ser capaz de organizar os appliances de NG Firewall em grupos de segurança, nos quais os appliances de NG Firewall atuarão com seus recursos somados;

4.1.3.7 Cada Grupo de Segurança deverá comportar, no mínimo, 8 (oito) appliances;

4.1.3.8 A solução deverá ser capaz de suportar, no mínimo, 4 (quatro) grupos de segurança;

4.1.3.9 A solução deverá ser capaz de conectar, no mínimo, 24 (vinte e quatro) appliances Next Generarion Firewall a 10 Gbps com interfaces 10GBase-SR do tipo SFP+ e 4 Appliances a 100 Gbps de forma redundante.

4.1.3.10 A solução deverá possuir no mínimo 06 (seis) interfaces de rede 10/100/1000BaseT com portas de cobre, do tipo UTP (RJ-45);

4.1.3.11 A solução de balanceamento deverá ser acompanhada de, no mínimo 8 (oito) transceptores para conectar os appliances NGFirewall;

4.1.3.12 A solução deverá possuir a quantidade de transceptores suficientes para conectar toda a solução à rede corporativa, o que inclui a gerência.

4.1.4 Do Gerência Centralizada (item 3 da tabela 3.1).

4.1.4.1 A solução de que trata este item deverá ser fornecida em dois appliances que funcionaram de forma redundante, Ativo-Ativo ou Ativo-Passivo;

4.1.4.2 Serão aceitas soluções em máquina virtual desde que sejam fornecidos junto, no mínimo 2 (dois) servidores capazes de suportar sua operação.

4.1.4.2.1 Os servidores de que trata o item anterior devem poder serem instalados em rack bastidor 19”;

4.1.4.2.2 Devem possuir 4 interfaces Ethertnet 10 Gigabits, compatíveis com o padrão IEEE 802.3ae sendo acompanhadas dos respectivos transceivers;

4.1.4.2.3 Devem possuir 4 (quatro) interfaces 100/1000Base-TX em conformidade como o padrão IEEE 802.3ab.

4.1.4.3 A solução deve permitir a gerência centralizada de todos os equipamentos e contextos virtuais que compõe a solução em uma única interface de gerenciamento;

4.1.4.4 Deverá permitir a criação de até 8 grupos de appliances NGF, os quais atuarão em perímetros de rede distintos.

4.1.4.5 Cada grupo de appliances, a que se refere o item anterior, deverá comportar, no mínimo, 8 (oito) appliances NGF, de modo a somar suas capacidades;

4.1.4.6 A interface de gerenciamento deverá ser capaz de gerenciar todos os perímetros de segurança compostos pelos equipamentos da solução;

4.1.4.7 A gerência centralizada deve ser fornecida em equipamentos separados dos appliances de segurança e dedicados a este fim;

4.1.4.8 A gerência centralizada da solução deverá ser ofertada por meio de 2 (dois) appliances específicos do mesmo fabricante da solução;

4.1.4.9 A Gerência centralizada deverá possuir o mínimo de 4TB (quatro terabytes) de área de armazenamento disponível em disco com RAID 1 ou RAID 10;

4.1.4.10 O Appliance deverá ter altura máxima de 2U e compatível com instalação em rack bastidor de 19" (dezenove polegadas) e deverá vir acompanhado de todos os acessórios para tal instalação, incluindo trilho e suporte articulado para cabos;

4.1.4.11 Fonte de alimentação com controle automático de tensão e com potência que não limite o desempenho dos processadores, acompanhada de mais uma fonte de igual capacidade, com características redundantes, e que possua tecnologia "Hot Pluggable". Deverão admitir operação considerando 110 V monofásico (F+N+T) ou 220 V bifásico (F+F+T), com variação de tensão de +/- 10%, 50-60 Hz, sem nenhum tipo de adaptação ou conversão externa;

4.1.4.12 A gerência centralizada deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede;

4.1.4.13 Deve permitir localizar, a partir de sua interface gráfica, onde está sendo utilizado determinado objeto de rede na base de regras;

4.1.4.14 A gerência centralizada deve permitir o gerenciamento das regras de segurança, configuração da arquitetura da solução, configuração de políticas de segurança, visualização de LOGs, geração de relatórios, correlação de eventos e captura de pacotes;

4.1.4.15 Além das funções de configuração a gerência centralizada da solução deverá operar também como um console de monitoramento visualização de gráficos, estatísticas e LOGs bem como a geração de relatórios do estado de funcionamento da solução, das atividades e dos eventos de segurança;

4.1.4.16 Deve informar a utilização dos recursos de CPU, memória e atividade de rede dos equipamentos que compõem o *cluster*;

4.1.4.17 Deve informar o número de conexões simultâneas e de novas conexões por segundo dos equipamentos que formam o *cluster*;

4.1.4.18 Deve estar licenciada, se necessário, para o limite máximo de usuários, objetos, regras de segurança, NAT e endereços IP suportados pela solução;

4.1.4.19 Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução;

4.1.4.20 O acesso para gerenciamento da solução deve suportar conexão via SSH, cliente específico ou WEB (via HTTPS);

4.1.4.21 Caso seja necessário a instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows (Windows 7 e superior);

4.1.4.22 Deve ser capaz de testar a conectividade dos equipamentos gerenciados;

4.1.4.23 Deve permitir o acesso/autenticação de usuários administradores via consulta a grupos de usuários LDAP/Active Directory;

4.1.4.24 Deve registrar e manter LOGs de auditoria referente às ações dos administradores;

4.1.4.25 Deve permitir visualizar a data/hora do último acesso dos administradores, bem como tentativas de acesso que falharam;

4.1.4.26 Deve implementar acesso à gerência baseado em perfil de usuário com, no mínimo, dois perfis: perfil para criar/alterar configurações e regras e perfil somente leitura;

4.1.4.27 Deve permitir o acesso de mais de um administrador ao mesmo tempo;

4.1.4.28 Deve permitir a delegação de funções de administração;

4.1.4.29 Deve permitir que os administradores, ao acessarem ao mesmo tempo a gerência, façam modificações, validem e revertam as configurações da solução simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;

4.1.4.30 Deve suportar o bloqueio de alterações nas configurações e regras, evitando o conflito de configurações entre diferentes administradores efetuando alterações simultaneamente;

4.1.4.31 Deve permitir a criação e distribuição de regras de segurança de forma centralizada;

4.1.4.32 A gerência centralizada deve permitir a criação e administração de regras de firewall e de controle de aplicação, bem como a criação e administração de regras de IPS, Antivírus e *Antispyware*;

4.1.4.33 Deve permitir a criação e administração de regras de filtro de *Web* (URL);

4.1.4.34 Deve suportar a identificação e utilização de usuários nas regras de segurança via integração/consulta à base de usuários do LDAP/Active Directory;

4.1.4.35 A solução deve possuir uma política unificada para criação de regras de controle de acesso que permita a criação de uma base de regras simples e granular combinando os principais recursos de controle de acesso tais como: Firewall, Controle de Aplicação, Filtro *Web*, Controle de aplicação, VPN e Identificação de Usuários;

4.1.4.36 Deve permitir monitoramento e pesquisa de logs (de acesso à gerência e de tráfego de usuários);

4.1.4.37 Deve prover meios/interface para monitoramento detalhado (*debugging*) do tráfego inspecionado;

4.1.4.38 Deve prover meios/interface para captura de pacotes;

4.1.4.39 Deve possibilitar a criação de regras para um determinado horário ou período de tempo (dia, mês, ano, dia da semana e hora);

4.1.4.40 Deve possuir funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes;

4.1.4.41 Deve permitir validar as regras antes de aplicá-las, exibindo eventuais inconsistências;

4.1.4.42 Deve possuir funcionalidade de validação de novas regras de inspeção antes de aplicá-las, avisando quando houver regras que ofusquem ou conflitem com outras regras já aplicadas;

4.1.4.43 Deve suportar "*rollback*" de configuração para a última configuração salva;

4.1.4.44 Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução;

4.1.4.45 Deve permitir a visualização e comparação das configurações atual, anterior e antigas (histórico de alterações);

4.1.4.46 Deve suportar agrupamento lógico de objetos para criação de regras;

4.1.4.47 Deve contabilizar a utilização das regras de segurança ("*hit counts*") individualmente;

4.1.4.48 Deve contabilizar o volume de dados trafegado correspondente a cada regra de segurança individualmente;

4.1.4.49 Deve permitir a identificação e exclusão de regras sem uso (regras com zero *hit count*);

4.1.4.50 Deve suportar a geração de alertas automáticos via e-mail, SNMP ou syslog;

4.1.4.51 Não deve ter limites diários para armazenamento de logs;

4.1.4.52 Deve gerar relatórios de utilização dos recursos por aplicação, URLs, ameaças, etc.;

4.1.4.53 Deve gerar relatórios de volume de conexões que foram bloqueadas pela solução;

4.1.4.54 Deve gerar relatórios com as principais fontes de conexões bloqueadas, suas origens, destinos e serviços/aplicações;

4.1.4.55 Deve permitir a personalização ou customização de relatórios;

4.1.4.56 Deve permitir a criação de relatórios com filtros de: endereço IP de origem, endereço IP de destino, usuário, máquina do domínio;

4.1.4.57 Deve permitir a criação de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego inspecionado;

4.1.4.58 Deve permitir a geração de relatórios em formato PDF;

4.1.4.59 Deve permitir a geração de relatórios com as principais aplicações por utilização de largura de banda;

4.1.4.60 Deve permitir a geração relatórios com os principais hosts por número de ameaças identificadas/bloqueadas;

4.1.4.61 Deve permitir a geração de relatório detalhando as atividades de um usuário ou grupo de usuários do Active Directory/LDAP, incluindo aplicações acessadas, categorias de URL, tempo de utilização por aplicação, tempo de utilização por URL/Categoria;

4.1.4.62 Deve permitir a geração de relatórios através da interface gráfica onde contenha no mínimo as seguintes informações: tipo de *malware*, identificador de evento, extensão do arquivo inspecionado, severidade da ameaça, horário do último evento, IP de origem, IP de destino e nome do usuário infectado de acordo a base do LDAP/Active Directory;

4.1.4.63 Deve permitir o envio automático de relatórios por e-mail através de agenda predeterminada (periodicidade diária, semanal e mensal);

4.1.4.64 Deve permitir a geração de relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, antivírus e *antispyware*), usuários, etc;

4.1.4.65 Deve correlacionar logs de filtro de conteúdo Web (URL *Filtering*), logs de ameaças (IPS, antivírus, *antispyware*, Sandbox) para identificar indicadores de compromissos e destacar hosts infectados com base em seu comportamento;

4.1.4.66 Deve prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e *antispyware*), e URLs que passaram pela solução;

4.1.4.67 Deve possibilitar a visualização e a geração de relatório de hosts infectados, do tipo “sumário executivo”, com possibilidade de customização para apresentação corporativa/gerencial;

4.1.4.68 Deve possuir interface para visualização gráfica de informações como: ameaças identificadas, bytes enviados e recebidos por interface, por zona de segurança, por aplicações, por categorias de URL, etc;

4.1.4.69 Deve possuir mecanismo do tipo "*drill-down*" para navegação nos relatórios em tempo real;

4.1.4.70 Deve permitir a criação de “*dashboards*” customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, *antispyware*, *malwares* do tipo "Zero Day" detectados em *sandbox* e tráfego bloqueado;

