CONTRATO TRT 16ª REGIÃO Nº 39/2018

PA Nº 2501/2018

CONTRATO DE AQUISIÇÃO DE SOLUÇÃO DE ALTA DISPONBILIDADE DE NEXT GENERATION FIREWALL QUE, ENTRE SI FAZEM A UNIÃO, POR INTERMÉDIO DO TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO, E A EMPRESA NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA.

Pelo presente instrumento particular, o **TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO**, com sede nesta cidade, na Avenida Vitorino Freire, nº 2001, Areinha, CNPJ/MF nº 23.608.631/0001-93, daqui por diante denominado **CONTRATANTE**, neste ato representado pela Exmª. Desembargadora Presidente, **SOLANGE CRISTINA PASSOS DE CASTRO CORDEIRO,** e, de outro lado, a empresa **NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA,** situada SCN – Quadra 05 – Torre Norte, sala 617 – Edifício Brasília Shopping – Asa Norte. Brasília – DF. CEP 70.715-900, inscrita no CNPJ/MF sob o nº 09.137.728/0001-34, doravante denominada **CONTRATADA**, legalmente representada pelo Senhor **BRUNO CÉSAR CARVALHO BORGES DA NÓBREGA**, RG nº 1.895.350 SSP/DF, inscrito no CPF sob o nº 584.242.531-91, e pela Senhora. **PATRÍCIA ANGELINA DA CONCEIÇÃO, RG nº 48.453.021-5 – SSP/SP**, inscrita no CPF sob o nº 346.994.838-01, ajustam entre si este contrato, na forma constante do PA nº 5201/2018, com base no **EDITAL DE PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS Nº 11.926/2017 – ARP nº 02/2018, gerenciada pelo TRT 12ª Região,** e seus Anexos,

conforme as disposições contidas na Lei 10.520/02, Decreto 3.555/00, Decreto 5.450/06, Decreti bº 7.892/2013, Decreto nº 8.250/2014 e, subsidiariamente, as Leis 8.666/93, nº 8.073/90 (CDC), e demais legislações aplicáveis à matéria, o qual se regerá pelas cláusulas e condições a seguir discriminadas:

CLÁUSULA PRIMEIRA – DO ATO AUTORIZATIVO

A celebração deste contrato decorre de despacho exarado pelo Diretor Geral do Tribunal Regional do Trabalho da 16ª Região, doc 22, do protocolo administrativo nº 2501/2018.

CLÁUSULA SEGUNDA - DO OBJETO DO CONTRATO

Constitui-se objeto da presente contratação a aquisição de solução de alta disponibilidade de Next Generation Firewall com gerenciamento centralizado e integrado, garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local ou remoto, no modelo 8x5 (das 08:00h às 12:00h e das 14:00h às 18:00h), pelo prazo de 60 (sessenta) meses, incluindo serviços de instalação e treinamento, conforme tabela de requisitos mínimos e itens abaixo:

ITEM	DESCRIÇÃO	QTIDADE	VLR UNIT	VLR TOTAL
2	Solução de alta disponibilidade de Next Generation Firewall Cluster com 2 appliances Firewall NG Tipo 2 •Throughput em Gbps:	01	R$ 580.000,00	**R$ 580.000,00**

	2 •Número de Conexões Simultâneas: 1.000.000 (um milhão) •Número de Novas Conexões por segundo: 60.000 (sessenta mil) •Disco Rígido com capacidade mínima: 64GB CFAST/SSD •Interfaces SFP+ 10Gb mínima: 4 •Interfaces SFP 1Gb mínimo: 6 •Serviços de instalação •Garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local ou remoto pelo fabricante, 8x5 (oito horas por dia, cinco dias na semana, de segunda a sextafeira), das 08:00h às 12:00h e das 14:00h às 18:00h, pelo prazo de 60 (sessenta) meses			
4	Sistema de Gerenciamento – Next Generation Security Management Solução de Gerenciamento centralizado e integrado •Incluindo serviços de instalação. •Garantia de funcionamento, atualização de assinaturas de	01	R$ 35.000,00	**R$ 35.000,00**

	proteção e suporte técnico local ou remoto, 8x5 (oito horas por dia, cinco dias na semana, de segunda a sextafeira), das 08:00h às 12:00h e das 14:00h às 18:00h, pelo prazo de 60 (sessenta) meses.			
5	Treinamento especializado - Voucher para treinamento especializado oficial do fabricante. •Presencial, em português. •Carga horária mínima de 40 horas. •Deverá ser realizado em uma das seguintes cidades: São Paulo, Rio de Janeiro ou Brasília	05	R$ 4.000,00	**R$ 20.000,00**
7	Transceiver SFP+ 10GB-SR •Alcance até 300m utilizando fibra óptica multimodo 2000MHz*km (MMF OM3). •Compatibilidade com o padrão de operação 10GBASE-SRL (alcance de até 100m utilizando fibra multimodo).	8	R$ 1.000,00	**R$ 8.000,00**
8	Transceiver SFP 1GBLX •Alcance até 10km utilizando fibra óptica monomodo.	8	R$ 1.000,00	**R$ 8.000,00**
9	Transceiver SFP 1GBSX •Alcance até 550m utilizando fibra óptica	2	R$ 500,00	**R$ 1.000,00**

	multimodo na seguinte especificação: 500MHz km MMF (OM2).			
10	Transceiver SFP 1GBTX •Alcance até 100m e compatibilidade com cabo par trançado categoria 5, suportando os padrões de 100 Megabit e 1 Gigabit Ethernet.	2	R$ 500,00	**R$ 1.000,00**
TOTAL DA DEMANDA				**R$ 653.000,00**

I – Especificação Técnica Detalhada:

a) Arquitetura da Solução:

a.1) É composta por solução de alta disponibilidade de Next Generation Firewall e solução de gerenciamento centralizado, fornecidas pelo mesmo fabricante. Cada solução de alta disponibilidade deverá ser composta por 02 (dois) equipamentos (appliances) funcionando em cluster, construídos especificamente para exercer a função de Next Generation Firewall, com hardware e software fornecidos pelo mesmo fabricante.

a.2) Cada equipamento (appliance) que compõe a solução de alta disponibilidade deve suportar, de forma integrada e simultânea, as funcionalidades de firewall, identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso à Internet (controle de aplicações e filtragem de URLs), prevenção de ameaças (IPS, Antivírus, Anti-Bot, Anti-Malware, Anti-Spyware), administração de largura de banda de serviço de Internet (QoS – Quality of Service), decriptografia e inspeção de tráfego SSL, suporte para conexões VPN IPSec e SSL;

a.3) Cada equipamento (appliance) que compõe a solução de alta disponibilidade deve suportar, e estar licenciado para, a criação de pelo menos 6 (seis) sistemas virtuais, independentes entre si.

a.4) A solução de gerenciamento centralizado deverá ser composta por, pelo menos, 01 (um) “appliance virtual” – solução de software baseada em máquina virtual, conforme os padrões estabelecidos pelo DMTF

(Distributed Management Task Force), ou sistema operacional desenvolvido pelo próprio fabricante da solução de gerenciamento que possa ser instalado e executado em ambiente virtual. A solução de gerenciamento será instalada em ambiente de virtualização e hardware de propriedade dos Tribunais participantes da Ata de contratação.

a.5) Todos os equipamentos e seus componentes deverão ser novos, sem uso, entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.

a.6) Não serão aceitos equipamentos em modo *End of Life* e *End of Support*.

b) Forma de Licenciamento:

Todos os componentes de software e/ou firmware da solução deverão ser fornecidos com licença de uso em caráter permanente para todas as funcionalidades, assinaturas, listas e demais métodos de detecção e prevenção de ameaças, bem como quantidades do contrato. O valor pago referente ao licenciamento deverá permitir a utilização por tempo indeterminado da última versão disponível na data do encerramento dos serviços de garantia, suporte técnico e atualização de versões, com exceção da funcionalidade de filtragem de conteúdo WEB, que poderá ter seu funcionamento interrompido após o término da vigência contratual, uma vez que poderá depender de serviços de nuvem de terceiros.

II - Características Gerais:

Serão adquiridos três modelos de appliances, de acordo com os itens 1, 2, 3 da tabela acima. Essa diferenciação decorre das diferentes necessidades dos Tribunais do Trabalho e, buscando o equilíbrio e melhor custo benefício, optou-se por três modelos de equipamentos de Firewall Next Generation:

III – Características de hardware por equipamento (appliance):

a) O equipamento deve ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação) e temperatura ambiente na faixa de 0 a 40°C;

b) O equipamento deve possuir 2 (duas) fontes de alimentação independentes, redundantes e hot-swappable, com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz,

ou auto-ranging. Deverá vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136;

c) O equipamento deve vir acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc.) para fixação em bastidor (rack) padrão EIA-310 com largura de 19' (dezenove polegadas);

d) Cada um dos equipamentos que compõem o Cluster deve possuir, portas SFP+ conforme tipo de equipamento e quantidades mínimas descritos na Tabela 1 Características do Cluster, transceivers SFP+ 10GB-LR e SFP+ 10GB-SR, para conexão ao meio via cabos de fibra óptica, deverá ser fornecido, conforme tipo de equipamento e quantidades mínimas, metade em SFP+ 10GB-LR e metade em SFP+ 10GB-SR;

e) Cada um dos equipamentos que compõem o Cluster deve possuir, portas SFP conforme tipo de equipamento e quantidades mínimas descritos na Tabela acima, Características do Cluster, transceivers SFP 1GB-LC-LX ou SFP 1GB-LC-SX, para conexão ao meio via cabos de fibra ótica. Esta quantidade de interfaces pode ser atendida através de portas SFP/SFP+ entregues preenchidas com transceiver com metade SFP 1GB-LC-LX e a outra metade em SFP 1GB-LC-SX;