4.1.4.71 Dever permitir a visualização dos logs de *malwares* modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, *antispyware*, Filtro Web e filtro de arquivos;

4.1.4.72 Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório deve mostrar o consumo de aplicações por usuário e grupos de usuários;

4.1.4.73 Deve possuir relatório e/ou interface para visualização de eventos, permitindo sumarização de informações contendo: IP de origem mais utilizada, IP de destino mais utilizado, regras de segurança mais utilizadas, aplicações/categorias de aplicações mais utilizadas, URLs/Categorias de URL mais utilizadas, usuários/grupos de usuários com maior atividade/maior tráfego contabilizado;

4.1.4.74 Deve ser possível exportar os LOGs em formato CSV;

4.1.4.75 Deve permitir a visualização das seguintes informações em tempo real (com atualização automática a cada minuto): situação de cada equipamento do *cluster*, principais aplicações, administradores autenticados na gerência, número de sessões simultâneas, status das interfaces, uso de CPU;

4.1.4.76 Deve possuir visualização sumarizada de todas as aplicações, ameaças e URLs que foram identificadas e controladas pela solução;

4.1.4.77 Deve possibilitar a filtragem dos logs gerados pela solução por, no mínimo: usuário, tipo de aplicação, endereço IP de origem e destino, país de origem e destino, horário;

4.1.4.78 Deve possuir funcionalidade de visualização e monitoramento de Log em tempo real;

4.1.4.79 Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de conexões bloqueadas com seus destinos e serviços, os mais frequentes ataques e ameaças de segurança detectados com suas origens e destinos, os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet, os usuários maiores consumidores de banda de Internet, os sítios na Internet mais visitados;

4.1.4.80 Deve permitir a geração automática e agendada dos relatórios;

4.1.4.81 Deve possuir mecanismo de pesquisa global na base de regras da 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 do mesmo na configuração do dispositivo;

4.1.4.82 Deve suportar o monitoramento via SNMP de falhas de hardware, inserção ou remoção de fontes, discos, utilização de CPU, utilização de memória, utilização de discos, número de túneis VPN *client-to-site* estabelecidos, número de sessões estabelecidas;

4.1.4.83 Deve atribuir automaticamente um número ("id") a cada nova regra de firewall, NAT, QoS, inspeção SSL e demais regras de inspeção de tráfego;

4.1.4.84 Deve permitir criação de regras com data de expiração.

4.2 Requisitos Externos

4.2.1 A CONTRATADA obedecerá aos critérios de gestão ambiental estabelecido nas legislações, normas e regulamentos específicos ao serviço, visando à melhoria e ao desempenho dos processos de trabalho quanto aos aspectos ambientais, sociais e econômicos.

4.2.2 A CONTRATADA deverá, em suas atividades, atender a legislação federal, estadual, municipal, normas e regulamentos em vigor.

4.2.3 As atividades desempenhadas pela CONTRATADA devem ser conduzidas considerando a preservação, conservação e a recuperação do ecossistema, desenvolvendo suas ações de forma a valorizar o bem-estar dos trabalhadores, promovendo a qualidade de vida.

4.2.4 A CONTRATADA deverá estabelecer ações de forma a promover o desenvolvimento das regiões previstas na execução do contrato, gerando benefícios e minimizando os impactos negativos, sociais, ambientais e econômicos.

4.2.5 A contratada deverá obedecer às determinações do PGRS (Plano de Gerenciamento de Resíduos Sólidos), e de seus desdobramentos como o PGRSS, o PGRCC, entre outros, do PJERJ.

4.2.6 A contratada deve realizar suas atividades de modo a minimizar os impactos negativos e potencializar os impactos positivos sobre a flora e a fauna, preservando e recuperando ecossistemas locais.

4.2.7 Os serviços de suporte técnico deverão respeitar no que couber, as normas e procedimentos de Segurança da Informação em vigor no ambiente operacional do PJERJ e, ainda, os seguintes dispositivos legais:

4.2.7.1 Lei Federal nº 8.666/93;

4.2.7.2 Lei Federal nº 10.520/02;

4.2.7.3 Ato Normativo PJERJ nº 9/2010;

4.2.7.4 Ato Normativo PJERJ nº 6/2014;

4.2.7.5 Ato Normativo PJERJ nº 10/2018;

4.2.7.6 Ato Normativo PJERJ nº 3/2019;

4.2.7.7 Ato Normativo PJERJ nº 8/2019;

4.2.7.8 Ato Executivo PJERJ nº 5298/2013;

4.2.7.9 Resolução CNJ nº 182/2013;

4.2.7.10 Portaria nº 317 do INMETRO, de 19/06/2012.

5. MODELO DA PRESTAÇÃO DE SERVIÇO / FORNECIMENTO DE BENS

5.1 Metodologia de Trabalho

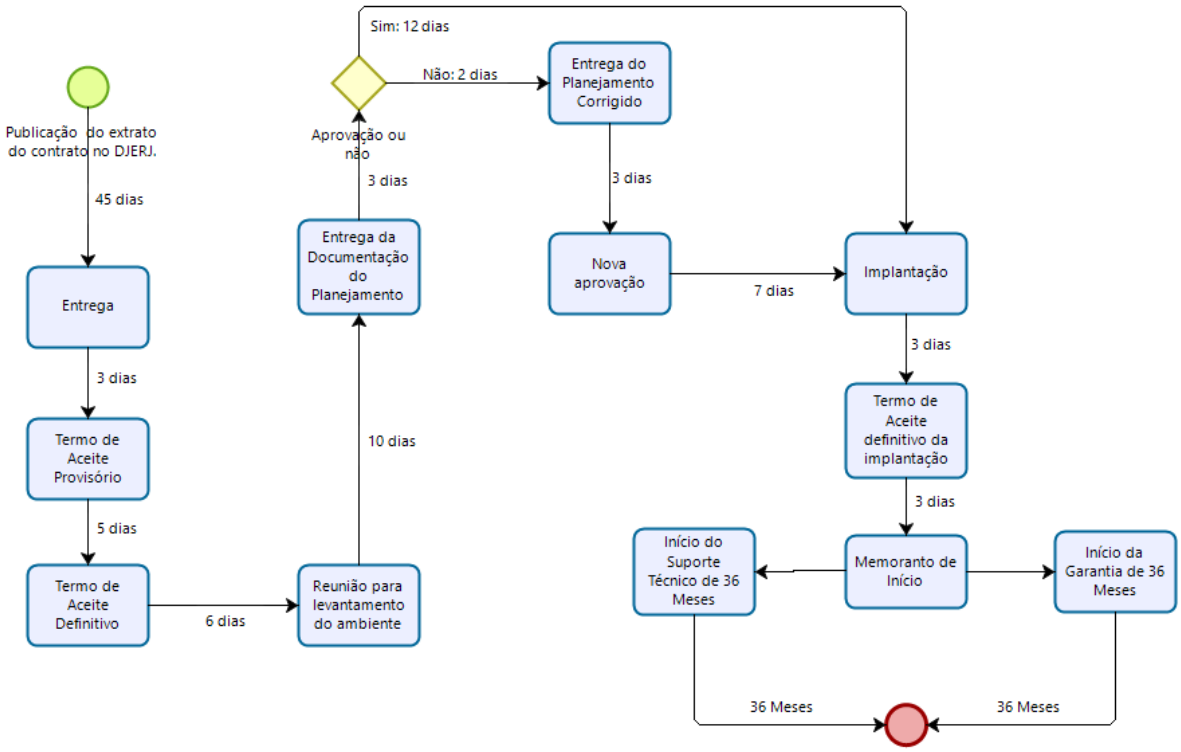
Item	Bem / Serviço	Forma de Fornecimento	Justificativa
1	APPLIANCES NEXT GENERATION FIREWALL	Integral	Adequar a capacidade de proteção ao ambiente tecnológico e a usuários à nova realidade de consumo de tráfego, utilização de VPN, bem como novas necessidades de proteção.
2	SOLUÇÃO DE BALANCEAMENTO PARA OS NG FIREWALLS	Integral	Prover a capacidade de escalonamento da solução, de modo a permitir que os recursos dos appliances sejam somados, além de prover redundância.

3	SOLUÇÃO DE GERÊNCIA CENTRALIZADA	Integral	Permitir, desde o início do funcionamento da solução, que seja realizada a gerência de forma eficiente, de modo a prover uma segurança eficaz para o ambiente.
4	SERVIÇO DE IMPLANTAÇÃO DA SOLUÇÃO	Integral durante o período definido para a implantação	Permitir uma implantação de forma segura, de modo a minimizar os riscos ao ambiente tecnológico.
5	SERVIÇO DE SUPORTE TÉCNICO	Serviços contínuos durante 36 (trinta e seis) meses	Garantir a correção de falhas e atualização de versão a contar do Memorando de início.
6	SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO	Por hora, sob Demanda no limite de 300 (trezentas) horas.	Garantir a assistência para implementação de melhorias no projeto original, a contar do memorando de início dos serviços.
7	SERVIÇO DE TREINAMENTO OFICIAL DA SOLUÇÃO	1(uma) turma de 4 (quatro) alunos	Permitir capacitação em conjunto com melhor absorção das informações
8	SERVIÇO DE GARANTIA	Serviços contínuos durante 36 (trinta e seis) meses	Garantir a atualização da solução e a substituição de equipamentos e/ou peças defeituosos. Todas as substituições de hardware e software (referente aos itens 1, 2 e 3 da tabela 3.1), deverão ter garantia de, no mínimo, de 36 (trinta e seis) meses, a contar da emissão do memorando de início que deverá ser emitido em até 3 (três) dias do Termo de Aceite Definitivo da Implantação, garantindo as atualizações de software, bem como as atualizações pertinentes às versões subsequentes.

5.1.1 Forma de Execução / Fornecimento

5.1.1.1 A execução do objeto será realizada no regime de empreitada por preço global para os itens 4, 5 e 8 e empreitada por preço unitário para os itens 6 e 7, todos da tabela 3.1.

5.1.1.2 A dinâmica da execução seguirá o fluxo abaixo cujos prazos estão expressos em dias corridos:



5.1.1.3 **Da entrega dos componentes da solução.**

5.1.1.3.1 Os Componentes da Solução (Appliances e demais acessórios), bem como qualquer componente da solução de gerência e balanceamento deverão ser entregues, nas dependências da Divisão de Redes do Departamento de Infraestrutura da Diretoria de Tecnologia do Poder Judiciário do Estado do Rio de Janeiro, situado na Av. Erasmo Braga 115, sala 111, corredor C da Lâmina I;

5.1.1.3.2 Todos os componentes e demais acessórios constantes dos itens da tabela 3.1 deverão ser entregues em até 45 (quarenta e cinco) dias corridos, contados da data de publicação do extrato do contrato no Diário da Justiça Eletrônico;

5.1.1.3.3 A CONTRATADA deverá se responsabilizar pela desembalagem, verificação e conferência dos itens que compõem a solução tecnológica adquirida: hardwares e acessórios, conforme especificados neste Termo de Referência, sempre acompanhada de responsável técnico designado pela CONTRANTANTE;

5.1.1.3.4 Será fornecido o aceite provisório em até 03 (três) dias corridos após a verificação dos equipamentos;

5.1.1.3.5 O Termo de Aceite Definitivo da Entrega dos Equipamentos será fornecido em até 5 (cinco) dias corridos após o termo de aceite provisório da entrega dos equipamentos conforme item acima, mediante à verificação e conferência;

5.1.1.3.6 Após a conferência referida no item 5.1.1.3.3, os itens que compõem a solução tecnológica deverão ser acomodados novamente em suas respectivas embalagens e estas deverão ser lacradas na presença do preposto da CONTRATADA e responsável técnico da CONTRATANTE, somente sendo desembalados quando da data da efetiva implantação da solução tecnológica.