f) Cada um dos equipamentos que compõem o Cluster deve possuir, no mínimo, 6 (seis) interfaces 1 (um) Gigabit-Ethernet padrão 1000Base-T, para conexão ao meio via cabos de cobre. Esta quantidade de interfaces pode ser atendida através de portas SFP/SFP+ entregues preenchidas com transceiver SFP 1000Base-T";

g) O equipamento deve possuir 1 (uma) porta de console para configuração e gerenciamento por interface de linha de comando (CLI);
h) O equipamento deve possuir, no mínimo, 1 (uma) interface dedicada para gerenciamento, além das interfaces descritas nas alíneas "d", "e", "f" e "g" anteriores;

i) O equipamento deve possuir, no mínimo, 1 (uma) interface dedicada para o sincronismo de estados da solução de alta disponibilidade, além das interfaces descritas nas alíneas "d", "e", "f" e "g" anteriores. A interface de sincronismo não precisa, necessariamente, estar rotulada para a finalidade de sincronismo do recurso de alta disponibilidade, sendo aceitável qualquer interface do equipamento;

j) O equipamento deve ser fornecido em sua capacidade máxima de processamento e memória;

k) O equipamento deve possuir, no mínimo, 1 U de altura;

l) O equipamento deve ser fornecido com todas as suas portas de comunicação,interfaces e afins habilitadas, operacionais e prontas para operação, sem custos adicionais;

m) O equipamento deve possuir certificação de conformidade sustentável de acordo com os padrões EPA (Environmental Protection Agency) ou similares, tais como EnergyStar, RoHS (Restriction on Harzardous Substances) ou WEEE (Waste Electrical and Eletronic Equipment) ou EMI Certifications FCC part 15, CE, EN55022, EN55024;

n) Deve informar a utilização dos recursos de CPU, memória, armazenamento interno e atividade de rede. Podendo ser mostrado também no sistema de gerência centralizado;

o) Deve informar o número de conexões simultâneas e de novas conexões por segundo do equipamento. Podendo ser mostrado também no sistema de gerência centralizado.

IV – Características de capacidade por equipamento (appliance):

a) Cada um dos equipamentos que compõem o Cluster deve possuir Taxa de transferência (throughtput) mínima conforme mencionado na tabela informativa nas Características Gerais com as funcionalidades de firewall, identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso à Internet (controle de aplicações e filtragem de URL's), prevenção contra ameaças (IPS, Antivirus, Anti-Bot, Anti-Malware, Anti-Spyware), decriptografia e inspeção de tráfego SSL, suporte para conexões VPN IPSec e SSL habilitadas simultaneamente;

b) Quando tratar-se dos firewall´s tipo 2 e 3 será acrescido a administração de largura de banda de serviço (QoS). Após teste de carga máxima;

c) As taxas de transferência indicadas devem ser alcançadas com a inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, sem prejuízo na performance do equipamento, e com todas as assinaturas, listas e demais métodos de controle de acesso e de detecção e prevenção de ameaças habilitados;

d) Quando tratar-se dos firewall´s tipo 2 e 3 será acrescido a administração de largura de banda de serviço (QoS). Após teste de carga máxima;

e) As taxas de transferência e quantidades de conexões acima indicadas devem ser alcançadas durante a realização de "teste de Conformidade", baseado na RFC- 3511 e descrito no ANEXO I que utilizará padrão de tráfego de dados similar ao encontradonos links de dados do TRT/SC (a partir de dados estatísticos previamente coletados), principalmente no que diz respeito à distribuição de protocolos, conexões e tamanhos de pacotes de dados.

V – Funcionalidades básicas por equipamento (appliance):

a) Deve suportar os protocolos IPv4 e Ipv6;

b) Deve suportar no mínimo 512 VLAN's no padrão 802.1q;

c) Deve suportar agregação de links no padrão 802.3ad;

d) Deve suportar flow control no padrão 802.3x;

e) Deve suportar os protocolos DHCP e DHCPv6;

f) Deve suportar o protocolo NTP;

g) Deve suportar as funcionalidades de roteamento estático e dinâmico, em IPv4 e Ipv6;

h) Deve suportar os protocolos RIP, OSPF v2, OSPF v3 e BGP v4;

i) Deve suportar os protocolos IGMP v2, IGMP v3 e PIM-SM;

j) Deve suportar os protocolos SNMP v2c e SNMP v3;

k) Deve possuir MIB própria contemplando, no mínimo, indicadores de estado do hardware e de performance do equipamento;

l) Deve suportar policy based routing (PBR), ou police based forwarding (PBF), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação;

m) Deve suportar o funcionamento nos modos sniffer (para inspeção de tráfego gerado por uma porta de rede espelhada), layer-2, layer-3 e suas combinações;

n) Deve permitir o acesso ao equipamento via CLI (console), SSH e interface web HTTPS;

o) Deve possuir funcionalidade de backup/restore de sua configuração e políticas de segurança;

p) Deve permitir o agendamento automático dos backups;

q) Deve armazenar os backups localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para equipamentos externos por meio dos protocolos FTP e SCP;

r) Deve criptografar e autenticar a comunicação com a solução de gerenciamento centralizado.

VI – Funcionalidades de identificação de usuários da solução (appliance):

a) Deve promover a integração com serviços de diretório LDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, Network Policy Server e Aruba ClearPass Policy Manager ou LDAP;

c) Não será permitida a utilização de agentes instalados nos servidores LDAP, Active Directory, RADIUS, Kerberos e proxies internos, e nem nos equipamentos dos usuários;

d) Não será permitida a interceptação ou espelhamento do tráfego destinado aos servidores LDAP, Active Directory, RADIUS, Kerberos e proxies internos;

e) Será permitido que a solução de gerenciamento centralizado possua um “appliance virtual” específico para atendimento às necessidades de identificação e autenticação de usuários;

f) Deve possuir portal de autenticação (captive portal) para a identificação e autenticação de usuários não registrados ou não reconhecidos por meio dos serviços indicados na alínea “b” acima;

g) O portal de autenticação deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP e Active Directory;

h) Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao Active Directory;

i) Deve registrar a identificação do usuário em todos os logs de eventos de acesso ou de ameaças gerados pelo equipamento;
j) Deve registrar os eventos dos usuários em tempo real, sem a utilização de processos em lote (batches) ou processos de correlação após a ocorrência do evento em questão;

k) Deve estar licenciado e permitia a identificação e autenticação de pelo menos 1.000 (um mil) usuários no equipamento tipo 1 e 5.000 (cinco mil) usuários no equipamento tipo 2 e 3.

VII – Funcionalidades de firewall por equipamento (appliance):

a) Não deve possuir restrições ao número de máquinas ou usuários protegidos;

b) Deve suportar a implementação tanto em modo transparente (layer-2) quanto em modo gateway (layer-3);

c) Deve suportar statefull inspection de tráfego IPv4 e IPv6;

d) Deve suportar controle de acesso para pelo menos 150 serviços e protocolos pré-definidos;

e) Deve suportar os protocolos H.323, SIP, SCCP e MGCP;

f) Deve suportar os protocolos RTCP, RTMP, RTSP e RTP;

g) Deve implementar mecanismo de conversão de endereços NAT (Network Address Translation), de forma a possibilitar a realização de NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional (possibilitando que um endereço tenha mais de um autorização e registro de eventos de acessos ou ameaças;

h) Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino;

i) Deve implementar mecanismo de proteção contra ataques de falsificação de endereços IP (anti-spoofing), tanto para IPv4 quanto para IPv6;

j) Deve implementar mecanismo de captura de pacotes;

k) Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP, na forma do item VI acima;

l) Deve suportar a utilização simultânea de políticas de segurança em IPv4 e IPv6;

m) Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horárioou período de tempo, e suas combinações;

n) Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas. Salvo as conexões atingidas pelas regras alteradas;

o) Deve possibilitar o registro dos fluxos de dados relativos a cada sessão, armazenando: endereços IP de origem e destino dos pacotes, traduções NAT, portas e protocolos de origem e destino, usuário identificado, status dos flags "ACK", "SYN" e "FIN" ou sinalizar nos logs que o Three-way-handshake não foi concluído com sucesso, ação sobre o pacote (permitido ou negado).

VIII – Funcionalidades de geolocalização por equipamento (appliance):

a) Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento;

b) Deve suportar a atualização automática das listas de geolocalização;

c) Deve aplicar as atualizações sem perda das conexões ativas;

d) Deve armazenar as listas de geolocalização no próprio equipamento;

e) Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países;

f) Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.