5.1.1.4 **Do serviço de Implantação (Item 4 da tabela 3.1).**

5.1.1.4.1 O serviço de implantação consiste nas seguintes ações:

5.1.1.4.1.1 Reuniões de alinhamento e planejamento;

5.1.1.4.1.2 Instalação e substituição física dos equipamentos atuais;

5.1.1.4.1.3 Configuração dos equipamentos para a operação no ambiente;

5.1.1.4.1.4 Migração das regras e demais configurações atualmente existentes;

5.1.1.4.1.5 Instalação/configuração da gerência centralizada e balanceamento dos NG Firewalls;

5.1.1.4.1.6 Qualquer outra ação necessária ao correto funcionamento da totalidade solução conforme exigido neste termo de referência.

5.1.1.4.2 O serviço deverá ser prestado nas dependências do Data Center do Poder Judiciário do Estado do Rio de Janeiro, localizado no Palácio da Justiça, na Av.

Erasmo Braga 115, corredor C, Sala 111, sob a supervisão de técnicos do Serviço de Segurança de Redes – SESER, e Serviço de Rede Corporativa, ambos da Divisão de Redes.

5.1.1.4.3 Em até 06 (seis) dias corridos, após a emissão do termo de aceite definitivo da entrega, a CONTRATADA deverá reunir-se com a equipe técnica da CONTRATANTE para levantamento do ambiente e alinhamento de informações visando ao planejamento da implantação da solução adquirida;

5.1.1.4.4 No prazo de até 10 (dez) dias corridos contados da data da realização da reunião referida no item anterior, deverá ser entregue, pela CONTRATADA, documentação com o planejamento para realização da implantação da solução, que deverá ser validada e aprovada pela equipe técnica da CONTRATANTE;

5.1.1.4.4.1 A documentação com o planejamento deverá conter, no mínimo, as ações necessárias à implantação, os técnicos que irão realizá-las, a previsão de tempo estimado por ação, o plano de Rolback, as premissas para a implantação e as ações necessárias por parte do CONTRATANTE;

5.1.1.4.4.2 Deverá ser entregue paralelamente um plano de manutenções preventivas, no qual deverá constar, no mínimo, a periodicidade recomendada (a qual não deverá ser superior a 6 meses), as ações a serem realizadas para a verificação da saúde do equipamento, as ações necessárias para atualização dos equipamentos, as premissas e as ações necessárias por parte da CONTRATANTE;

5.1.1.4.5 A equipe técnica da CONTRATANTE terá até 3 (três) dias corridos, contados da entrega da documentação com o planejamento para realização da implantação da solução para validação e aprovação deste planejamento, data na qual deverá ser avaliado o planejamento de manutenções preventivas.

5.1.1.4.6 Após a aprovação, a CONTRATADA deverá realizar a implantação no prazo de 12 (doze) dias corridos.

5.1.1.4.7 No caso de a equipe técnica da CONTRATANTE não validar e aprovar o plano de implantação, a CONTRATADA terá até 2 (dois) dias corridos, contados da data

desta informação, para proceder às correções e ajustes necessários e a CONTRATANTE mais 3 (três) dias corridos para sua aprovação;

5.1.1.4.8 Após a aprovação do plano de implantação corrigido, a CONTRATADA deverá realizar a implantação no prazo de 7 (sete) dias corridos;

5.1.1.4.9 Da documentação para planejamento da implantação deverá constar plano de contingência (rollback) para o caso de insucesso da migração;

5.1.1.4.10 O plano de implantação deverá ser executado na próxima Janela de Manutenção autorizada para este fim pela DGTEC;

5.1.1.4.11 No caso de não ser possível a execução da migração da solução tecnológica na Janela de Manutenção, conforme estabelecida no item anterior, esta deverá ser realizada impreterivelmente na próxima Janela que se seguir;

5.1.1.4.12 A CONTRATADA deverá implantar e testar os equipamentos ofertados, contemplando, no mínimo, as seguintes atividades:

5.1.1.4.12.1 Completa Instalação, implantação, configuração, migração, testes e ajustes em produção de toda a solução ofertada;

5.1.1.4.12.2 Análise preliminar da topologia e operação da solução de CONTRATANTE em funcionamento anteriormente à migração;

5.1.1.4.12.3 Documentação de todas as atividades contempladas no processo de migração da solução a ser entregue em meio impresso e digital no formato PDF.

5.1.1.4.13 A finalização da implantação deverá ocorrer em até 31 (trinta e um) dias corridos contados do termo de aceite definitivo da entrega dos equipamentos;

5.1.1.4.14 O Aceite Definitivo da Implantação ocorrerá em até 3 (três) dias corridos do fim da implantação com sucesso;

5.1.1.4.15 A implantação será considerada com sucesso depois de verificada a estabilidade do ambiente tecnológico em funcionamento com a nova tecnologia;

5.1.1.4.16 Três dias após a emissão do Termo de Aceite Definitivo da Implantação, será assinado o Memorando de Início da Contratação.

5.1.1.5 **Do Suporte Técnico (item 5 da tabela 3.1).**

5.1.1.5.1 O Suporte técnico a ser fornecido pela CONTRATADA, pelo prazo de 36 (trinta e seis) meses, terá início a contar da assinatura do memorando de início e incluirá as manutenções corretivas e preventivas necessárias ao bom funcionamento da solução;

5.1.1.5.2 Entende-se como manutenção preventiva, toda e qualquer ação de monitoramento, controle e atualização da solução com o objetivo de reduzir ou impedir falhas no desempenho e/ou funcionamento regular da solução como um todo;

5.1.1.5.2.1 A Manutenção preventiva deverá ser realizada periodicamente em intervalos não superiores a 6 (seis) meses, com o primeiro marco contado a partir da assinatura do memorando de início;

5.1.1.5.2.2 A manutenção preventiva deverá ser precedida de um plano contendo as ações a serem realizadas nos equipamentos, o qual deverá ser aprovado pelo fiscal do contrato.

5.1.1.5.3 Entende-se como manutenção corretiva a recuperação de falhas que levam a solução a uma degradação ou parada na sua operação.

5.1.1.5.4 Faz parte da manutenção corretiva a identificação da necessidade de substituição de hardware ou outro componente da solução, a qual deverá ocorrer pela garantia da solução, segundo o item 6.11.4;

5.1.1.5.5 A CONTRATADA deverá fornecer suporte telefônico gratuito do tipo 0800, em regime 24x7 (vinte e quatro horas por dia, sete dias por semana), 365 dias ao ano para resolução de problemas técnicos;

5.1.1.5.6 A abertura do chamado para suporte técnico ocorrerá por e-mail ou telefone, devendo a CONTRATADA efetuar o registro em até 10 (dez) minutos;

5.1.1.5.7 A CONTRATADA deverá fornecer ao contratante, informes periódicos de acompanhamento do progresso do reparo, com intervalo não superior a 30 (trinta) minutos, bem como, indicar um telefone de contato ou outro meio de comunicação pelo qual o contratante possa obter informações quanto ao andamento do chamado e a previsão de solução do problema.

5.1.1.5.8 Os problemas reportados para o suporte técnico serão classificados de acordo com seu grau de severidade, segundo a seguinte classificação:

5.1.1.5.8.1 Severidade 1: Interrupção total ou degradação dos sistemas corporativos, tornado indisponível a sua utilização pelos usuários;

5.1.1.5.8.2 Severidade 2: degradação parcial do desempenho dos sistemas corporativos, tornando os seus tempos de resposta inviáveis para uso eficiente pelos usuários;

5.1.1.5.8.3 Severidade 3: Perda de funcionalidade ou configuração, que não inviabilize ou torne indisponível o uso dos sistemas corporativos pelo usuário, sendo de fácil e rápida correção.

5.1.1.5.9 O prazo para o início do atendimento remoto e solução do problema deve ser específico para cada grau de severidade, segundo a seguinte classificação:

5.1.1.5.9.1 Severidade 1: iniciar o atendimento em até 15 (quinze) minutos, após a abertura do chamado pelo contratante, com resolução do problema em até 2 (duas) horas contados da abertura;

5.1.1.5.9.2 Severidade 2: iniciar o atendimento em até 30 (minutos), após a abertura do chamado pelo contratante, com resolução do problema em até 4 (quatro) horas contados da abertura;

5.1.1.5.9.3 Severidade 3: Iniciar o atendimento em até 60 (sessenta) minutos, após a abertura do chamado pelo contratante, com resolução do problema em até 24 (vinte e quatro) horas contados a partir da abertura.

5.1.1.5.10 Os prazos estabelecidos, quando não respeitados são passíveis de descontos, pela sua não observância, podendo ser prorrogados em situações excepcionais, a critério do contratante, mediante justificativa técnica apresentada pela CONTRATADA;

5.1.1.5.11 Para chamados de Severidade 1 e 2, atendidos remotamente e não resolvidos no prazo máximo estipulado, o contratante, a seu critério, poderá exigir que a CONTRATADA atenda ao chamado de forma presencial, nas instalações do contratante, com prazo máximo de solução de 24 (vinte e quatro) horas corridas,

contadas a partir do término do prazo original de solução do chamado, sem prejuízo para eventual aplicação de desconto por descumprimento do nível mínimo de serviço contratado;

5.1.1.5.12 Caso este prazo de 24 (vinte e quatro) horas corridas também não seja cumprido, o desconto pelo chamado originalmente não atendido será dobrado;

5.1.1.5.13 Para serviços de severidade 1 e 2, diante da complexidade do problema, a CONTRATADA poderá indicar em até 1 (uma) hora, a contar do fim do prazo para início do atendimento, a necessidade de executar uma solução de contorno (provisória), bem como solicitar ao contratante prazo para implementação desta solução de contorno (provisória) e novo prazo para a solução definitiva, que dependerá de aprovação do contratante;

5.1.1.5.14 Os prazos e descontos são aplicados em relação à solução definitiva, até que seja indicada a necessidade de uma solução de contorno (provisória);

5.1.1.5.15 Os descontos são aplicados de forma subsequente, no caso de atraso na indicação da solução de contorno aprovada (nesta hipótese incidindo o desconto previsto para a solução definitiva), descumprimento do prazo de implementação da solução de contorno (provisória) e também no caso de descumprimento do novo prazo da solução definitiva;

5.1.1.5.16 No caso de ser indicada solução de contorno após o descumprimento do prazo para a solução definitiva incidirão os descontos previstos para descumprimento de prazo da solução definitiva até esta data e se descumprido o prazo para a implementação da solução provisória será acrescido este, bem como também acrescido o desconto se descumprido o novo prazo para a solução definitiva;

5.1.1.5.17 Não haverá aceite provisório no serviço de suporte, exceto nos casos em que houver solução de contorno (provisória), quando o aceite provisório se dará na data em que o contratante considerou satisfatória a implementação da solução de contorno (provisória);

5.1.1.5.18 O aceite definitivo do serviço de suporte técnico ocorrerá na data em que o contratante considerou satisfatória a implementação da solução definitiva;

5.1.1.5.19 Mensalmente, até o 5º dia útil do mês, a CONTRATADA deverá apresentar relatório detalhado, com consolidação final, demonstrando todos os atendimentos realizados no mês anterior, caso haja, os resultados atingidos e os descumpridos, as datas dos aceites definitivos e os eventuais descontos aplicados;

5.1.1.5.20 O contratante tem prazo de 5 (cinco) dias úteis para analisar o relatório de fechamento entregue pela CONTRATADA, bem como verificar o resultado alcançado e solicitar possíveis correções no relatório.