IX – Funcionalidades de controle de acesso à internet por equipamento (appliance):

a) 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;

b) Deve ser capaz de identificar aplicações, independentemente das portas e protocolos, bem como das técnicas de evasão utilizadas;
c) Deve ser capaz de identificar se as aplicações estão utilizando sua porta default;

d) Deve ser capaz de identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS;

e) Deve ser capaz de identificar aplicações criptografadas usando SSL;

f) Deve ser capaz de identificar um mínimo de 2.000 (duas mil) aplicações, incluindo, mas não se limitando a: peer-to-peer, streaming de áudio e vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email;

g) Deve ser capaz de identificar, no mínimo, as seguintes aplicações: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger ou Facebook Chat, Google+, Google Talk, Tinder, Instagram, Twitter, Linkedin, Dropbox, Google Drive, One Drive ou Microsoft One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex;

h) Deve permitir a criação de assinaturas para identificação de aplicações proprietárias do órgão, sem a necessidade de ação ou intervenção do fabricante;

i) Deve suportar a atualização automática da base de assinaturas utilizada na identificação das aplicações;

j) Deve aplicar as atualizações sem perda das conexões ativas;

k) Deve armazenar a base de assinaturas no próprio equipamento;

l) Deve classificar as aplicações em categorias, tecnologia e fator de risco;

m) Deve identificar os usuários que estão utilizando as aplicações, na forma do VI acima;

n) Deve permitir o bloqueio de aplicações que não estejam utilizando suas portas default;

o) Deve suportar a implementação de políticas de segurança baseadas em: aplicações, categorias de aplicações, fator de risco, endereço IP de

origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações;
p) Deve permitir a utilização ou bloqueio individualizado das aplicações, como BitTorrent e Skype, para determinados usuários ou grupos de usuários;

q) Deve permitir registrar todos os fluxos autorizados/bloqueados das aplicações, incluindo o usuário identificado;

r) Deve alertar o usuário quando uma aplicação for bloqueada;

s) Deve permitir o controle de uso de banda de download ou upload utilizada pelas aplicações (traffic shaping) baseado em: endereço IP ou rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações;

t) Deve ser capaz de efetuar a classificação de conteúdo de páginas web em HTTP e HTTPS, baseado em listas de categoria;

u) Deve possuir no mínimo 60 categorias de URLs, incluindo, mas não se limitando, às seguintes categorias ou suas semelhantes: adult, chat, drugs, gambling, games, hacking, hate speech, remote proxies, social networks, streaming media, violence, weapons;

v) Deve permitir sobrescrever as categorias de uma URL que se considere indevidamente classificada;

w) Deve permitir a criação de categorias customizadas;

x) Deve permitir a inclusão de URLs customizadas nas categorias já existentes ou previamente customizadas;

y) Deve suportar a atualização automática das listas de categorias;

z) Deve aplicar as atualizações sem perda das conexões ativas;

aa) Deve armazenar as listas de categoria no próprio equipamento;

ab) Deve identificar os usuários que estão acessando as páginas web, na forma do item VI acima;

ac) Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, fator de risco, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações;

ad) Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada no próprio equipamento, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada;

ae) Deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado, informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" ou a inclusão de usuário e senha, para possibilitar o usuário continuar acessando o site);

af) Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado.

X – Funcionalidades de prevenção de ameaças por equipamento (appliance):

a) Deve possuir, no mínimo, funcionalidades de IPS, Antivírus, Anti-Bot, Anti-Malware e Anti-Spyware;

b) Deve possuir, no mínimo, os seguintes mecanismos de detecção: assinaturas de vulnerabilidades e exploits, assinaturas de ataques, validação de protocolos, detecção de anomalias, IP defragmentation, remontagem de pacotes TCP, detecção baseada em comportamento, nível de severidade do ataque e nível de confiança de detecção do ataque;

c) Deve possuir proteção contra ataques de negação de serviço DoS e DDoS;

d) Deve possuir assinaturas para bloqueio de ataques “buffer overflow”;

e) Deve possuir mecanismo automático de captura de pacotes de eventos de IPS, para fins de troubleshooting e análise forense;

f) Deve ser capaz de inspecionar tráfego criptografado usando SSL;

g) Deve ser capaz de inspecionar integralmente todos os pacotes de dados, independentemente de seus tamanhos, sem prejuízo na performance do equipamento, até os limites indicados no item IV acima;
h) Deve possuir referência cruzada da base de assinaturas de detecção com os identificadores CVE (Common Vulnerabilities and Exposures);

i) Deve possibilitar a criação de assinaturas customizadas;

j) Deve identificar os usuários relacionados aos eventos de IPS, na forma do item VI acima;

k) Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque, com origem/destino em determinado endereço IP/rede CIDR;

l) Deve permitir a criação de políticas de segurança que bloqueiam um determinado ataque por meio de uma ação de DROP/RESET, com origem/destino em determinado endereço IP/rede CIDR;

m) Deve permitir a criação de exceções/exclusões de inspeção de uma determinada assinatura ou grupo de assinaturas, com origem/destino em determinado endereço IP/rede CIDR;

n) Deve permitir registrar todos os eventos de IPS, incluindo o usuário identificado;

o) Deve identificar e bloquear a comunicação com botnets;

p) Deve bloquear malwares e spywares;

q) Deve inspecionar e bloquear vírus nos seguintes tipos de tráfego, no mínimo: HTTP, HTTPS e SMTP;

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

s) Deve suportar a inspeção de vírus em arquivos comprimidos utilizando o algoritmo deflate (zip, gzip, etc.);

t) Deverá suportar bloqueio de download de pelo menos 50 tipos de arquivos;

u) Deve suportar a atualização automática das bases de assinaturas;

v) Deve aplicar as atualizações sem reboot do equipamento e nem perda das conexões ativas, que não sejam alteradas pelas atualizações;

w) Deve armazenar as bases de assinaturas no próprio equipamento;

x) Deve identificar os usuários relacionados aos eventos de bloqueio, na forma do item VI acima;

y) Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de uma determinada ameaça, com origem/destino em determinado endereço IP/rede CIDR;

z) Deve permitir a criação de políticas de segurança que bloqueiem uma determinada ameaça, com origem/destino em determinado endereço IP/rede CIDR;

aa) Suportar notificações e alertas via email, SNMP traps e log de pacotes.

XI – Características de QoS por equipamento (appliance):

a) Deve permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário;

b) Deve suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp);

c) Deve suportar a priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP e MGCP;

d) Deve suportar a marcação de pacotes DiffServ;

e) Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

XII – Características de inspeção SSL por equipamento (appliance):

a) Deve identificar, decriptografar e analisar o tráfego SSL tanto em conexões de entrada (Inbound) quanto de saída (Outbound);

b) Deve permitir a decriptografia da área útil do pacote de dados (payload) para fins de controle de acesso à Internet e proteção contra ameaças;

c) Deve permitir a diferenciação de conexões pessoais (Bancos, Shopping, etc.) e conexões não pessoais por meio de classificação automática.

XIII – Características de VPN por equipamento (appliance):

a) Deve disponibilizar licenciamento para VPN site-to-site e client-to-site, sem limite do número de usuários simultâneos e sem limite do uso de túneis, respeitando o limite previsto no item IV acima;

b) Deve suportar, no mínimo, 1.000 (um mil) túneis VPN IPSec simultâneos;

c) Deve suportar, no mínimo, 2.000 (dois mil) usuários VPN SSL;

d) Deve suportar VPN site-to-site em topologia Full Meshed (todos os gateways possuem links específicos para todos os demais gateways) e Estrela (gateways satélites se comunicam somente com um único gateway central);

e) Deve suportar criptografia AES-128, AES-256.;

f) Deve suportar integridade de dados com SHA-1 e SHA-256;

g) Deve suportar o protocolo IKE, fases I e II;

h) Deve suportar os algoritmos RSA e Diffie-Hellman groups 1, 2, 5 e 14;

i) Deve suportar NAT-T (NAT Traversal);

j) Deve suportar VPN IPSec client-to-site;

k) Deve possuir cliente próprio para instalação nos dispositivos móveis dos usuários, sem custo adicional e sem limite do número de usuários;

l) O cliente de VPN client-to-site deve ser compatível ou suportar o cliente nativo de pelo menos: Windows XP, Windows Vista (32 e 64 bits), Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 8.1 (32 e 64 bits), Windows 10 (32 e 64 bits), Apple IOS, Android, Mac OSx 10 ou Linux. Pode fornecer também, mais não obrigatorio, opção Clientless com autenticação via browser, para fechar a VPN através de um portal SSL;

m) Deve suportar atribuição de endereço IP nos clientes remotos de VPN;

n) Deve suportar atribuição de DNS nos clientes remotos de VPN;

o) Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF ou BGP;

p) O túnel VPN do cliente ao gateway (client-to-site) deve fornecer uma solução de autenticação única (single-sign-on) aos usuários, integrando-se com as ferramentas de Windows login;

q) Deve permitir criar políticas por usuário e grupos para tráfego de VPN client-to-site;

r) Deve suportar autoridade certificadora integrada ao gateway VPN ou à solução de gerenciamento centralizado ou CA externa de terceiros;

s) Deve promover a integração com diretórios LDAP e Active Directory para a autenticação de usuários de VPN e regras de acesso;

t) Deve suportar os métodos de autenticação de VPN: usuário e senha de base interna do próprio equipamento, usuário e senha de diretório LDAP, usuário e senha do Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado ou CA externa de terceiros, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil;

u) Deve suportar a integração com autoridades certificadoras de terceiros quepossam gerar certificados no formato PKCS#12;

v) Deve suportar a solicitação de emissão de certificados à uma autoridade certificadora de confiança (enrollment) via SCEP (Simple Certificate Enrollment Protocol) ou CSR (Certificate Signing Requests);
w) Deve suportar a leitura e verificação de CRLs (certification revogation lists);

x) Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.

XIV – Características de alta disponibilidade:

a) Deve operar em alta disponibilidade (HA) nativamente no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo com no mínimo 2 (dois) membros, com sincronismo de estados integrado;
b) Deve suportar o balanceamento de carga interno na arquitetura ativo/ativo;

c) Deve sincronizar: todas as configurações, sessões TCP/IP, tabelas NAT, listas e assinaturas utilizadas para controle de acesso à Internet e proteção contra ameaças, tabelas FIB, associações de segurança das VPNs;

d) Deve monitorar a falha dos links de comunicação;

e) Deve ser capaz de identificar e iniciar automaticamente um procedimento de failover sempre que ocorrer: a falha de um dos membros do cluster, a falha de qualquer componente ou processo crítico de um dos membros do cluster, a falha de um dos links de comunicação monitorados;

f) Deve ser capaz de realizar os procedimentos de failover sem perda das conexões ativas, interrupções de tráfego.