5.1.1.6 **Suporte Técnico Especializado (item 6 da tabela 3.1).**

5.1.1.6.1 Durante o período de vigência do contrato, a CONTRATADA deverá fornecer, Suporte Técnico Especializado por 36 (trinta e seis) meses, contados da data do memorando de início;

5.1.1.6.2 O suporte técnico especializado, será realizado sob demanda da CONTRATANTE, até o total de 300 (trezentas) horas, que serão distribuídas pelo contratante, considerando a complexidade, a dificuldade e a prioridade do projeto;

5.1.1.6.3 O contratante não está obrigado a utilizar a quantidade de horas estimada para esta contratação;

5.1.1.6.4 Os serviços serão requisitados pelo contratante, mediante a definição do escopo para cada atividade, conforme a demanda determinada pelo PJERJ;

5.1.1.6.5 O contratante poderá solicitar a substituição de técnicos indicados pela contratada, que não estejam utilizando a melhor técnica vigente, devendo a empresa indicar, como substituto, profissional técnico qualificado;

5.1.1.6.6 Antes do início de cada serviço, deverão ser realizadas 1 (uma) ou mais reuniões para planejamento da execução do serviço entre os representantes da contratada e contratante;

5.1.1.6.7 Após cada reunião a CONTRATADA deverá apresentar, no prazo de 5 (cinco) dias corridos, a ata da reunião que deverá ser aprovada pelo contratante;

5.1.1.6.8 O Suporte Técnico Especializado visa executar as seguintes ações:

5.1.1.6.8.1 Implantar melhorias operacionais;

5.1.1.6.8.2 Realizar atividades de análise, preparação, planejamento e acompanhamento de projetos a serem realizados pela CONTRATANTE e que envolvam à solução tecnológica adquirida;

5.1.1.6.8.3 Realizar procedimentos de instalação, configuração, atualização e ajustes de componentes de software e hardware;

5.1.1.6.8.4 Realizar o repasse de conhecimentos e esclarecimentos relacionados à solução tecnológica adquirida, sempre que demandados pela equipe técnica do CONTRATANTE;

5.1.1.6.9 O Suporte técnico especializado deverá ser solicitado mediante abertura de chamado, através de e-mail ou telefone tipo “0800” a ser fornecido pela CONTRATADA;

5.1.1.6.10 Quando solicitada, a CONTRATADA deverá elaborar o planejamento e o cronograma de execução do serviço, dentro do prazo de 10 (dez) horas úteis;

5.1.1.6.11 Hora útil é a hora trabalhada nas dependências do contratante ou remotamente com autorização deste;

5.1.1.6.12 Em caso de o planejamento ser feito remotamente, o tempo de planejamento consumido será de 10 (dez) horas;

5.1.1.6.13 Será emitido o Termo de Aceite Definitivo do Suporte Técnico Especializado, a cada projeto realizado e aprovado pelo CONTRATANTE, após verificação de atendimento dos objetivos pretendidos.

5.1.1.7 **Treinamento Oficial na Solução (item 7 da tabela 3.1).**

5.1.1.7.1 A CONTRATADA deverá fornecer para 1 (uma) turma de 4 (quatro) participantes, o treinamento oficial na solução, contemplando a sua operação e gerenciamento;

5.1.1.7.2 Uma vez solicitado, a CONTRATADA terá o prazo de 30 dias para organizar o treinamento;

5.1.1.7.3 Somente os treinamentos poderão ser objeto de subcontratação, desde que fornecido por empresa especializada e licenciada para tal;

5.1.1.7.4 Os instrutores deverão ser credenciados pelo fabricante da solução;

5.1.1.7.5 A carga horária para o treinamento oficial da solução não deverá ser inferior a 40 (quarenta) horas e deverá compreender os níveis básico, intermediário e avançado;

5.1.1.7.6 Será aceito treinamento oficial on-line e/ou eletrônico, desde que cumpra as exigências mínimas de carga horária, conteúdo e material didático, e que a CONTRATADA disponibilize um instrutor habilitado para esclarecer dúvidas dos participantes;

5.1.1.7.7 O material didático a ser fornecido, sem ônus para o contratante, deverá conter todas as informações, testes, exemplos e exercícios necessários ao bom acompanhamento das aulas, de modo que os participantes não necessitem de qualquer outro material de apoio;

5.1.1.7.8 O material didático deverá ser, preferencialmente, em português, podendo ser em inglês, na hipótese de fazer parte de um curso oficial das soluções tecnológicas e não exista material disponível em português;

5.1.1.7.9 O treinamento deverá abranger a utilização de toda a solução de gerência fornecida;

5.1.1.7.10 A CONTRATADA deverá fornecer todos os equipamentos necessários à realização dos treinamentos, como computadores ou qualquer outro equipamento necessário durante o andamento das aulas;

5.1.1.7.10.1 No caso de o treinamento for ministrado de forma on-line, embora não seja necessário o fornecimento de equipamentos físicos pessoais (computadores desktop, notebooks) deverá ser fornecido acesso à ambiente de operação da solução destinada a treinamentos.

5.1.1.7.11 As datas e horários de treinamento deverão ser previamente acordados com o CONTRATANTE;

5.1.1.7.12 Os treinamentos, quando presenciais, deverão ser ministrados na cidade do Rio de Janeiro;

5.1.1.7.13 A CONTRATADA deverá entregar certificados de participação para os alunos que concluírem o treinamento;

5.1.1.7.14 Ao fim do treinamento, será feita, por cada participante, uma avaliação para indicar se ele foi satisfatório ou insuficiente;

5.1.1.7.15 No caso de insatisfatório ou insuficiente o treinamento, este deverá ser ministrado novamente, sem ônus para o contratante, efetuando-se as melhorias e correções necessárias;

5.1.1.7.16 O treinamento será considerado satisfatório, quando a maioria absoluta dos participantes assim o considerarem;

5.1.1.7.17 A avaliação será realizada através de um formulário que será confeccionado pela contratada e deverá conter, no mínimo, nome, matrícula e a opção de satisfação com 2 (dois) indicadores, “sim” e “não”;

5.1.1.7.18 O formulário será entregue pela contratada aos participantes ao final do treinamento;

5.1.1.7.19 Cada participante devolverá o formulário, devidamente preenchido, ao instrutor da contratada;

5.1.1.7.20 A contratada deverá entregar, em até 3 (três) dias corridos do fim do treinamento (Treinamento Oficial da Solução), todos os formulários aos fiscais do contrato, a fim de que o termo de aceite provisório possa ser emitido;

5.1.1.7.21 Após o recebimento dos formulários de cada uma das turmas, o contratante terá o prazo de 3 (três) dias corridos para efetuar o aceite provisório;

5.1.1.7.22 O aceite definitivo do treinamento será dado no prazo máximo de 10 (dez) dias corridos, após fornecimento do aceite provisório e desde que já tenham sido entregues todos os certificados dos participantes dos treinamentos.

6. ELEMENTOS PARA GESTÃO DO CONTRATO

6.1 Papéis e Responsabilidades

Papel	Entidade	Responsabilidades
Fiscal Demandante	PJERJ-DGTEC	• Representar a Unidade Demandante do contratante, acompanhando a execução física do Contrato e seus aspectos funcionais;

Papel	Entidade	Responsabilidades
		• Informar ao Fiscal Técnico, para providências, quaisquer problemas no funcionamento da solução; • Zelar pelo fiel cumprimento do Contrato.
Fiscal Técnico	PJERJ-DGTEC	• Fiscalizar a execução física do Contrato quanto aos aspectos técnicos da solução, acompanhando, inclusive, a prestação de serviços relativos à garantia técnica; • Zelar pelo fiel cumprimento do Contrato; • Representar o contratante nas questões técnicas e operacionais do Contrato; • Prestar informações técnicas ao Gestor, para possibilitar a análise administrativa e financeira do Contrato; • Anotar em registro próprio todas as ocorrências relacionadas à execução do Contrato, informando a data e o nome dos profissionais eventualmente envolvidos, determinando o que for necessário à regularização das faltas ou defeitos; • Relatar, por escrito, ao Gestor qualquer fato que gere atraso ou impossibilidade de cumprimento do Contrato. • Solicitar a substituição de qualquer profissional da CONTRATADA que não corresponda ao desempenho das atribuições definidas no documento de referência ou cuja atuação, permanência ou comportamento sejam considerados prejudiciais, inconvenientes ou insatisfatórios à disciplina do CONTRATANTE, ao interesse público e/ou à segurança operacional; • Recusar o recebimento material, utensílio, ferramenta ou equipamento, ou solicitar a substituição daqueles que não sejam os especificados no contrato, que não atendam ao padrão de qualidade necessário ou na hipótese de entrega irregular. • O fiscal e o fiscal substituto, no prazo de 9 (nove) dias a contar da autuação, atestarão a nota fiscal apresentada pela CONTRATADA, após confrontar os valores e as quantidades constantes do documento com os estabelecidos no contrato,

Papel	Entidade	Responsabilidades
		bem como as medições dos serviços nas datas de referência.
Fiscal administrativo/Agente Administrativo	PJERJ-DGLOG	• Fiscalizar o Contrato quanto aos aspectos administrativos; • Zelar pelo fiel cumprimento do Contrato.
Gestor do Contrato	PJERJ-DGTEC	• Representar a Unidade Demandante do contratante acompanhando toda a execução do Contrato; • O gestor acompanhará a contratação em todas as suas fases, da elaboração à execução do contrato. • Planejar a contratação, supervisionar a elaboração do respectivo documento de referência e gerenciar o contrato vigente; • Zelar pelo fiel cumprimento do Contrato; • Representar o contratante nas questões administrativas e financeiras; • Prestar informações técnicas necessárias à análise administrativa e financeira do Contrato; • O gestor e/ou gestor substituto, na ausência do fiscal e fiscal substituto, no prazo de 9 (nove) dias a contar da autuação, atestará a nota fiscal apresentada pela CONTRATADA, após confirmada a execução do objeto contratado.
Preposto	CONTRATADA	• Representar a empresa CONTRATADA; • Acompanhar a execução do Contrato e atuar como principal interlocutor junto ao contratante, participando, inclusive, das reuniões para as quais for convocado; • Receber, diligenciar, encaminhar e responder às principais questões técnicas, legais e administrativas no curso da execução contratual.

6.2 Deveres e Responsabilidades do CONTRATANTE:

6.2.1 Prestar, por intermédio do Gestor do Contrato, ou quem por ele for designado, as informações e esclarecimentos pertinentes ao serviço contratado que venham a ser solicitados pela CONTRATADA;

6.2.2 Registrar os incidentes e problemas ocorridos durante a execução do contrato;

6.2.3 Analisar, mensalmente, o relatório do serviço, referente ao mês anterior, observando o cumprimento dos serviços exigidos, em até 7 (sete) dias úteis do seu recebimento, aplicando os descontos em caso de descumprimento.

6.2.4 Comunicar oficialmente à CONTRATADA quaisquer falhas verificadas na fiscalização do cumprimento dos serviços prestados.

6.2.5 Efetuar o pagamento devido à CONTRATADA pela execução dos serviços prestados, nos termos e prazos contratualmente previstos, após terem sido devidamente atestados e visados, de acordo com as normas vigentes.

6.2.6 Exercer permanente fiscalização na execução do serviço registrando ocorrências relacionadas com a execução do objeto contratado e determinando as medidas necessárias à regularização dos problemas observados, também quanto ao cumprimento, pela Contratada, das leis, normas e regulamentos ambientais, sanitários, trabalhistas, previdenciário, tributário e fiscais.

6.2.7 Permitir o acesso dos profissionais da CONTRATADA nas dependências da CONTRATANTE, relacionadas com a execução do contrato, desde que estejam devidamente identificados.

6.2.8 Comunicar à CONTRATADA, com antecedência, do planejamento estratégico de mudanças e inovações no ambiente tecnológico que estejam relacionados à execução do contrato.

6.3 Deveres e responsabilidades da CONTRATADA:

6.3.1 Na seleção dos profissionais que empregará na execução dos serviços, incumbe à Contratada proceder à avaliação acerca da aptidão profissional e psicológica destes, inclusive no tocante à comprovação dos requisitos técnicos exigidos, bem como no que tange ao cumprimento do artigo 3º da Resolução nº 7 de 18 de outubro de 2005 do Conselho Nacional de Justiça que disciplina sobre a vedação à prática de nepotismo.

6.3.2 A CONTRATADA deverá observar rigorosamente todos os itens do Termo de Referência, executando os serviços de acordo com as especificações e normas aplicáveis, utilizando

ferramental apropriado e dispondo da infraestrutura e equipe técnica exigidas para a perfeita execução do contrato;

6.3.3 Seguir as instruções e observações efetuadas pelo Gestor do Contrato, ou a quem este designar, bem como reparar, corrigir, remover, reconstruir ou substituir às suas expensas, no todo ou em parte, serviços efetuados em que se verificarem vícios, defeitos ou incorreções;

6.3.4 Reportar formal e imediatamente ao Gestor do Contrato, ou a quem este designar, quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução do serviço;

6.3.5 Prestar todos os esclarecimentos que forem solicitados pela CONTRATANTE, sempre por escrito, assim como quaisquer entendimentos com o Fiscal ou o Gestor do Contrato, não sendo consideradas alegações, solicitações ou quaisquer declarações verbais;

6.3.6 A CONTRATADA, independentemente da atuação do Fiscal Técnico do Contrato, não se eximirá de suas responsabilidades quanto à execução dos serviços e o fornecimento de bens, responsabilizando-se pelo fiel cumprimento das obrigações constantes no Termo de Referência;

6.3.7 A CONTRATADA cumprirá a legislação constitucional, tributária, civil, trabalhista, previdenciária, social, ambiental, de saúde e segurança ocupacional, assim como se responsabilizará pela permanente manutenção da validade da documentação jurídica, fiscal, ambiental, sanitária, trabalhista, previdenciária, técnica e econômico-financeira da empresa, em observância a periodicidade prevista na legislação vigente;

6.3.8 Detalhar e repassar, conforme orientação e interesse do CONTRATANTE, todo o conhecimento técnico utilizado na execução do serviço contratado;

6.3.9 A CONTRATADA indicará formalmente um preposto como responsável pelo gerenciamento dos serviços, autorizado a tratar com a CONTRATANTE a respeito de todos os aspectos que envolvam a execução do contrato, devendo fornecer todas as informações sobre o referido preposto, na reunião inaugural, tais como: nome, endereço eletrônico, telefones e horário de atendimento, para que o mesmo possa ser encontrado sempre que necessário. O documento emitido pela Contratada indicando o preposto deverá ser entregue na reunião

inaugural, e conterá as seguintes informações: nome, endereço eletrônico, telefones fixos e celular;

6.3.10 Responsabilizar-se-á integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas no edital, caso os prazos, indicadores e condições não sejam cumpridos;

6.3.11 Garantir a execução do serviço sem interrupção, mantendo equipe dimensionada adequadamente para a regular execução do serviço, substituindo ou contratando profissionais sem ônus para a CONTRATANTE;

6.3.12 Responder civil e administrativamente, sem prejuízo de medidas outras que possam ser adotadas, por quaisquer perdas ou danos causados a CONTRATANTE ou a terceiros, em razão de ação ou omissão, dolosa ou culposa, sua ou de seus profissionais, em razão da execução do serviço contratado, independentemente de outras cominações contratuais ou legais a que estiver sujeito;

6.3.13 Facilitar as ações do Fiscal Técnico do Contrato e do Gestor do Contrato, fornecendo informações ou promovendo acesso à documentação dos serviços em execução, atendendo prontamente às observações e às exigências por eles apresentadas quanto ao cumprimento das obrigações contratuais;

6.3.14 Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do CONTRATANTE;

6.3.15 A CONTRATADA não poderá se valer do contrato para assumir obrigações perante terceiros, dando-o como garantia, nem utilizar os direitos de crédito a serem auferidos em função dos serviços prestados, em quaisquer operações de desconto bancário, sem prévia autorização do CONTRATANTE;

6.3.16 Substituir por outro profissional de qualificação igual ou superior qualquer um dos seus profissionais cuja qualificação, atuação, permanência ou comportamento da execução do

objeto deste contrato forem julgados prejudiciais, inconvenientes ou insatisfatórios à disciplina da CONTRATANTE ou interesse do serviço público, sempre que exigido pelo Gestor do Contrato;

6.3.17 Cumprir e fazer cumprir por seus profissionais as normas e os regulamentos internos do CONTRATANTE.

6.3.18 Responsabilizar-se zelando pela limpeza e conservação dos ambientes onde desempenhe o serviço contratado;

6.3.19 A CONTRATADA deverá manter durante toda a execução do contrato, todas as condições de habilitação e qualificação exigidas na licitação, apresentando, sempre que exigido, os comprovantes de regularidade fiscal;

6.3.20 Em até 48 horas após o recebimento do empenho, a contratada deverá apresentar-se ao órgão técnico responsável pelo contrato – DGTEC/DEINF/DIRED, localizado na Avenida Erasmo Braga 115, sala 111, corredor C, Lâmina I, Centro, Rio de Janeiro, para reunião de alinhamento, esclarecimento e ciência dos termos do contrato;

6.3.21 A Contratada fornecerá crachá de identificação, em que constem o nome da empresa, o do profissional, o registro geral e a fotografia, devendo manter os profissionais, identificados, mediante o uso permanente de crachá;

6.3.22 A Contratada, na ocorrência de reclamações atinentes a quaisquer aspectos da execução contratual, inclusive quanto ao emprego inadequado de material ou equipamentos, se obriga a providenciar a sua imediata correção, sem ônus para o Contratante, garantindo a manutenção da qualidade dos serviços;

6.3.23 A Contratada se responsabilizará pela idoneidade e pelo comportamento de seus profissionais, prepostos ou subordinados, e, ainda, arcará com o ônus de indenizar o dano que, por culpa ou dolo os seus profissionais causarem ao Poder Judiciário do Estado do Rio de Janeiro ou a terceiros, inclusive pela má utilização dos bens (materiais, utensílios e equipamentos) disponibilizados pela Administração Pública, para a realização dos serviços, obrigando-se a repor desvios, desperdícios, perdas ou quaisquer outros prejuízos que venham a ocorrer;

6.3.24 A Contratada deverá zelar para que todos os seus profissionais executem suas atividades seguindo as normas e procedimentos técnicos e de qualidade, segurança, meio ambiente, higiene e saúde;

6.3.25 A Contratada executará os serviços sob condições que atendam às determinações constantes nas Normas Regulamentadoras de Segurança e Medicina do Trabalho do Ministério do Trabalho;

6.3.26 A Contratada instruirá os seus profissionais quanto à prevenção de incêndios nas áreas da contratante, seguindo as orientações da Diretoria Geral de Segurança Institucional (DGSEI).

6.4 Formas de Acompanhamento do Contrato

Eventos	Forma de Acompanhamento
Entrega dos componentes da solução	• Verificação do prazo de entrega; • Validação do funcionamento dos componentes; • Emissão de Termo de Aceitação Provisória antes da validação do funcionamento dos componentes; • Emissão do Termo de aceitação definitiva.
Implantação	• Participação nas reuniões; • Aprovação do projeto, plano e cronograma de implantação, elaborado pela CONTRATADA; • Avaliação dos serviços prestados, para emissão do termo de aceite definitivo da implantação de acordo com o projeto a ser apresentado; • Reuniões presenciais, ou on-line na conveniência do CONTRATANTE, entre o Gestor, o Fiscal do Contrato e o Preposto da CONTRATADA para avaliação do serviço prestado no período e verificação do atendimento aos requisitos contratuais estabelecidos, com periodicidade a ser definida pelo Gestor do Contrato; • Emissão do Termo de Aceitação Definitiva.
Suporte Técnico	• Verificação dos prazos acordados para a manutenção preventiva e corretiva da solução.

Suporte Técnico Especializado	• Através de relatórios atestando as horas de consultoria ministradas e o conteúdo; • Avaliação e aprovação do planejamento e cronograma apresentado por escrito pela CONTRATADA; • Avaliação da execução dos serviços ordenados, após comunicação do término pela CONTRATADA; • Emissão do termo de aceite definitivo, de acordo com as horas consumidas e comprovadas em relatório técnico.
Treinamento Oficial da Solução	• Verificação das credenciais da fornecedora do treinamento; • Verificação da carga horária dos treinamentos no final da sua execução; • Verificação do material didático; • Avaliação do treinamento; • Emissão do termo de aceite definitivo após recepção de todos os certificados.
Garantia da Solução	• Verificação dos prazos para atualização e troca de equipamentos ou peças da solução.

6.5 Qualidade de Serviço do Objeto a ser recebido

6.5.1 Instrumento de Medição de Resultado.

6.5.1.1 Os descontos que eventualmente ocorram devido a um não atendimento aos níveis exigidos serão calculados no mês da ocorrência e terão que ser aplicados no mês imediatamente subsequente;

6.5.1.2 Os índices de medição de resultado e os descontos estão previstos baixo:

1 – **COMPONENTES DA SOLUÇÃO**.	
Indicador:	Tempo de Entrega dos componentes da solução.
Limite Máximo Aceitável:	45 (quarenta e cinco) dias corridos contados da data do início da publicação do extrato do contrato no diário oficial.

Desconto no caso de descumprimento dos prazos estabelecidos.	• Após os 45 dias, desconto de 0,3% ao dia sobre o valor contratado para o item. • Após 60 dias, 0,5% ao dia sobre o valor contratado para o item. • Após 90 dias será declarada a inexecução total do contrato.