XV – Funcionalidades da Gerência Centralizada:

a) A solução deve ser do tipo "appliance virtual" – solução de software baseada em máquina virtual, conforme os padrões estabelecidos pelo DMTF (Distributed Management Task Force), ou sistema operacional desenvolvido pelo próprio fabricante da solução de gerenciamento que possa ser instalado e executado em ambiente virtual – compatível com VMware vSphere 5.5 ou superior. Será aceito combinação de dois appliances virtuais, para compor solução de gerenciamento centralizado e armazenamento de logs;

b) Deve estar licenciada e permitir a gerência centralizada de todos os equipamentos e contextos virtuais que compõem a solução de alta disponibilidade;

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

d) Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõe a solução de alta disponibilidade;

e) Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os clusters;

f) Deve suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas de Next Generation Firewall,

filtragem de URLs, monitoração de logs, debugging, troubleshooting e captura de pacotes;

g) Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura;

h) Deve permitir, de forma granular, assinalar permissões para os administradores criarem outros usuários, alterar configurações, ler configurações, etc;

i) Deve permitir a delegação de funções de administração;

j) Deve suportar o bloqueio de alterações, evitando o conflito de configurações entre diferentes administradores efetuando alterações simultaneamente;

k) Deve registrar em log de auditoria as ações dos usuários administradores;

l) Deve suportar a identificação e utilização de usuários nas políticas de segurança, na forma do item VI acima;

m) Deve suportar agrupamento lógico de objetos ("object grouping") para criação de regras;

n) Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas;

o) Deve contabilizar a utilização ("hit counts") ou o volume de dados trafegados correspondente a cada regra de filtragem ("Access Control Entry") individualmente;

p) Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

q) Deve permitir distribuição centralizada de pacotes de atualização;

r) Deve ser capaz de testar a conectividade dos equipamentos gerenciados;

s) Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos;

t) Deve permitir localizar em quais regras um objeto está sendo utilizado;

u) Deve prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes, regras equivalentes ou um conjunto de regras que possa ser condensado em uma única regra;

v) Deve permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico);

w) Deve suportar a geração de alertas automáticos via email, SNMP ou syslog;

x) Deve suportar rollback de configuração para a última configuração salva;

y) Deve permitir validar as regras antes de aplicá-las;

z) Deve permitir a visualização e comparação das configurações atual, anterior e antigas;

aa) Deve permitir a exportação automática e agendada de logs via SCP;

ab) Deve possuir relatórios de utilização dos recursos por aplicação, URLs, ameaças, etc;

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

ad) Deve permitir a criação de relatórios customizados;

ae) Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, em dereço IP de origem e destino, país de origem e destino, usuário e horário;

af) 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;

ag) Deve permitir a geração automática e agendada dos relatórios;

ah) Deve estar licenciada para receber pelo menos 10.000 (dez mil) registros de log por segundo e 100 GBytes de logs diários;

ai) Deve permitir a utilização de pelo menos 10 TBytes de espaço em disco.

XVI – Treinamento Especializados:

O serviço de capacitação deve consistir na oferta de treinamentos oficiais com abordagem prática voltada a todos os requisitos funcionais da solução contratada, tanto relativo a aspectos operacionais, que inclui a utilização prática de todas as principais funcionalidades da ferramenta, como administrativos, que inclui o gerenciamento, suporte e parametrização da solução;

a) Treinamento oficial para no mínimo 51 pessoas;

b) Voucher para treinamento oficial do fabricante;

c) A carga horária mínima do treinamento não poderá ser inferior a 40 horas, a turma conterá no mínimo 5 pessoas e máximo de 12 pessoas e a ementa deverá contemplar, no mínimo. Termo de Referência – Solução de Segurança de Redes;

d) Os treinamentos deverão ocorrer usando-se dois turnos diários de até 4 horas cada, com intervalos de 15 minutos em cada turno e 1 hora entre os turnos;

e) Os treinamentos deverão ser realizados no Brasil, em português, em uma das seguintes cidades: São Paulo, Rio de Janeiro ou Brasília;

f) O local de treinamento deverá possuir todas as facilidades para um perfeito desempenho das atividades incluindo os recursos áudio visuais e laboratórios necessários, sem ônus algum para o Contratante;

g) Toda a documentação didática necessária aos cursos de treinamento deverá ser disponibilizada em papel impresso e mídia digital;

h) Todos os recursos didáticos necessários à realização do treinamento, incluindo, sala de aula, datashow, apostilas, bloco de anotações e caneta para cada treinando em cada turno de treinamento, deverão ser fornecidos pela entidade responsável pela realização do treinamento;

i) São produtos esperados de todos os treinamentos:

i.1) Aulas presenciais teóricas e práticas;

i.2) Material didático previamente submetido e aprovado pelo Contratante;

i.3) Referências para estudos e pesquisas complementares;

j) O Contratante poderá, a seu critério, reproduzir o material didático usado e treinar multiplicadores para repetir o treinamento sem custos adicionais;

k) Fornecimento de certificado de participação no curso com descrição e carga horária, nome do participante e escrito em português;

l) Os custos referentes ao deslocamento, hospedagem e alimentação dos treinandos serão de responsabilidade do Contratante;

XVII – Transceivers Opticos:

a) Transceivers SFP+ 10GB-LR;

a.1) Alcance até 10km utilizando fibra óptica monomodo (SMF, G.652);

a.2) Compatibilidade com o padrão de operação 10GBASE-LRL (Alcance de até 1 km utilizando fibra monomodo);

b) Transceivers SFP+ 10GB-SR;

b.1) Alcance até 300m utilizando fibra óptica multimodo 2000 MHz*km (MMF OM3);

b.2) Compatibilidade com o padrão de operação 10GBASE-SRL (Alcance de até 100m utilizando fibra multimodo);

c) Transceivers SFP 1GB-LX;

c.1) Alcance até 10 km utilizando fibra monomodo ;

d) Transceivers SFP 1GB-SX;

d.1) Alcance até 550m utilizando fibra multimodo na seguinte especificação: 500 MHz km MMF (OM2);

e) Transceivers SFP 1GB-TX;

e.1) Alcance até 100 metros e compatibilidade com cabo par trançado categoria 5, suportando os padrões de 100 Megabit e 1 Gigabit Ethernet.

CLÁUSULA TERCEIRA – DA EXECUÇÃO DO CONTRATO

A prestação dos serviços obedecerá ao seguinte:

I – Da Entrega e Instalação:

Caberá a CONTRATADA a elaboração e execução do plano de implementação dos novos equipamentos e software de gerenciamento, envolvendo:

a) Instalação dos equipamentos novos, sem prejuízo da operação da rede atual;

b) Documentação de Planejamento e implementação detalhada do equipamento adquirido;

c) Substituição dos firewalls existentes;

d) Configuração das funcionalidades Next Generation Firewall, IPS, proteção avançada contra ameaças, QoS, controle de aplicativos e VPN IPSEC;

e) Migração das regras de firewall e NAT existentes;

f) Criação dos usuários administradores;

g) Criação de perfis de usuários da VPN IPSEC;

h) Customização de regras de acesso de acordo com as necessidades do TRT;

i) Integração com o LDAP ou Active Directory;

j) Realização de backup das configurações;

k) Operação Assistida de Funcionamento da Solução, que consiste da disponibilização de um técnico residente, das 8h às 17h, com intervalo para almoço, no endereço do CONTRATANTE, devidamente identificado, para sanar quaisquer dúvidas e problemas que ocorrerem na operação da solução;

k.1) Este técnico deverá ser certificado pelo fabricante do equipamento;

k.2) Esta operação assistida será efetuada durante dois dias contados a partir da instalação do equipamento;

l) Testes de Aceite e Funcionamento;

m) Fornecimento da documentação de todo o projeto;

n) A instalação dos equipamentos deverá ser efetuada pela CONTRATADA ou Fabricante, conforme orientação do Serviço de Infraestrutura, observados os seguintes itens:

n.1) Todos os componentes necessários para o correto funcionamento dos equipamentos ofertados devem ser fornecidos pela CONTRATADA;
n.2) Caberá à CONTRATADA ou Fabricante a montagem dos equipamentos no RACK, já existente;

o) A entrega deverá ocorrer no prazo máximo de 60 dias a contar da emissão da nota de empenho. A não entrega no prazo especificado ocasionará multa de 2% no valor total do contrato.

II – Garantias:

A CONTRATADA fornecerá solução de alta disponibilidade de Next Generation Firewall com gerenciamento centralizado e integrado; com garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local ou remoto, 8x5 (das 08:00 às 12:00 e das 14:00 às 18:00), pelo prazo de 60 (sessenta) meses; incluindo serviços de instalação e treinamento personalizado, sem custos adicionais à CONTRATANTE, nos prazos e condições estipuladas neste documento e seus anexos.

a) Entende-se por garantia de funcionamento todos os serviços e atividades necessários para manter a solução em perfeito estado de funcionamento, tais como: manutenção corretiva, substituição de peças e componentes, atualizações de versões, revisões e/ou distribuições (releases) e correções (patches) dos programas (softwares, firmwares, drivers), ajustes técnicos, etc;

b) A garantia de funcionamento deverá ser prestada no mínimo em regime 8x5 (das 08:00 às 12:00 e das 14:00 às 18:00) (8 horas por dia, 5 dias por semana);

c) Entende-se por atualização de assinaturas de proteção todos os serviços e atividades, manuais ou automatizados, necessários para manter a solução em seu nível de identificação e proteção mais atualizado, tais como: atualização de assinaturas de prevenção de intrusão, assinaturas de identificação de vírus, assinaturas de identificação de aplicações, listas de classificação de URLs, listas de geolocalização, listas de endereços IP's utilizados por botnets, listas de endereços IP's de reputação duvidosa, etc;

d) A atualização de assinaturas de proteção deverá ser prestada conforme as Especificações Técnicas constantes neste documento e seus anexos;

e) Entende-se por suporte técnico todos os serviços e atividades necessários ao esclarecimento de dúvidas ou orientação técnica da Equipe Técnica do CONTRATANTE, visando ao uso adequado e otimizado da solução;

f) O suporte técnico deverá disponibilizar o acesso, por meio da Internet, de base de documentos e conhecimentos mantida pela fabricante da solução, contemplando seus manuais de instalação, utilização e correção de problemas, bem como dicas de utilização, configuração e melhores práticas de uso, dentre outros.