2 – **IMPLANTAÇÃO**	
Indicador (1):	Reunião para levantamento do ambiente e alinhamento.
Limite Máximo Aceitável (1):	Até 6 (seis) dias corridos após a emissão do Termo de Aceite Definitivo da entrega dos equipamentos.,
Descontos no caso de descumprimento dos prazos estabelecidos (1).	• Após 6 (seis) dias, desconto de 0,3% do valor do item por dia de atraso. • Após 10 (dez) dias, desconto de 0,5% do valor do item por dia de atraso. • Após 30 (trinta) dias será declarada a inexecução total do contrato.
Indicador (2):	Entrega da documentação do planejamento
Limite Máximo Aceitável (2):	10 (dez) dias corridos após Reunião para levantamento do ambiente e alinhamento.
Descontos no caso de descumprimento dos prazos estabelecidos (2).	• Após 10 (dez) dias, desconto de 0,3% do valor do item por dia de atraso. • Após 15 (quinze) dias, 0,5% do valor do item por dia de atraso. • Após 30 dias será declarada a inexecução total do contrato.
Indicador (3):	Entrega da documentação do planejamento corrigido.
Limite Máximo Aceitável (3):	2 (dois) dias corridos após a não aprovação do primeiro planejamento.
Descontos no caso de descumprimento dos prazos estabelecidos (3).	• Após 2 (dois) dias, desconto de 0,5% do valor do item por dia de atraso; • Após 5 (cinco) dias, 0,8% do valor do item por dia de atraso; • Após 30 dias será declarada a inexecução total do contrato.
Indicador (4):	Entrega da implantação da tecnologia
Limite Máximo Aceitável (4):	31 (trinta e um) dias corridos após a emissão do Termo de Aceite Definitivo da entrega dos equipamentos.
Descontos no caso de descumprimento dos prazos estabelecidos (4).	• Após 31 (trinta e um) dias, desconto de 0,5% do valor do item por dia de atraso; • Após 45 (quarenta e cinco) dias, desconto 0,8% do valor do item por dia de atraso; • Após 60 dias, será declarada a inexecução total do contrato.

3 – **SUPORTE TÉCNICO**.

Indicador:	Início do Atendimento para Severidade 1
Limite Máximo Aceitável:	15 (quinze) minutos após a abertura do chamado.
Desconto no caso de descumprimento dos prazos estabelecidos.	• A cada 5 (cinco) minutos excedentes do prazo, desconto de 0,5% (zero virgula cinco por cento) sobre o valor da fatura mensal. • Após 60 (sessenta) minutos da abertura do chamado, 1% de desconto a cada 5 (cinco) minutos de não atendimento.
Indicador:	Resolução do problema de Severidade 1
Limite Máximo Aceitável:	2 (duas) horas contadas da abertura do chamado.
Desconto no caso de descumprimento dos prazos estabelecidos.	• Após as 2 (duas) horas de prazo, desconto de 1% do valor mensal do serviço para cada 30 minutos de atraso. • Após 24 (vinte e quatro) horas, incidirá cumulativamente na multa do item **Erro! Fonte de referência não encontrada.**, neste caso após instauração do procedimento apuratório e decisão do eventual recurso interposto.
Indicador:	Início do Atendimento para Severidade 2
Limite Máximo Aceitável:	30 (trinta) minutos após a abertura do chamado.
Desconto no caso de descumprimento dos prazos estabelecidos.	• A cada 10 (dez) minutos excedentes do prazo, desconto de 0,5% (zero virgula cinco por cento) sobre o valor da fatura mensal. • Após 60 (sessenta) minutos da abertura do chamado, 1% de desconto a cada 10 (dez) minutos de não atendimento.
Indicador:	Resolução do problema de Severidade 2
Limite Máximo Aceitável:	4 (quatro) horas contadas da abertura do chamado.
Desconto no caso de descumprimento dos prazos estabelecidos.	• Após as 4 (quatro) horas de prazo, desconto de 1% do valor mensal do serviço para cada 30 minutos de atraso. • Após 24 (vinte e quatro) horas, incidirá cumulativamente na multa do item **Erro! Fonte de referência não encontrada.**.
Indicador:	Início do Atendimento para Severidade 3
Limite Máximo Aceitável:	60 (sessenta) minutos após a abertura do chamado.
Desconto no caso de descumprimento dos prazos estabelecidos.	• A cada 30 (trinta) minutos excedentes do prazo, desconto de 0,5% (zero virgula cinco por cento) sobre o valor da fatura mensal. • Após 6 (seis) horas da abertura do chamado, 1% de desconto a cada 1 (uma) hora de não atendimento.
Indicador:	Resolução do problema de Severidade 3
Limite Máximo Aceitável:	24 (vinte e quatro) horas contadas da abertura do chamado.

Desconto no caso de descumprimento dos prazos estabelecidos.	• Após as 24 (vinte e quatro) horas de prazo, desconto de 1% do valor mensal do serviço para cada 1 (uma) hora de atraso. • Após 72 (setenta e duas) horas, incidirá cumulativamente na multa do item **Erro! Fonte de referência não encontrada.**.

4 – **TREINAMENTO OFICIAL DA SOLUÇÃO**.	
Indicador:	Fornecimento do Treinamento Oficial da Solução
Limite Máximo Aceitável:	Organização do treinamento em até 30 (trinta) dias após a solicitação do treinamento.
Desconto no caso de descumprimento dos prazos estabelecidos.	• Após o limite máximo aceitável incidirá desconto de 0,5% (zero vírgula cinco por cento) do valor do serviço por dia de atraso.

5 – **GARANTIA DA SOLUÇÃO**.	
Indicador:	Atualização da Solução.
Limite Máximo Aceitável:	Atualização da solução na data estipulada para tal.
Desconto no caso de descumprimento dos prazos estabelecidos.	• 5% (cinco por cento) do valor mensal do serviço a cada não realização do serviço sem prévia justificativa.
Indicador:	Substituição de equipamentos ou peças defeituosos que estiverem causando problemas de severidade 1.
Limite Máximo Aceitável:	24 (vinte e quatro) horas após constatação e solicitação da troca.
Desconto no caso de descumprimento dos prazos estabelecidos.	• 0,5% (zero virgula cinco por cento) do valor do contrato para cada hora de atraso após as 24 (vinte e quatro) horas estipuladas para Severidade 1.
Indicador:	Substituição de equipamentos ou peças defeituosos que estiverem causando problemas de severidade 2.
Limite Máximo Aceitável:	48 (quarenta e oito) horas para troca de equipamento ou peça avariados que produzam efeitos segundo o descrito na Severidade 2.

Desconto no caso de descumprimento dos prazos estabelecidos.	• 0,5% (zero virgula cinco por cento) do valor do contrato para cada hora de atraso após as 48 (quarenta e oito) horas estipuladas para Severidade 2.
Indicador:	Substituição de equipamentos ou peças defeituosos que estiverem causando problemas de severidade 3.
Limite Máximo Aceitável:	120 (cento e vinte) horas para troca de equipamento ou peça avariados que produzam efeitos segundo o descrito na Severidade 3.
Desconto no caso de descumprimento dos prazos estabelecidos.	• 0,3% (zero virgula três por cento) do valor do contrato para cada hora de atraso após as 120 (cento e vinte) horas estipuladas para Severidade 3.

6.6 Estimativa de Volume de Bens / Serviços

6.6.1 Bem / Serviço

6.7 Prazos e Condições

6.7.1 O prazo do contrato é de 36 (trinta e seis) meses, contado da data indicada no memorando de início do serviço, expedido pelo órgão fiscal, após a formalização do contrato e publicação de seu extrato no Diário da Justiça Eletrônico, o que ocorre após a emissão do respectivo empenho, sendo prorrogável na forma do art. 57, inciso II, da Lei federal nº 8.666/93, por meio de termo aditivo que conterá cláusula de rescisão amigável, para os serviços de suporte técnico, suporte técnico especializado, treinamento oficial da solução e garantia da solução e de 86 dias contados da publicação do extrato do contrato no Diário da Justiça Eletrônico, na forma abaixo descrita:

Item	Descrição	Prazo
1	SOLUÇÃO DE NEXT GENERATION FIREWALL	Entrega em até 45 (quarenta e cinco) dias corridos contados da publicação do extrato do contrato no Diário da Justiça Eletrônico mais 3 (três) dias para emissão do TAP e 5 (cinco) dias para emissão do TAD
2	SERVIÇO DE IMPLANTAÇÃO	Em até 31 (trinta e um) dias contados da emissão do termo de aceite definitivo do da Entrega dos componentes da solução

		de IPS mais 3 (três) dias para emissão do TAD e 3 (três) dias para emissão do memorando de início
3	SUPORTE TÉCNICO	36 (trinta e seis) meses a contar da emissão do Memorando de início.
4	SUPORTE TÉCNICO ESPECIALIZADO	Sob demanda durante o prazo de 36 (trinta e seis) meses a contar do memorando de início dos serviços.
5	TREINAMENTO OFICIAL DA SOLUÇÃO	O serviço será solicitado pelo contratante em até 6 (seis) meses contado da assinatura do memorando de início dos serviços.
6	GARANTIA DA SOLUÇÃO	36 (trinta e seis) meses a contar da emissão do Memorando de Início da Contratação.

6.8 Aceite, Alteração e Rescisão

6.8.1 Condição de Aceite

6.8.1.1 A aceitação provisória da entrega dos componentes da solução ocorrerá em até 3 dias corridos da entrega no local de implantação na Av. Erasmo Braga 115, 1º andar, Corredor C, Sala 111, Data Center, mediante emissão de Termo de Aceite Provisório, para efeitos de posterior conferência do funcionamento e conformidade dos equipamentos às especificações técnicas constantes deste Termo de Referência;

6.8.1.2 O Termo de Aceite Definitivo da entrega dos componentes da solução ocorrerá em até 5 (cinco) dias corridos após a aceitação provisória e, mediante a verificação e conferência dos equipamentos, acompanhada de pelo menos um representante da CONTRATADA, que será responsável por abrir as caixas para conferência e lacrá-la novamente até o dia da implantação;

6.8.1.3 Caberá a CONTRATADA a substituição dos componentes rejeitados, no todo ou em parte, por razões de defeito ou não conformidade com as especificações técnicas, correndo a suas expensas os custos inerentes.

6.8.1.4 O Termo de Aceite Definitivo da Implantação será emitido em até 3 (três) dias corridos a contar da entrada em operação da solução;

6.8.1.5 Será concedido o aceite definitivo do suporte técnico mensalmente, em relação ao mês anterior, uma vez verificado o atendimento aos índices de medição de resultado (IMR).

6.8.1.6 No caso de não atendimento total ao IMR, o aceite será dado mediante desconto a ser informado baseando-se no índice.

6.8.1.7 O aceite provisório do serviço de Suporte Técnico Especializado será fornecido tão logo o projeto e/ou implementação requeridos estejam completados, ou se opte pela sua não continuidade.

6.8.1.8 O aceite definitivo do Suporte Técnico Especializado será concedido em 7 (sete) dias corridos, uma vez verificada a estabilidade da implantação e/ou qualidade do projeto.

6.8.1.9 Caso o projeto ou implantação de que trata o item anterior não atenda às expectativas, a CONTRATANTE poderá solicitar as adequações antes do fornecimento do aceite definitivo.

6.8.1.10 O Aceite definitivo em relação ao serviço de Suporte Técnico Especializado deverá conter o número de horas de suporte prestados.