III – Do Prazo e Condições de entrega:

O prazo de entrega e instalação da solução será de, no máximo, 60 (sessenta) dias corridos, contados a partir da assinatura do contrato;

IV – Análise do atendimento a políticas socioambientais:

Seguindo as políticas socioambientais do Tribunal, todos os equipamentos no final de seus contratos, se não existir renovação serão doados para nova utilização ou para serem descartados da maneira mais correta, evitando impacto ao meio ambiente ou ajudando outros órgãos da administração pública a terem equipamentos sem necessidade de compra.

a) Se forem passíveis de renovação, e a tecnologia estiver ainda em uso, está será efetuada para garantir o maior retorno do investimento feito;

b) Todo o descarte de peças e embalagens será feita segundo as portarias em vigor no ato do descarte.

V - Conformidade Técnica e Legal:

Técnica:

A presente contratação deve observar a Resolução n.º 182, de 17 de outubro de 2013, que "Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ)."

Legal:

- A Contratada deverá seguir todas as Normas, Políticas e Procedimentos de Segurança estabelecidas pelo Contratante para execução do Contrato, tanto nas dependências do Contratante como externamente., bem como manter sob sigilo, sob pena de responsabilidade civil, penal e administrativa, todo e qualquer assunto de interesse do Tribunal ou de terceiros de que tomar conhecimento em razão da prestação do serviço.

- A presente contratação deve observar a Lei n.° 8.666, de 21 de junho de 1993, que institui normas para licitações e contratos da Administração Pública.

VI – Forma de comunicação entre as Partes:

A comunicação entre as partes dar-se-á por meio de mensagens de correio eletrônico, atendimentos registrados com número de protocolo único e que podem ser efetuados por telefone, sítio na Internet ou mensagens de correio eletrônico, ligações telefônicas para a central de atendimento da Contratada ou números telefônicos do contratante.

VII – Dos Níveis Mínimos de Serviço (NMS):

O fornecedor contratado deverá assegurar a disponibilidade da solução conforme os Níveis Mínimos de Serviço

(NMS), através de número telefônico específico para o fim ou e-mail na forma abaixo estabelecida:

a) No momento da abertura do chamado, será informada a prioridade para o atendimento de acordo com as seguintes definições:

- Prioridade 1 (Crítica): Este Nível de severidade é aplicado em situações de emergência ou problema crítico, caracterizado pela existência de ambiente paralisado;

- Prioridade 2 (Alta) : Este nível de severidade é aplicado em situações de alto impacto, incluindo os casos de degradação severa de desempenho da solução. Também se aplica a esta severidade casos onde um appliance para de funcionar, ocasionando a perda da alta disponibilidade da solução. Outros exemplos para esta severidade: Perda de redundância, reinicialização de módulos, slots ou portas com defeitos, perda de funcionalidades;

- Prioridade 3 (Média): Este nível de severidade é aplicado em situações de baixo impacto ou de problemas que se apresentam de forma intermitente;

- Prioridade 4 (Baixa): Este nível de severidade é aplicado em situações de dúvidas técnicas em relação ao uso ou à implementação da solução;

Prazos	prioridade			
	1	2	3	4
Início do atendimento	Até 30 minutos após a abertura do chamado	Até 1 hora após a abertura do chamado	Até 4 horas após a abertura do chamado	Até 8 horas após a abertura do chamado
Solução definitiva	Em até 6h do início do atendimento	Em até 12h do início do atendimento	Em até 24h do início do atendimento	Em até 72h do início do atendimento
Tolerância mensal de descumprimento	0	1	2	3

b) Caso existam ocorrências que ultrapassem os níveis de tolerância informados na tabela acima, serão aplicadas as penalidades previstas no § 1º da cláusula dezessete;

c) As ocorrências terão seu tempo de resposta pausado às 00h00min, voltando a correr às 06h00min e correrão normalmente em feriados e finais de semana, com exceção do intervalo de tempo acima;

d) Os atendimentos às solicitações de severidade crítica ou alta deverão ser realizados nas instalações do CONTRATANTE (on-site) e não poderão ser interrompidos até o completo restabelecimento dos serviços, salvo em casos excepcionais, autorizados pelo CONTRATANTE, mesmo que se estendam por períodos noturnos, sábados, domingos e feriados. Tal situação não implicará em custos adicionais ao CONTRATANTE;

e) Os atendimentos às solicitações de severidade média poderão ser realizados remotamente ou nas instalações do CONTRATANTE (on-site), conforme o caso, e não poderão ser interrompidos até o completo restabelecimento dos serviços, salvo em casos excepcionais, autorizados pelo CONTRATANTE, mesmo que se estendam por períodos noturnos, sábados, domingos e feriados. Tal situação não implicará em custos adicionais ao CONTRATANTE;

f) Os atendimentos às solicitações de severidade baixa poderão ser realizados remotamente, de segunda à sexta-feira, respeitando o horário de funcionamento do CONTRATANTE. Caso seja necessário o atendimento nas instalações do CONTRATANTE (on-site), tal situação não implicará custos adicionais ao CONTRATANTE;

g) A interrupção do atendimento de uma solicitação, de quaisquer das severidades, por parte da CONTRATADA sem prévia autorização da Equipe Técnica do CONTRATANTE será caracterizada como um descumprimento mensal para efeitos de aplicação dos descontos apresentados na cláusula dezessete, § 1º;

h) Concluído o atendimento, a CONTRATADA comunicará o fato à Equipe Técnica do CONTRATANTE e solicitará autorização para o fechamento do chamado. Caso o CONTRATANTE não confirme o pleno atendimento da solicitação, o chamado permanecerá aberto até que seja efetivamente atendido. Nesse caso, a Equipe Técnica fornecerá as pendências relativas à solicitação em aberto;

i) O CONTRATANTE encaminhará formalmente à CONTRATADA, quando da reunião de apresentação inicial, a relação nominal da Equipe Técnica autorizada a abrir e fechar solicitações de suporte técnico;

j) Todas as solicitações de atendimento serão registradas pelo fiscal do contrato e pela CONTRATADA, para acompanhamento e controle da execução do contrato;

k) A CONTRATADA apresentará um Relatório de Atendimento, enviado por meio de correio eletrônico, contendo datas e horas de chamada, de início e de término do atendimento, descrição da necessidade de atendimento, e as providências adotadas e toda e qualquer informação pertinente ao chamado após o encerramento do mesmo;

l) A equipe técnica do CONTRATANTE informará à CONTRATADA quanto ao recebimento e aceite do Relatório de Atendimento;

m) Na abertura do chamado a CONTRATADA deverá fornecer o número de protocolo e o horário de abertura e encaminhar mensagem de correio eletrônico com tais informações para os endereços dos fiscais do contrato em até meia hora após o registro, procedimento que servirá como evidência em caso de contestação de penalidades. O cálculo para aferição da desconformidade do tempo de resposta considerará o tempo de resposta descrito nos níveis mínimos de serviço;

n) Para fins de aferição dos níveis mínimos de serviço, ao final, o chamado será considerado: completamente atendido ou não atendido, não havendo possibilidade de atendimento parcial;

o) Quando a solução depender de ações do CONTRATANTE o tempo de solução do chamado deve ser pausado até a conclusão da parte que não cabe a contratada, depois continuar de onde havia parado antes da solicitação do outro ator no processo;

p) Todas as ações provenientes de um chamado deverão ser amplamente comunicadas ao CONTRATANTE. Sendo que o CONTRATANTE deverá ser comunicado no mínimo em dois momentos, no início e no final de cada atendimento;

q) Os níveis mínimos de serviço serão aferidos mensalmente e eventuais descumprimentos atestados no Termo de Aceite Provisório;

r) Toda indisponibilidade causada pela CONTRATADA, poderá gerar multa de acordo com o NMS descrito acima;

s) Faculta-se à CONTRATADA substituir temporariamente um componente defeituoso por outro de mesmas características técnicas, ou superior;

t) A CONTRATADA deverá realizar a substituição definitiva do referido componente no prazo de 30 (trinta) dias corridos;

t.1) A substituição definitiva de componentes, caso necessária, deverá ser feita por itens novos e para primeiro uso;

u) A critério do CONTRATANTE, a CONTRATADA substituirá, em caráter definitivo, o componente já instalado, por um novo e para primeiro uso, em perfeito estado de funcionamento, no prazo de 30 (trinta) dias corridos, em quaisquer dos seguintes casos:

u.1) Ocorrência de 3 (três) ou mais defeitos que comprometam o seu perfeito funcionamento, dentro de um período qualquer de 30 (trinta) dias corridos; e

u.2) Somatório dos tempos de paralisação de quaisquer componentes que ultrapasse 15 (quinze) horas dentro de um período qualquer de 30 (trinta) dias corridos;

v) Qualquer substituição de componente, temporária ou definitiva, só será permitida após prévia avaliação técnica e autorização por parte da Equipe Técnica do CONTRATANTE.

VIII – Requisitos Técnicos Específicos que deverão ser atendidos pela Contratada:

Para os equipamentos:

a) Os componentes utilizados para manutenção do equipamento deverão ser novos, e entregues montados, instalados e configurados dentro dos ambientes de Datacenter dos órgãos contratantes;

b) Os componentes deverão ser fornecidos com todos os itens acessórios de hardware e software necessários a sua perfeita instalação e funcionamento, incluindo cabos, fibras, conectores, interfaces, suportes, drivers de controle, programas de configuração, etc;

c) As peças e equipamentos que compõem a solução de Next Generation Firewall, deverão manter total compatibilidade entre si, devendo manter o padrão de funcionamento utilizado pelos contratantes;

d) Os componentes deverão ser entregues acompanhados de suas documentações técnica completa e atualizada em português, contendo manuais, guias de instalação, devendo ser fornecida em sua forma original não sendo aceitas cópias de qualquer tipo;

d.1) Caso não exista documentação original em português, será aceita documentação original, desde que na língua inglesa;

e) Todos os drivers atualizados dos componentes necessários ao perfeito funcionamento e operação do equipamento devem ser disponibilizados aos Tribunais em sítio da Internet ou por meio de atendimento aos chamados técnicos;

f) Os componentes deverão ter identificação do fabricante com número de série único, registrado na BIOS, do equipamento para abertura de chamado;

g) Todas as despesas da equipe técnica responsável pela montagem e instalação dos componentes correrão por conta do fornecedor.
Para os serviços:

a) As novas versões dos produtos deverão ser entregues acompanhadas e suas documentações técnica completa e atualizada em português, contendo manuais, guias de instalação que poderão ser entregues em formato eletrônico;

a.1) Caso não exista documentação original em português, será aceita documentação original, desde que na língua inglesa;

b) Todas as despesas da equipe técnica responsável pela solução de problemas e instalação dos produtos correrão por conta do fornecedor.