6.8.1.11 Os serviços de Treinamento serão ministrados por Centro Oficializado pelo fabricante, dentro das especificações de adequação ao conteúdo e a carga horária previstos neste Termo de Referência ou de forma online desde que não haja prejuízo para a qualidade da transferência de conhecimento.

6.8.1.12 Caso o treinamento, seja considerado insatisfatório pela maioria absoluta dos participantes, este deverá ser fornecido novamente pela CONTRATADA, sem ônus para o CONTRATANTE.

6.8.1.13 A execução dos serviços de Suporte Técnico e suporte técnico especializado entrará em vigor a contar da data da emissão do Termo de Aceite Definitivo da implantação da solução.

6.8.2 Condição de Alteração

6.8.2.1 As eventuais alterações deverão possuir as devidas justificativas, em caso de ocorrência de quaisquer das situações previstas no artigo 65 da Lei 8666/93. Do qual destacamos os seguintes itens:

6.8.2.1.1 Quando houver modificação do projeto ou das especificações, para melhor adequação técnica aos seus objetivos;

6.8.2.1.2 Quando necessária a modificação do valor contratual em decorrência de acréscimo ou diminuição quantitativa de seu objeto, nos limites permitidos por lei;

6.8.2.1.3 O contratado fica obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nos serviços até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

6.8.3 Condição de Rescisão

6.8.3.1 Constituem motivo para rescisão, as condições descritas nos artigos 78 e 79 da Lei 8666/93, do qual destacamos os seguintes itens:

6.8.3.2 O não cumprimento de cláusulas contratuais, especificações, projetos ou prazos;

6.8.3.3 O cumprimento irregular de cláusulas contratuais, especificações, projetos e prazos;

6.8.3.4 A lentidão do seu cumprimento, levando a Administração a comprovar a impossibilidade da conclusão do fornecimento, nos prazos estipulados;

6.8.3.5 O atraso injustificado no início do serviço;

6.8.3.6 O desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a sua execução, assim como as de seus superiores;

6.8.3.7 O cometimento reiterado de faltas na sua execução.

6.8.3.8 Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa;

6.8.3.9 A rescisão poderá ser amigável, por acordo entre as partes, reduzida a termo no processo da licitação, desde que haja conveniência para o CONTRATANTE.

6.9 Justificativa para o não parcelamento do objeto

6.9.1 O objeto deste Termo de Referência trata de um conjunto de atividades inter-relacionadas, cuja execução deve ser realizada pelo mesmo Fornecedor, a fim de que o funcionamento adequado do ambiente e dos recursos computacionais, juntamente com o conhecimento consolidado de suas características e funcionalidades garantam um perfeito atendimento ao usuário final.

6.9.2 Devido ao nível de integração dessa tecnologia/serviços, a execução fracionada, prestada por diferentes Fornecedores, certamente acarretará incompatibilidades, demoras e, principalmente, graves riscos de segurança, que prejudicarão o suporte aos usuários e, consequentemente, à prestação jurisdicional.

6.9.3 Além disso, a centralização da responsabilidade em uma única empresa contratada, facilita o acompanhamento de problemas e soluções e a verificação das suas causas e atribuição de responsabilidades, aumentando, consequentemente, o controle sobre a execução do objeto licitado.

6.9.4 A existência de tarefas comuns em diversas atividades permite também a economia de recursos na prestação dos serviços, já que o mesmo prestador pode executar atividades de serviços diferentes, o que tende a reduzir o custo da contratação.

6.9.5 Pelas razões apresentadas fica evidente, portanto, que o parcelamento do objeto é tecnicamente inviável e contrário ao interesse público.

6.10 Condições de Pagamento

6.10.1 Etapa/Fase/Item

Item	Descrição	Forma	Pagamento
1	Appliances Next Generation Firewall	Pagamento Único	Após aceite definitivo da entrega dos appliances com todos os acessórios solicitados neste Termo de Referência.
2	Solução de Balanceamento para os NG Firewalls	Pagamento único	Após aceite definitivo da entrega da solução com todos os acessórios solicitados neste Termo de Referência.
3	Solução de Gerência Centralizada	Pagamento Único	Após aceite definitivo da entrega dos appliances com

			todos os acessórios solicitados neste Termo de Referência.
4	Serviço de Implantação da Solução	Pagamento Único	Pagamento após o aceite definitivo da Implantação
5	Serviço de suporte técnico	36 Parcelas fixas mensais	Pagamento a cada mês após a verificação dos índices de medição de resultado.
6	Serviço de suporte técnico especializado;	Por hora, sob demanda no mês	Após Faturamento, depois da emissão do termo de aceite definitivo, de acordo com as horas consumidas e comprovadas em relatório técnico.
7	Serviço de treinamento oficial da solução	Por turma de 4 participantes	Pagamento após a realização do treinamento com a expedição do devido certificado e emissão do termo de aceite definitivo.
8	Serviço de garantia.	36 Parcelas fixas mensais	Pagamento a cada mês após a verificação do instrumento de medição de resultado.

6.10.2 Condição de Pagamento

6.10.2.1 Os pagamentos devidos à CONTRATADA serão efetuados mediante apresentação da fatura/nota fiscal emitida por seu estabelecimento, em correspondência à obrigação cumprida.

6.10.2.2 A CONTRATADA deverá entregar na Divisão de Apoio Administrativo à Execução de Contratos de Prestação de Serviços – DICON, situada, na Praça XV de Novembro nº 02 – sala 305 – Centro/RJ, a Nota Fiscal discriminando os serviços executados pelo período correspondente e com CNPJ idêntico ao constante do contrato, acompanhada dos documentos abaixo elencados, sob pena de ser recusada a referida nota pela unidade gestora do contrato:

6.10.2.2.1 Certidão de Regularidade Fiscal do FGTS;

6.10.2.2.2 Certidão Negativa de Débito do INSS, podendo ser apresentada por meio da Certidão Negativa de Débitos relativos aos Tributos Federais e à Dívida Ativa da

União, em conformidade com a Portaria Conjunta RFB/PGFN nº 1.751, de 2 de outubro de 2014, e da Certidão Negativa de Débitos Trabalhistas (CNDT), devidamente válidas;

6.10.2.2.3 Documentação relativa à comprovação do adimplemento de suas obrigações trabalhistas, previdenciárias.

6.10.2.3 O pagamento da fatura/nota fiscal deverá ocorrer no prazo de 30 (trinta) dias, contados da data da sua autuação no Protocolo do PJERJ, por meio de crédito em conta corrente no Banco Bradesco S.A., informada pelo Contratado;

6.10.2.4 Após conferida cada fatura/nota fiscal, a atestação da execução em conformidade com o contrato deve ser feita por dois servidores, fiscal e fiscal substituto, e na ausência destes, pelo gestor e/ou gestor substituto, respectivamente, no prazo de 9 (nove) dias a contar da autuação. Os autos são devolvidos ao Agente Administrativo (DECOP – Departamento de Execução de Contratos e Prestação de Serviços), que deve visar à nota fiscal em 9 (nove) dias, a contar do recebimento do processo. Os prazos acima não devem exceder 18 (dezoito) dias entre a data da autuação e a liberação para pagamento;

6.10.2.5 Após, o Agente Administrativo do contrato a encaminhará à Diretoria-Geral de Planejamento, Coordenação e Finanças (DGPCF), acompanhada da devida documentação;

6.10.2.6 No caso de notas fiscais em desacordo com o documento de referência ou com qualquer circunstância que desaconselhe seu pagamento, estas poderão ser recusadas pelo contratante ou, uma vez recebidas as notas, o prazo previsto para o pagamento deverá ser interrompido e somente reiniciará a partir da respectiva regularização;

6.10.2.7 O processamento do pagamento observará a legislação pertinente à liquidação da despesa pública.

6.11 Garantia Técnica/Garantia da Solução

6.11.1 A solução, envolvendo todos os seus componentes (hardware e software), deverá ter garantia de, no mínimo, de 36 (trinta e seis) meses, após a assinatura do memorando de início, garantindo as atualizações da aplicação de gerenciamento e controle, bem como as atualizações pertinentes às versões subsequentes;

6.11.2 A garantia deve contemplar a atualização do sistema operacional durante todo o período de sua vigência, independentemente da demanda de atualização ser ocasionada por necessidade de correção ou pela implementação de novos releases ou funcionalidades;

6.11.3 `A CONTRATADA deverá prover garantia de correção relativa às atualizações de software e versões fornecidas com funcionamento indevido;

6.11.4 A garantia deverá contemplar a substituição dos equipamentos avariados, sejam eles peças ou o equipamento inteiro, cujos problemas não puderem ser sanados pelo serviço de manutenção corretiva e preventiva previstos neste termo de referência;

6.11.5 Durante o período de garantia o FORNECEDOR deverá garantir o fornecimento de peças sobressalentes e mão de obra para manutenção;

6.11.6 O FORNECEDOR deverá fornecer um equipamento igual ou superior para substituição do equipamento defeituoso enquanto este estiver fora para conserto;

6.11.7 A garantia deve permitir que a equipe técnica da Contratante entre em contato diretamente, de forma excepcional e mediante justificativa que embase suas motivações, com Engenheiros e técnicos do fabricante da solução lotados no Brasil ou no exterior; o contato poderá ser por meio telefônico, e-mail, videoconferência ou presencialmente, conforme acordo entre as partes e levando em consideração a gravidade da situação que venha a motivá-lo.

6.12 Garantia Contratual

6.12.1 Será exigida uma garantia contratual de 5% (Cinco por cento) do valor total do contrato;

6.12.2 A validade da garantia deverá estar em consonância com o prazo de vigência contratual. No caso de alteração do valor do contrato ou prorrogação de sua vigência, a garantia será readequada ou renovada nas mesmas condições e parâmetros, mantido o percentual sobre o valor atualizado do contrato;

6.13 Propriedade, Sigilo e Restrições

6.13.1 Direito de Propriedade

6.13.1.1 Não se aplica uma vez que esta contratação não envolve direito autoral e direito de propriedade intelectual.

6.13.2 Condição de Manutenção de Sigilo

6.13.2.1 A CONTRATADA deverá manter sigilo sobre todo e qualquer assunto concernente ao contratante ou a terceiros, que tomar conhecimento em razão da execução do contrato, sob pena de rescisão contratual, responsabilidade civil, penal e administrativa, no caso de divulgação e o fornecimento de dados e informações obtidas em decorrência dos serviços objeto do contrato, devendo orientar os seus profissionais nesse sentido**;**

6.13.2.2 A CONTRATADA firmará, através de seus representantes, antes do início da execução do contrato, Termo de Ciência e Compromisso de Manutenção de Sigilo, conforme documento interno do contratante.