Parágrafo único - Os prazos de adimplemento das obrigações admitem prorrogação nos casos especificados no § 1º do art. 57 da Lei 8666/93, e a solicitação dilatória, que deverá ser sempre por escrito, fundamentada e instruída com os documentos necessários à comprovação das alegações, deverá ser recebida antes do encerramento dos prazos máximos, cabendo ao Contratante autorizar novo prazo.

CLÁUSULA QUARTA - DO RECEBIMENTO DO OBJETO

Nos termos das alíneas “a” e “b” do inciso I do art. 73 c/c art. 15, § 8º, ambos da Lei nº 8.666/93, o objeto será recebido:

• **Provisoriamente**, no momento do recebimento dos equipamentos e, mediante Termo de Recebimento Provisório assinado, para efeito de posterior verificação de que os mesmos se encontram operacionais e em condições de serem recebidos. O recebimento provisório consiste na identificação e conferência dos equipamentos, com ênfase na integridade física e quantitativa.

• **Definitivamente**, para os Itens 2, 4, 7, 8, 9 e 10, definitivamente, mediante Termo de Recebimento Definitivo, assinado, e após instalação que comprove a operacionalidade do equipamento e a adequação dos equipamentos às exigências das cláusulas contratuais e da proposta da CONTRATADA. O período de garantia dos equipamentos terá início somente a partir do recebimento definitivo dos bens; Para o Item 5, o recebimento definitivo ocorrerá após a emissão e entrega dos certificados do treinamento.

§ 1º - A Contratada é obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, *ex vi* do art. 69 da Lei nº 8.666/93, ainda que essa verificação se dê após o recebimento definitivo.

§ 2º - O Contratante rejeitará, no todo ou em parte, *obra, serviço ou fornecimento* executado em desacordo com este contrato, *ex vi* do art. 76 da Lei nº 8.666/93.

CLÁUSULA - QUINTA – DA VIGÊNCIA

O contrato vigorará por 60 (sessenta) meses, a partir da data da assinatura, obedecido o período admitido na legislação em vigor (art. 57, inc. II, da Lei nº 8.666/93, conforme nova redação que lhe deu a Lei n° 9.648/98).

§ 1º - O prazo de vigência não se confunde com o prazo de execução de que trata a cláusula terceira.

§ 2º - O Contratante convocará a Contratada para assinar termo aditivo ou instrumento equivalente dentro do prazo de 10 (dez) dias, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei n° 8.666/93 e demais sanções administrativas dispostas na cláusula dezessete, não restritivas a estas.

§ 3º – O início da contagem do prazo a qual refere-se o parágrafo anterior dar-se-á a partir do primeiro dia útil seguinte ao aviso eletrônico ou comunicação escrita encaminhada à Contratada. O ato convocatório será realizado preferencialmente via e-mail.

CLÁUSULA SEXTA – DAS PRERROGATIVAS DO CONTRATANTE

São as seguintes as prerrogativas da Administração, conferidas em razão do regime jurídico dos contratos administrativos instituídos pelo art. 58 da Lei nº 8.666/93, em relação a eles:

a) modificá-lo, unilateralmente, para melhor adequação às finalidades de interesse público, respeitados os direitos da Contratada;

b) rescindi-lo, unilateralmente, nos casos especificados no inc. I do art. 79;
c) fiscalizar-lhe a execução;

d) aplicar sanções motivadas pela inexecução total ou parcial do ajuste.

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATADA

A Contratada se obriga a:

a) observar e cumprir, estritamente, os termos da proposta e as condições ora estabelecidas, obedecendo a critérios e prazos acordados pelas exigências técnicas constantes do edital;

b) manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

b.1) a regularidade fiscal e trabalhista deverá ser mantida durante todo o período contratual, sob pena de rescisão contratual e de execução da retenção sobre os créditos da empresa e/ou da eventual garantia, a título de multa, para ressarcimento dos valores e indenizações devidos à Administração, além das penalidades previstas em lei;

c) a Contratada que for Optante pelo Simples Nacional deverá apresentar a Declaração, conforme modelo constante no Anexo IV da Instrução Normativa nº 1.234/2012 da Receita Federal do Brasil, no momento da apresentação da primeira nota fiscal/fatura decorrente da assinatura do contrato ou da prorrogação contratual;

c.1) a Contratada deverá informar imediatamente qualquer alteração da sua permanência no Simples Nacional;

d) prestar todos os esclarecimentos que forem solicitados pelo responsável pelo acompanhamento e fiscalização da execução do Contrato;

e) obedecer, no que couber, aos princípios e normas de condutas estabelecidas no Código de Ética do Contratante;

f) manter serviço de registro de incidentes, serviço de assistência técnica e auxílio para configurações da rede disponíveis por telefone e meio eletrônico.

CLÁUSULA OITAVA – DAS OBRIGAÇÕES DO CONTRATANTE

O Contratante se obriga a:

a) acompanhar a execução do contrato, nos termos do inciso III do art. 58 c/c o art. 67 da Lei nº 8.666/93, através dos responsáveis pelo acompanhamento e fiscalização da execução do contrato, que exercerá ampla e irrestrita fiscalização do objeto do presente contrato, a qualquer hora, determinando o que for necessário à regularização das faltas ou defeitos observados, inclusive quanto às obrigações da Contratada;

b) proporcionar todas as facilidades necessárias à boa execução deste contrato;

c) efetuar os pagamentos devidos à Contratada, nos prazos e condições ora estabelecidos;

d) prestar as informações e esclarecimentos que venham a ser solicitados pela Contratada.

CLÁUSULA NONA – DA GESTÃO E FISCALIZAÇÃO DA EXECUÇÃO DO CONTRATO

As atividades de fiscalização e acompanhamento da execução dos contratos, em conformidade com as disposições contidas no inciso III do art. 58 c/c o art. 67 da Lei nº 8.666/93, nos arts. 2º, 3º e 4º da Portaria PRESI nº 243/10, e no art. 2º, inciso XII, alíneas “a”, “b” e “c” da Resolução CNJ 182/13, serão executadas pelos servidores designados pela Diretoria Geral, devendo ser informada à Contratada.

§ 1º – Caberá ao Gestor do Contrato, as atribuições de:

a) gerir a execução contratual.

b) acompanhar e cobrar as ações de fiscalização efetuadas pelos fiscais;

c) comunicar a Administração as possíveis anomalias, bem como as necessidades de prorrogação ou não dos contratos sob sua responsabilidade.

§ 2º – Caberá aos Fiscais Demandante e Técnico, as atribuições de:

a) fiscalizar a execução do presente contrato, de modo a que sejam cumpridas, integralmente, as condições constantes de suas cláusulas;

b) comprovar e relatar por escrito as eventuais irregularidades;

c) determinar o que for necessário à regularização de faltas ou defeitos verificados, podendo sustar a execução de quaisquer trabalhos, em casos de desacordo com o especificado ou por motivo que caracterize a necessidade de tal medida;

d) exigir que a Contratada mantenha organizado e atualizado um sistema de controle relativo ao cumprimento de suas obrigações, assinado por seu representante e pelo fiscal indicado no *caput* desta cláusula ou por servidor por ele designado;

e) verificar a conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do contrato.

§ 3º – Caberá aos Fiscais Administrativos, as atribuições de:

a) controlar os prazos de vigência e de reajuste dos contratos;

b) apreciar preliminarmente os pedidos de reajuste, repactuação e revisão contratuais;

c) verificar, ao longo de todo o contrato, a manutenção das condições de qualificação e habilitação das empresas contratadas;

d) efetuar o cálculo da multa moratória e compensatória.

§ 4º - A fiscalização exercida pelo Contratante não excluirá ou reduzirá a responsabilidade da Contratada pela completa e perfeita execução do objeto contratual, tampouco restringe a responsabilidade integral e exclusiva da Contratada quanto à integralidade e à correção dos fornecimentos a que se obrigou, suas consequências e implicações perante terceiros, próximas ou remotas.

§ 5º - A Contratada declara aceitar, integralmente, todos os métodos e processos de inspeção, verificação e controle a serem adotados pelo Contratante.

CLÁUSULA DEZ – DO PREPOSTO DA CONTRATADA

A Contratada deverá, às suas expensas, manter preposto, aceito pelo Contratante, para representá-lo na execução do contrato, obedecido o disposto no art. 68 da § 1º – Caso houver necessidade de substituição do preposto, a nova indicação deverá ser informada por escrito ao Contratante (contendo telefone, celular, *e-mail* e endereço), podendo ser realizada por meio eletrônico ao fiscal do contrato, no prazo máximo de até 07 (sete) dias corridos após a substituição.

§ 2º – A indicação do novo preposto deverá ser juntada aos autos do processo correspondente pelo fiscal.

§ 3º – O preposto deverá possuir os conhecimentos e a capacidade profissional compatíveis com a função e ter competência para resolver todo e qualquer assunto relacionado com os serviços prestados.