6.14 Mecanismos Formais de Comunicação

Documento	Emissor	Destinatário	Meio	Periodicidade
Termo de Compromisso de Manutenção de Sigilo (FRM-DGTEC-041-09)	PJERJ CONTRATADA	PJERJ (Gestor do Contrato)	Entrega pessoal/ Correio	Até a data indicada no memorando de início
Termo de Ciência (FRM-DGTEC-041-08)	CONTRATADA	PJERJ	Entrega pessoal/ Correio	Eventual
Relatório de Atendimento Técnico (RAT)	CONTRATADA	DGTEC	E-mail	A cada atendimento técnico
Memorando de Início dos serviços	PJERJ	CONTRATADA	Papel timbrado	3 (três) dias a contar do Termo de Aceite Definitivo da Implantação

Nota Fiscal	CONTRATADA	PJERJ	Entrega pessoal	Após o faturamento do serviço realizado
Abertura de Chamados Técnicos	PJERJ	CONTRATADA	Canal de comunicação, sem ônus para o contratante, provido e atualizado pela CONTRATADA	Eventual
Termo de Aceite Provisório	PJERJ	CONTRATADA	Papel Timbrado ou e-mail	Após aprovação provisória
Termo de Aceite Definitivo	PJERJ	CONTRATADA	Papel Timbrado ou e-mail	Após aprovação definitiva
Formulário de Avaliação dos Treinamentos	PJERJ	CONTRATADA	Papel Timbrado ou meio eletrônico	Após a realização de cada treinamento
Ofício: utilizado para quaisquer questões administrativas durante a execução do Contrato	PJERJ	CONTRATADA	Entrega pessoal/ Correio	Eventual
Mensagem eletrônica: questões administrativas ou técnicas durante a execução do Contrato	PJERJ	CONTRATADA	Internet	Eventual
Relatório Mensal de Documento Interno Obrigatório de Acompanhamento de Contrato	PJERJ	CONTRATADA	Papel Timbrado	Mensal

7. ESTIMATIVA DE PREÇO

7.1. Incluem-se na estimativa de preços dos serviços: tributos, tarifas e emolumentos; encargos sociais, trabalhistas, insumos, contribuições ou obrigações decorrentes da legislação trabalhista, fiscal, previdenciária e demais custos que envolvem a prestação dos serviços.

8. ADEQUAÇÃO ORÇAMENTÁRIA

8.1. Conforme especificado no Edital.

9. SANÇÕES APLICÁVEIS

9.1. Nos casos de descumprimento dos prazos e obrigações contratuais previstas neste Termo de Referência, serão aplicadas multas à CONTRATADA conforme disposto a seguir, garantidos o contraditório e a ampla defesa;

9.1.1. Para o serviço de suporte técnico 24x7:

9.1.1.1. Até 10% (dez por cento) sobre o valor total do serviço, caso seja caracterizada inexecução parcial, que ocorrerá quando a Contratada sofrer 3 (três) glosas consecutivas ou 6 (seis) glosas alternadas no período de 1 (um) ano, sem justificativa;

9.1.1.2. Até 10% (dez por cento) sobre o valor do serviço, em caso de atraso de mais de 24 (vinte e quatro horas) na resposta para solução do problema de hardware classificados como severidade 1 ou severidade 2, indicadas nos itens 5.1.1.5.8.1 e 5.1.1.5.8.2;

9.1.1.3. Até 15% (quinze por cento) sobre o valor do serviço em caso de inexecução parcial do objeto, que será caracterizada quando o problema

relatado, de software ou hardware, não for solucionado em até 15 (quinze) dias, contados da sua abertura;

9.1.1.4. Até 10% (dez por cento) sobre o valor total do serviço em caso de atraso de mais de 26 (vinte e seis) horas na resposta inicial de problemas classificados como severidade 1 conforme item 5.1.1.5.9.1;

9.1.1.5. Até 8% (oito por cento) sobre o valor total do serviço em caso de atraso de mais de 34 (trinta e quatro) horas na resposta inicial de problemas classificados como severidade 2, conforme item 5.1.1.5.9.2;

9.1.1.6. Até 5% (cinco por cento) sobre o valor total do serviço em caso de atraso de mais de 72 (setenta e duas) horas na resposta inicial de problemas classificados como severidade 3 conforme item 5.1.1.5.9.3.

9.1.2. Poderão, ainda, ser aplicadas multas de:

9.1.2.1. Até 1,5% (um e meio por cento) sobre o valor do contrato, pela utilização de peças e/ou componentes fora das condições estabelecidas no termo de referência;

9.1.2.2. Até 1,5% (um e meio por cento) sobre o valor total do contrato, no caso de não atendimento ou atendimento parcial a qualquer requisito estipulado no item 4.1 do termo de referência “Requisitos internos”;

9.1.3. O rol das infrações descritas acima não é exaustivo, não excluindo, portanto, a aplicação de outras sanções previstas na Lei nº 8.666/93 e nas demais legislações específicas, conforme consta no item “DAS SANÇÕES” do edital.

9.2. Com fundamento no artigo 7º da Lei nº 10.520/2005 e, subsidiariamente, nos artigos 86 e 87 da Lei 8.666/1993, a CONTRATADA ficará sujeita às sanções previstas em contrato no caso de descumprimento das obrigações pactuadas, sem prejuízo das responsabilidades civil e criminal, e assegurada a prévia e ampla defesa.

9.3. As multas serão aplicadas por meio de procedimento apuratório, respeitando a ampla defesa.

10. CRITÉRIOS DA SELEÇÃO DE FORNECEDOR

10.1 Consórcio

10.1.1 Não será admitida a participação de pessoas jurídicas em consórcio, qualquer que seja sua forma de constituição, por não se tratar de execução contratual de alta complexidade.

10.2 Cooperativas

10.2.1 Não é inerente aos serviços objeto deste termo de referência a presença dos elementos de subordinação, pessoalidade e habitualidade na relação de trabalho entre os profissionais e a contratada, ficando permitida a contratação de cooperativa.

10.2.2 Requisitos de Capacitação e Experiências

10.2.2.1 Os profissionais da CONTRATADA responsáveis pela execução dos serviços objeto desta contratação deverão ser especializados na tecnologia implantada, o que deverá ser comprovado na reunião de alinhamento mediante certificados de competência e participação em projetos similares;

10.2.2.2 Os Instrutores que ministrarão os treinamentos deverão ser habilitados para o esclarecimento das dúvidas dos participantes.

10.3 Critérios de Seleção

10.3.1 Caracterização da Solução de Tecnologia da Informação

10.3.2 Licitação

Modalidade	Pregão, em sua forma eletrônica, em conformidade com a lei 10.520/02.

Tipo	Menor preço global.
Justificativa	Por se tratar de prestação de serviços comuns.

10.3.3 Qualificação Técnica

10.3.3.1 A licitante deverá apresentar atestado(s) de capacidade técnica, firmados por órgão do poder público ou pessoa jurídica de direito privado, comprovando haver prestado, satisfatoriamente, serviços compatíveis em características, quantidades e prazos com o objeto licitado, cuja(s) parcela(s) de maior relevância é(são) a(s) seguinte(s):

10.3.3.1.1 que a empresa tenha fornecido solução de NGFirewall (Next Generarion Firewall – Firewall de Próxima Geração) e realizado a sua implantação;

10.3.3.1.2 que a empresa tenha prestado suporte técnico na solução de NGFirewall por, no mínimo, 12 meses.

10.3.3.2 Os atestados de capacidade técnica deverão referir-se a serviços prestados no âmbito da atividade econômica principal ou secundária especificadas no contrato social vigente.

10.3.3.3 Será admitida, para fins de comprovação de quantitativo mínimo de tempo de prestação do serviço, a apresentação de diferentes atestados de atividades compatíveis ou similares executadas de forma concomitante, equivalendo tal situação, para fins de comprovação de capacidade técnico-operacional, a uma única contratação;

10.3.3.4 A licitante deverá fornecer declaração firmada pelo seu responsável legal de que a empresa se compromete, durante a vigência do contrato, em manter profissional(is) técnico(s) qualificado(s) para o atendimento nos prazos identificados neste Termo de Referência, garantindo a qualidade na prestação dos serviços, inclusive quanto aos equipamentos disponibilizados;

10.3.3.5 A licitante deverá fornecer declaração firmada pelo seu responsável legal de que se responsabiliza pelo descarte sustentável do lixo eletrônico de peças e

componentes, objeto da presente contratação, oriundos do pós-consumo deste PJRJ bem como é aderente as normas contidas na Portaria 317 de 19/06/2012 do INMETRO, com vistas à melhoria do desempenho de processos produtivos quanto aos aspectos ambientais, sociais e econômicos;

10.3.3.6 As visitas aos locais de execução do objeto serão realizadas mediante prévio agendamento pelo e-mail dired.licita@tjrj.jus.br, acompanhadas de funcionário designado pela DIRED**,** devendo ser realizada com cada uma das licitantes, individualmente, com o fim de se evitar conhecimento prévio acerca do universo de concorrentes;

10.3.3.7 Na hipótese de não haver visitação por decisão da licitante interessada, esta deverá apresentar declaração assinada por seu representante legal afirmando ser desnecessária a visita, porque a empresa conhece as condições e os locais onde serão executados os serviços contratados, nos termos do artigo 30, inciso III, da Lei nº 8.666/93;

10.3.3.8 Não exercida a faculdade, por motivo exclusivo da licitante, esta poderá participar do processo licitatório, mas não poderá alegar desconhecimento que a escuse de cumprir qualquer cláusula do contrato, se vencedora do certame.

10.3.3.9 A licitante deverá fornecer toda a documentação técnica, atualizada, relativa à solução, que comprove a realização dos itens pedidos neste termo de Referência.

10.3.3.10 A Licitante, quando do fornecimento da documentação a que se refere o item anterior, deverá indicar, para cada funcionalidade, onde está descrita na documentação.

10.3.4 Qualificação econômico-financeira

10.3.4.1 Balanço patrimonial e demonstrações contábeis do último exercício social comprovando índices de Liquidez Geral (LG), Liquidez Corrente (LC) e Solvência Geral (SG) superiores a 1 (um);

10.3.4.2 Patrimônio Líquido de, no mínimo, 10% (dez por cento) do valor estimado para a contratação, em caso de não atendimento ao item.

10.3.5 Critérios de Aceitabilidade de Preços Unitários e Globais

10.3.5.1 Como critério de aceitabilidade da proposta adotar-se-á o do preço máximo global estimado para o certame, bem como os valores unitários máximos por item.

10.3.5.2 Na hipótese de algum item encontrar-se acima dos valores unitários estimados, deverá a proponente readequá-lo, mantido o valor global de sua proposta, sob pena de desclassificação.

10.3.6 Critérios de Julgamento

10.3.6.1 Menor preço global

10.3.7 Do reajustamento

10.3.7.1 Passado 1 (um) ano da data limite para apresentação da proposta, o valor dos serviços objeto deste termo de referência poderá ser reajustado, aplicando-se o Índice de Custos da Tecnologia da Informação (ICTI), mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA, mediante negociação entre as partes e a requerimento da licitante, desde que demonstrado que as variações dos custos efetivamente ocorridos causaram desequilíbrio econômico-financeiro, com a devida justificativa e acompanhado de planilha com a demonstração analítica da variação dos componentes de custo, visando à análise e possível aprovação pelo Tribunal.

11 . ANEXOS

11.1 Anexo A – Termo de Compromisso e Manutenção de Sigilo;

11.2 Anexo B – Termo de Ciência e de Compromisso de Sigilo.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO		
Integrante Demandante	**Integrante Técnico**	**Integrante Administrativo**
_____ Alexandre José Pereira da Silva 01/32023	_____ Marcos Stallone Santos 01/19816	_____ Ana Cristina de Souza Ignacio 10/16798

Rio de Janeiro, ____ de _____ de 2021.

_____
Humberto Vieira da Cruz
Mat.4101004
Diretor Geral de Tecnologia da Informação