§ 4º – O Contratante poderá, a seu exclusivo critério, rejeitar a indicação do preposto se julgar que os requisitos exigidos não foram cumpridos, e solicitar a sua substituição, a qualquer tempo, no prazo máximo de 3 (três) dias a contar da notificação, que poderá ser feita por meio de *e-mail*.

CLÁUSULA ONZE – DO PREÇO

O valor do presente contrato é de **R$ 653.000,00** (seiscentos e cinqüenta e três mil reais), assim discriminado:

ITEM	DESCRIÇÃO	QTIDADE	VLR UNIT	VLR TOTAL
2	Solução de alta disponibilidade de Next	01	R$ 580.000	**R$ 580.000,00**

	Generation Firewall *Cluster* com 2 *appliances Firewal* / NG Tipo 2			
4	Solução de alta disponibilidade de Next Generation Firewall *Cluster* com 2 *appliances Firewal* / NG Tipo 3	01	R$ 35.000,00	**R$ 35.000,00**
5	**Solução de gerenciamento centralizado e integrado**	05	R$ 4.000,00	**R$ 20.000,00**
7	**Transceiver SFP+ 10GB-SR**	08	R$ 1.000,00	**R$ 8.000,00**
8	**Transceiver SFP 1GB-LX**	08	R$ 1.000,00	**R$ 8.000,00**
9	**Transceiver SFP 1GB-SX**	02	R$ 500,00	**R$ 1.000,00**
10	**Transceiver SFP 1GB-TX**	02	R$ 500,00	**R$ 1.000,00**

Parágrafo único - Estão incluídas no preço todas as despesas relativas à consecução eficiente e integral do objeto deste contrato.

CLÁUSULA DOZE – DA LIQUIDAÇÃO E DO PAGAMENTO

A liquidação e o pagamento serão assim efetuados:

a) a Contratada poderá apresentar o documento de cobrança corretamente preenchido, à Seção de Cadastramento Processual, situado no térreo do prédio-sede, situado à Avenida Senador Vitorino Freire, 2001, Areinha. São Luís/MA. CEP 65030-015.

b) a Fiscalização deverá proceder a certificação de que trata o art. 3º, § 5º da Portaria PRESI nº 243/10;

c) o pagamento deverá ser em parcela única, em até 30 (trinta) dias após a emissão do termo de recebimento definitivo;

d) para todos os fins, considera-se como data de pagamento, o dia da emissão da ordem bancária;

e) os pagamentos serão realizados de acordo com o cronograma de desembolso do Governo Federal, em moeda corrente nacional, sendo efetuada a retenção na fonte dos tributos e contribuições elencados nas

disposições determinadas pelos órgãos fiscais e fazendários em conformidade com as instruções normativas vigentes;

f) havendo erro na (s) nota (s) fiscal (is)/fatura (s) ou qualquer circunstância que impeça a liquidação da despesa, aquela será restituída ou será comunicada a irregularidade à Contratada, ficando pendente de pagamento até que esta providencie as medidas saneadoras. Nesta hipótese, o prazo para o pagamento iniciar-se-á após a regularização da situação e/ou a reapresentação do documento fiscal, não acarretando qualquer ônus para o Contratante;

g) a Contratada será a responsável direta pelo faturamento a que se propõe, não podendo ser aceito documento de cobrança (nota fiscal/fatura) emitido por empresa com Cadastro Nacional de Pessoa Jurídica – CNPJ diferente ao daquela, ainda que do mesmo grupo empresarial, excepcionando-se, apenas, o CNPJ da filial da Contratada do Estado onde os serviços serão efetivamente prestados;

h) a Contratada deverá apresentar, sempre que solicitado pelo Contratante, as certidões abaixo discriminadas:

• CRF – Certificado de Regularidade do FGTS, emitido pela CEF;

• Certidão Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União, emitida em conjunto pela Secretaria da Receita Federal e Procuradoria- Geral da Fazenda Nacional.

• CNDT - Certidão Negativa de Débitos Trabalhistas, emitida pela Justiça do Trabalho;

• Prova de regularidade para com a Fazenda Estadual do seu domicílio ou de sua sede;

• Prova de regularidade para com a Fazenda Municipal do seu domicílio ou de sua sede;

i) o descumprimento reiterado da obrigação da apresentação das certidões elencadas na alínea anterior e a manutenção em situação irregular perante as obrigações fiscais e trabalhistas poderão dar ensejo à rescisão contratual, respeitada a ampla defesa, em face de configurada a inexecução do contrato e a ofensa à regra trazida no art. 55, inciso XIII, da Lei nº 8.666/1993;

j) o Contratante poderá reter o pagamento dos valores referentes ao fornecimento realizado nas hipóteses da cláusula dezesseis, limitado ao valor do dano, ressalvada a possibilidade de rescisão contratual;

k) o Contratante poderá deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela Contratada, nos termos deste contrato;

l) no ato do pagamento será retido na fonte o Imposto sobre a Renda de Pessoa Jurídica, a contribuição sobre o lucro, a contribuição para a seguridade social (CONFINS) e a contribuição para O PIS/PASEP, todos da Secretaria da Receita Federal. No entanto, não recairá esta retenção sobre pessoas jurídicas que apresentarem a Declaração de Optante do Simples, conforme modelo constante no Anexo IV da Instrução Normativa nº. 1.234/2012 , da Receita Federal ou cópia da Consulta ao Portal do Simples Nacional da apresentação da primeira nota fiscal/fatura decorrente de assinatura contratual e de prorrogação contratual.

CLÁUSULA TREZE – DO REAJUSTE

Os preços constantes do contrato serão reajustados, respeitada a periodicidade mínima de um ano a contar da data limite para apresentação da proposta ou da data do último reajuste, limitado o reajuste à variação do **Índice Nacional de Preços ao Consumidor Amplo** - IPCA, publicado pelo Instituto Brasileiro de Geografia e Estatística – IBGE, ou de outro índice que passe a substituí-lo, e na falta deste, em caráter excepcional, será admitida a adoção de índices gerais de preços de acordo com a seguinte fórmula:

$$R = \frac{I - Io}{Io} \times P, \text{ onde:}$$

R = reajuste procurado;
I = índice relativo ao mês de reajuste;
Io = índice relativo ao mês da data limite para apresentação da proposta;

P = preço atual dos serviços/contrato;

§ 1º - Em caso de ocorrência de deflação ou qualquer outro evento que possa implicar redução do valor contratual para adequá-lo aos preços de mercado, será provocada pelo Contratante mediante a apresentação de planilha com demonstração analítica da variação dos componentes dos custos do contrato no período correspondente, com vistas à definição do novo valor contratual a ser aplicado.

§ 2º - O valor e a data do reajuste serão informados no contrato mediante apostila.

CLÁUSULA CATORZE – DA DOTAÇÃO ORÇAMENTÁRIA

O recurso para atender à despesa acima correrá por conta do orçamento próprio, Programa de Trabalho 02.126.0571.2C73.0001 – Manutenção do Sistema Nacional de Tecnologia da Informação, Natureza da Despesa: 3390-30 – Material de Consumo; 3390.39 – Outros Serviços de Terceiros – PJ; 4490.39 – Outros Serviços de Terceiros – PJ; 4490.52 – Equipamentos e Material Permanente.

CLÁUSULA QUINZE – DA SUBCONTRATAÇÃO

É vedada a transferência ou cessão do contrato, assim como consórcio entre empresas para participar do certame.

CLÁUSULA DEZESSEIS - DA RESPONSABILIDADE CIVIL

A Contratada é responsável pelos danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo Contratante, *ex vi* do art. 70 da Lei nº 8.666/93.

CLÁUSULA DEZESSETE – DAS SANÇÕES ADMINISTRATIVAS

Pela inexecução total ou parcial do contrato, a Administração poderá, garantida a ampla defesa, aplicar à Contratada as seguintes sanções:

§ 1º – Em razão do nível de impacto, conforme cláusula terceira, item VII:

a) No caso de não possibilidade de registro de chamados na CONTRATADA dentro do horário acordado, cada não atendimento será considerado descumprimento de nível mínimo de serviço com prioridade 1, com aplicação das penalidades nela previstas;

b) Não cumprimento do prazo estipulado para entrega estabelecido, que é de 60 dias após emissão da nota de empenho:

b.1) Atraso de 1 a 19 dias, resultará em multa de 0,013% do valor do contrato por dia de atraso;

b.2) Atrasos de 20 a 31 dias, resultará em multa de 0,013% do valor do contrato;

b.3) Atraso de mais de 32 dias poderá resultar em rescisão contratual;
c) Caso existam ocorrências que ultrapassem os níveis de tolerância informados na tabela constante da cláusula terceira, inc. VII, *alínea* "a", serão aplicadas as seguintes penalidades:

c.1) Multa:

c.1.1) De 0,013% (treze milésimos por cento) sobre o valor global do contrato, por cada hora ou fração de atraso na conclusão de atendimentos de prioridade 1 – crítica, até o limite de 2% (dois por cento) sobre o valor global do contrato, no mês de apuração;

c.1.2) De 0,010% (dez milésimos por cento) sobre o valor global do contrato, por cada hora ou fração de atraso na conclusão de atendimentos de prioridade 2 – alta, até o limite de 2% (dois por cento) sobre o valor global do contrato, no mês de apuração;

c.1.3) De 0,005% (cinco milésimos por cento) sobre o valor global do contrato, por cada hora ou fração de atraso na conclusão de atendimentos de prioridade 3 – média, até o limite de 1% (um por cento) sobre o valor global do contrato, no mês de apuração;

c.1.4) De 0,003% (três milésimos por cento) sobre o valor global do contrato, por cada hora ou fração de atraso na conclusão de atendimentos de prioridade 4 – baixa, até o limite de 1% (um por cento) sobre o valor global do contrato, no mês de apuração;

c.1.5) De 1% (um por cento) sobre o valor global do contrato, a cada mês em que for apurada a descontinuidade dos serviços de suporte técnico, atualizações de versões e de listas de assinaturas;

c.1.6) De 1% (um por cento) sobre o valor global do contrato, a cada mês em que for apurada a irregularidade da composição da Equipe de Atendimento Técnico da CONTRATADA;
d) A indisponibilidade do registro de incidentes, do serviço de assistência técnica e do auxílio para configurações da rede acarretará multa de 0.013%, do valor do contrato e a equipe de fiscalização deverá avaliar a conveniência de proceder o distrato.

§ 2º – Aos casos não previstos no § 1º, poderão ser aplicadas as seguintes sanções:

a) advertência, nos termos do inc. I do art. 87 da Lei nº 8.666/93, que será aplicada em caso de infrações que correspondam a pequenas irregularidades verificadas na execução do contrato, que venham ou não causar danos ao Contratante ou a terceiros.

b) multa:

b.1) multa moratória, nos termos do art. 86 da Lei nº 8.666/93: decorrente de atraso injustificado no cumprimento dos prazos estipulados, arbitrada em 0,3% (zero vírgula três por cento) por dia sobre o valor do(s) item(s) em mora, limitada a 10%;

b.2) multa compensatória, nos termos do inc. II do art. 87 da Lei nº 8.666/93:

b.2.1) por inexecução total: arbitrada em 10% (dez por cento) do valor total do contrato e aplicada na ocorrência das hipóteses enumeradas nos inc. I a XI e XVIII do art. 78 da Lei nº 8.666/93 das quais resulte inexecução do contrato com prejuízo para a Administração;

b.2.2) por inexecução parcial: arbitrada em 10% (dez por cento) do valor do item, e aplicada em dobro no caso de reincidência, nas hipóteses enumeradas nos inc. I a XI e XVIII art. 78 da Lei nº 8.666/93 das quais resulte execução parcial do contrato com prejuízo para a Administração;

b.3) 0,3% (zero vírgula três por cento) por dia sobre o valor total do contrato, limitada a 10%, e aplicada em dobro no caso de reincidência, pelo descumprimento das demais obrigações e condições determinadas no presente contrato não especificadas nas alíneas “b.1” e “b.2”, não eximindo a Contratada de outras sanções cabíveis;

b.4) multa de 1% (um por cento) sobre o valor da nota fiscal, a ser aplicada na ocorrência de violação da obrigação da manutenção da regularidade fiscal e trabalhista;

c) impedimento de licitar ou contratar com a União, pelo prazo de 05 (cinco) anos, sem prejuízo nos termos do art. 7º da Lei nº 10.520/02, que será aplicada nas seguintes hipóteses: não celebrar o contrato, deixar de entregar ou apresentar documentação falsa para o certame, ensejar o retardamento da execução do seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal;

d) declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior, ex vi do inc. IV do art. 87 da Lei nº 8.666/93, será imputada nas hipóteses previstas no inciso anterior, desde que a razoabilidade e proporcionalidade assim a recomendem;

f) as sanções previstas nas alíneas “a”, “c” e “d” poderão ser aplicadas junto com a da alínea “b”.

§ 3º – A multa moratória não impede que a Administração rescinda unilateralmente o contrato e aplique as outras sanções previstas nesta cláusula e na Lei nº 8.666/93.

§ 4º – O prazo para apresentação de defesa prévia contra as penalidades previstas nesta cláusula será de 5 (cinco) dias úteis, contados a partir da notificação.

CLÁUSULA DEZOITO – DA RESCISÃO

A inexecução total e a parcial do contrato fulcradas nos inc. I a XVIII do art. 78 ensejam a sua rescisão, que pode ser

determinada por ato unilateral e escrito da Administração, ou amigável, conforme os inc. I e II do art. 79, com as conseqüências contratuais e as previstas no art. 80, todos da Lei nº 8.666/93.

§ 1º – A rescisão poderá, ainda, ocorrer por conveniência da Administração, mediante notificação escrita, com antecedência mínima de 30 (trinta) dias.

§ 2º – O descumprimento reiterado da obrigação da apresentação das certidões elencadas na alínea "h" da cláusula doze e a manutenção em situação irregular perante as obrigações fiscais e trabalhistas poderão dar ensejo à rescisão contratual, respeitada a ampla defesa, em face de configurada a inexecução do contrato e a ofensa à regra trazida no art. 55, inciso XIII, da Lei nº 8.666/1993.

CLÁUSULA DEZENOVE – DOS RECURSOS ADMINISTRATIVOS

Dos atos da Administração decorrentes da aplicação da Lei nº 8.666/93 cabem recurso, representação e pedido de reconsideração, nos termos do art. 109.

CLÁUSULA VINTE – DA FUNDAMENTAÇÃO LEGAL E DA VINCULAÇÃO AO EDITAL E À PROPOSTA

I - O presente contrato fundamenta-se:

• na Lei nº 10.520/02;
• na Lei nº 8.666/93 e alterações posteriores, subsidiariamente;
• no Decreto nº 3.555/00;
• no Decreto nº 5.450/05;
• no Decreto nº 5.504/05;
• no Decreto nº 7.892/13.
• nos preceitos de Direito Público e, supletivamente, os princípios da Teoria Geral dos Contratos e as disposições de Direito Privado, nos termos do caput do art. 54 da Lei nº 8.666/93;
• no Decreto nº 6.106/07, alterado pelo Decreto nº 6.420/08;

II - E vincula-se aos termos:

• do edital do processo PRE 11926/2017, nos termos do inciso XI do art. 55 da Lei nº 8.666/93;
• da proposta da Contratada, nos termos do § 1º do art. 54 da Lei nº 8.666/93;

CLÁUSULA VINTE E UMA – DA INTIMAÇÃO DOS ATOS

A intimação dos atos relativos à rescisão do contrato a que se refere o inc. I do art. 79 da Lei nº 8.666/93, à suspensão temporária e à declaração de inidoneidade será feita mediante publicação na imprensa oficial (§ 1º do art. 109 da Lei nº 8.666/93).

CLÁUSULA VINTE E DUAS – DA ALTERAÇÃO DO CONTRATO

O disposto neste contrato somente poderá ser alterado pelas partes por meio de termos aditivos, asseguradas as prerrogativas conferidas à Administração enumeradas no caput do art. 58 da Lei nº 8.666/93 e na cláusula sexta, mediante a apresentação das devidas justificativas e autorização prévia da autoridade competente, assegurados os direitos da Contratada de que tratam os §§ 1º e 2º do art. 58 da mesma Lei.

CLÁUSULA VINTE E TRÊS – DAS DISPOSIÇÕES FINAIS

Além das disposições trazidas no presente contrato, aplicam-se, ainda, o seguinte:

a) a prestação de serviços, objeto do presente contrato, não gera vínculo empregatício entre os empregados da Contratada e a Administração, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta;

b) nada no presente contrato poderá ser interpretado como a criar quaisquer vínculos trabalhistas entre empregados da Contratada e o Contratante. A Contratada assume toda a responsabilidade por todos os

encargos trabalhistas decorrentes da prestação de serviços por seus empregados;

c) a tolerância de uma parte para com a outra quanto ao descumprimento de qualquer uma das obrigações assumidas neste contrato não implicará novação ou renúncia de direito. A parte tolerante poderá exigir da outra o fiel e cabal cumprimento deste contrato a qualquer tempo;

d) as obrigações contidas nas cláusulas sétima e oitava não são de natureza exaustiva, podendo constar no presente termo obrigações referentes as partes ou a cada parte, que não estejam incluídas no rol de obrigações acima citado;

e) os termos e disposições constantes deste contrato prevalecerão sobre quaisquer outros entendimentos ou acordos anteriores entre as partes, expressos ou implícitos referentes às condições nele estabelecidas;

f) é vedado à Contratada caucionar ou utilizar o presente contrato para qualquer operação financeira;

g) a Contratada se compromete a guardar sigilo absoluto sobre as atividades decorrentes da execução dos serviços e sobre as informações a que venha a ter acesso por força da execução dos serviços objeto deste contrato;

h) os casos omissos serão dirimidos pela Administração, que poderá disponibilizar em meio eletrônico informações adicionais e expedir normas complementares, em especial sobre as sistemáticas de fiscalização contratual e repactuação.

CLÁUSULA VINTE E QUATRO – DA PUBLICAÇÃO

O Contratante é responsável pela publicação do extrato do presente contrato no Diário Oficial da União, nos termos e prazos previstos no parágrafo único do art. 61 da Lei nº 8.666/93.

CLÁUSULA E CINCO - DO FORO

Para dirimir quaisquer questões decorrentes do presente Contrato, Fica eleito o Foro da Justiça Federal, Seção Judiciária no Maranhão, nesta cidade de São Luís.

Assim, para firmeza e validade do que foi avençado, foi o presente Contrato lavrado no Tribunal Regional do Trabalho da Décima Sexta Região (art. 60 da Lei Nº 8.666/1993), o qual depois de lido e achado de acordo, vai assinado pelas partes, na presença das testemunhas abaixo.

São Luís, de de 2018.

SOLANGE CRISTINA PASSOS DE CASTRO CORDEIRO
Desembargadora Presidente
TRT 16ª REGIÃO

PATRICIA ANGELINA DA CONCEICAO:34699483801
Assinado de forma digital por PATRICIA ANGELINA DA CONCEICAO:34699483801
Dados: 2018.11.14 16:58:24 -02'00'

PATRÍCIA ANGELINA DA CONCEIÇÃO
NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA

BRUNO CESAR CARVALHO BORGES DA NOBREGA:58424253191
Assinado de forma digital por BRUNO CESAR CARVALHO BORGES DA NOBREGA:58424253191
Dados: 2018.11.14 17:00:22 -02'00'

BRUNO CÉSAR CARVALHO BORGES DA NÓBREGA
NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA

Testemunhas:

1. _____
Identificação nº:

2. _____
Identificação nº: