CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº 089/2023

Pelo presente instrumento particular, o **INSTITUTO NACIONAL DE TECNOLOGIA E SAÚDE – INTS**, Organização Social detentora do Contrato nº 113/2022 firmado com o municipio de Aracaju, inscrita no CNPJ n° 11.344.038/0001-06, com sede na Av. Professor Magalhaes Neto, n.º 1856, sala 806, Edif. TK Tower, Caminho das Árvores, CEP 41.810-012, Salvador/BA, neste ato representada por seu Vice-presidente, Presidente, o **Sr. José Jorge Urpia Lima**, inscrito sob o CPF/MF nº 123.126.815-87 e portador da cédula de identidade RG nº 916317-42, doravante denominada **CONTRATANTE**, e, de outro lado, **TLD TELEDATA COMERCIO E SERVICOS LTDA**, pessoa jurídica de direito privado, inscrita no CNPJ sob nº 33.927.849/0001-64, com sede na Rua Soldado Luiz Gonzaga das Virgens, 111, Caminho das Árvores, Salvador, Bahia, CEP 41820-560, neste ato representada por **Ricardo Luiz de Oliveira**, portador(a) da cédula de identidade RG nº: 7352838-26 SSP/BA, CPF n° 684.548.135-00, daqui por diante denominado simplesmente **CONTRATADA**, no final assinado na presença de 02 (duas) testemunhas, têm justo e contratado nos termos e estipulações das normas jurídicas incidentes neste instrumento, que mutuamente outorgam e aceitam, de acordo com as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA – DO OBJETO

O presente Contrato tem por objeto o fornecimento de Solução de Gerenciamento de Segurança da informação, com Gerência centralizada, englobando o fornecimento de todo software, subscrições, através da locação de Solução de Segurança Cibernética – NGFW, com fornecimento de todo hardware, software, subscrições, instalação, configuração e suporte técnico, a fim de atender as necessidades da Maternidade Municipal Maria de Lourdes Santana Nogueira em Aracaju/SE, nas condições e especificações constantes no contrato e na Proposta apresentada ao **CONTRATANTE**, os quais passarão a ser parte integrante do presente ajuste, independentemente de sua transcrição.

Parágrafo Primeiro – Nenhuma modificação poderá ser introduzida nos detalhes e especificações e preços, sem o consentimento prévio, por escrito, do **CONTRATANTE**.

Parágrafo Segundo – Na necessidade de quaisquer outras disposições complementares, serão devidamente acrescentadas, das quais ambas as partes terão o conhecimento integral e a devida aceitação por meio de Termo Aditivo.

CLÁUSULA SEGUNDA – DOS SERVIÇOS E EQUIPAMENTOS

Os serviços e equipamentos solicitados deverão ser executados na Maternidade Municipal Marial de Lourdes Santana Nogueira, situada na Avenida São João Batista Costa, s/n, bairro 17 de março, Aracaju/SE, com acesso principal pela Rua Procurador José Costa Cavalcante (antigo acesso 09) no mínimo, de acordo com as disposições constantes nesse contrato, podendo as especificações ser alteradas de acordo com a demanda da maternidade ou conforme a solicitação do INTS.

Parágrafo Primeiro – O serviço compreenderá no fornecimento de todo o equipamento para uso, bem como a configuração, manutenção, treinamento e suporte técnico, nos padrões determinados pela **CONTRATANTE** e especificações necessárias as atividades desta.

Parágrafo segundo – Os equipamentos solicitados, devem seguir as características estipuladas no Termo de Referência e executados de acordo com a listagem de serviços descritas abaixo:

- **Solução de Firewall - funcionalidades básicas:**
    a) Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux;
    b) A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que, todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração;
    c) Deverá possuir minimamente as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, Otimização WAN, DLP – Data Leak Prevention, Controladora Wireless, Virtualização e Retenção de Log em Cloud;
    d) Firewall com capacidade mínima de processamento de 6 (seis) Gbps;

e) IPS com capacidade mínima de processamento de 1 (um) Gbps;
f) Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 800 (oitocentos) Mbps;
g) Inspeção SSL Throughput com capacidade mínima de processamento de 700 (setecentos) Mbps;
h) VPN com capacidade de, pelo menos, 6 (seis) Gbps de tráfego IPSec;
i) VPN SSL com capacidade de, pelo menos, 850 (oitocentos e cinquenta) Mbps de tráfego;
j) Deverá suportar 1.400.000 (um milhão e quatrocentos mil) conexões simultâneas;
k) Deverão ser licenciados para suportar, pelo menos, 200 (duzentos) usuários de VPN SSL;
l) Deverá suportar, pelo menos, 40.000 (quarenta mil) novas conexões por segundo;
m) Deverá suportar, pelo menos, 150 (cento e cinquenta) túneis de VPN Site-Site;
n) Deverá suportar, pelo menos, 2.000 (dois mil) túneis de VPN Client-Site;
o) Deverá possuir, pelo menos, 2 (duas) interfaces SFP 1GE.
p) Deverá possuir, pelo menos, 6 (seis) interfaces RJ 45;
q) Deverá suportar operação em modo de alta disponibilidade (cluster) e estar licenciados para operar desta forma, em modo ativo-ativo;
r) Deverá possuir licença para número ilimitado de usuários e endereços IP;
s) Deverá possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de UTP durante a vigência contratual;
t) Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 40 (quarenta) Pontos de Acesso sem fio;
u) Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 15(quinze) equipamentos;
v) Deverá ser realizado a instalação inicial do equipamento que está restrito a entrega do equipamento, conferência de itens e teste inicial de funcionamento;

w) Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários;
x) Deverá incluir licença para a funcionalidade de VPN SSL;
y) Deverá incluir licença para atualização de vacina de antivírus/antispyware;
z) Deverá incluir licença de atualização para filtro de conteúdo Web;
aa) Deverá incluir licença de atualização do IPS e da lista de aplicações detectadas;
bb) Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

- **Funcionalidades de Firewall:**

a) Deverá possuir controle de acesso à internet por endereço IP de origem e destino;
b) Deverá possuir controle de acesso à internet por sub-rede;
c) Deverá suportar tags de VLAN (802.1q);
d) Deverá possuir ferramenta de diagnóstico do tipo tcpdump;
e) Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;
f) Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
g) Deverá suportar single-sign-on para Active Directory, Novell eDirectory, Citrix e RADIUS;
h) Deverá possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);
i) Deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;
j) Deverá permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
k) Deverá permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;

l) Deverá possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

m) Deverá suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

n) Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;

o) Deverá suportar aplicações multimídia, como: H.323 e SIP;

p) Deverá possuir tecnologia de firewall do tipo Statefull;

q) Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

r) Deverá permitir o funcionamento em modo transparente tipo "bridge" sem alterar o endereço MAC do tráfego;

s) Deverá suportar PBR – Policy Based Routing;

t) Deverá permitir a criação de VLANS no padrão IEEE 802.1q;

u) Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

v) Deverá permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;

w) Deverá permitir forwarding de camada 2 para protocolos não IP;

x) Deverá suportar forwarding multicast;

y) Deverá suportar roteamento multicast PIM Sparse Mode e Dense Mode;

z) Deverá permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;

aa) Deverá permitir o agrupamento de serviços

bb) Deverá permitir o filtro de pacotes sem a utilização de NAT;

cc) Deverá permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

dd) Deverá possuir mecanismo de anti-spoofing;

ee) Deverá permitir criação de regras definidas pelo usuário;

ff) Deverá permitir o serviço de autenticação para tráfego HTTP e FTP;

gg) Deverá permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

hh) Deverá possuir a funcionalidade de balanceamento e contingência de links;

ii) Deverá suportar sFlow;

jj) O dispositivo deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando, ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY;

kk) Deverá ter a capacidade de permitir a criação de regras de firewall específicas para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows;

ll) Deverá ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;

mm) Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

nn) Deverá permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;

oo) Deverá suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;

pp) Deverá permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;

qq) Deverá possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I,

H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;

rr) Deverá suportar SIP, H.323 e SCCP NAT Traversal;

ss) Deverá permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;

tt) Deverá possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

- **Funcionalidade de Traffic Shaping e priorização de tráfego:**

a) Deverá permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

b) Deverá permitir modificação de valores DSCP para o DiffServ;

c) Deverá permitir priorização de tráfego e suportar ToS;

d) Deverá limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;

e) Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

f) Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

g) Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

h) Deverá permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;

i) Deverá controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;

j) Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

k) Deverá ter a capacidade de permitir a criação de perfis de controle de banda específicos para tipos de dispositivos identificados automaticamente (funcionalidade essa conhecida como BYOD – Bring

Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

- **Funcionalidade de Anti-Spam de Gateway:**
    a) Deverá permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;
    b) Deverá possuir filtragem de e-mail por palavras chaves;
    c) Deverá permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;
    d) Deverá possuir, para a funcionalidade de anti-spam, o recurso de RBL;
    e) Deverá permitir a checagem de reputação da URL no corpo da mensagem de correio eletrônico;
    f) Deverá ter a capacidade de permitir a criação de perfis de AntiSpam específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

- **Funcionalidade de Anti-Spam de Gateway:**
    a) Deverá possuir solução de filtro de conteúdo Web integrado à solução de segurança;
    b) Deverá possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;
    c) Deverá possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;
    d) Deverá possuir a funcionalidade de cota de tempo de utilização por categoria;
    e) Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:
        a. Proxy anônimo;
        b. Webmail;
        c. Instituições de saúde;
        d. Notícias;
        e. Phishing;
        f. Hackers;

g. Pornografia;

h. Racismo;

i. Websites pessoais;

j. Compras.

f) Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

g) Deverá permitir a criação de, pelo menos, 05 (cinco) categorias personalizadas;

h) Deverá permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;

i) Deverá prover Termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado;

j) Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

k) Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

l) Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

m) Deverá exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

n) Deverá permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;

o) Deverá permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

p) Deverá permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

q) Deverá permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;

r) Deverá filtrar o conteúdo baseado em categorias em tempo real;

s) Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;
t) Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
u) Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
v) Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem;
w) Deverá ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;
x) Deverá permitir o bloqueio de redirecionamento HTTP;
y) Deverá permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;
z) Deverá possuir Proxy Explícito e Transparente;
aa) Deverá implementar roteamento WCCP e ICAP;
bb) Deverá ter a capacidade de permitir a criação de perfis de filtragem Web específicos para tipos de dispositivos identificados automaticamente (funcionalidade essa conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

- **Funcionalidade de detecção de intrusão**

a) Deverá permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;
b) Deverá possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;
c) Deverá estar orientado à proteção de redes;
d) Deverá permitir funcionar em modo transparente, sniffer e router;
e) Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
f) Deverá permitir a criação de padrões de ataque manualmente

g) Deverá possuir integração à plataforma de segurança;
h) Deverá possuir capacidade de remontagem de pacotes para identificação de ataques;
i) Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a webserver, para que seja usado para proteção específica de Servidores Web;
j) Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
k) Deverá ter a capacidade de permitir a criação de perfis de inspeção específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows;
l) Deverá possuir mecanismos de detecção/proteção de ataques;
m) Deverá possuir reconhecimento de padrões;
n) Deverá possuir análise de protocolos;
o) Deverá possuir detecção de anomalias;
p) Deverá possuir detecção de ataques de RPC (Remote Procedure Call);
q) Deverá possuir proteção contra-ataques de Windows ou NetBios;
r) Deverá possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);
s) Deverá possuir proteção contra-ataques DNS (Domain Name System);
t) Deverá possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;
u) Deverá possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);
v) Deverá possuir métodos de notificação de detecção de ataques
w) Deverá possuir alarmes na console de administração;
x) Deverá possuir alertas via correio eletrônico;
y) Deverá possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

z) Deverá ter a capacidade de resposta/logs ativa a ataques;
aa) Deverá prover a terminação de sessões via TCP resets;
bb) Deverá armazenar os logs de sessões;
cc) Deverá atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
dd) Deverá mitigar os efeitos dos ataques de negação de serviços;
ee) Deverá permitir a criação de assinaturas personalizadas;
ff) Deverá possuir filtros de ataques por anomalias;
gg) Deverá permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
hh) Deverá permitir filtros de anomalias de protocolos;
ii) Deverá suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
jj) Deverá suportar verificação de ataque na camada de aplicação;
kk) Deverá suportar verificação de tráfego em tempo real, via aceleração de hardware;
ll) Deverá possuir as seguintes estratégias de bloqueio: pass, drop e reset

- **Funcionalidade de VPN**

a) Deverá possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
b) Deverá possuir suporte a certificados PKI X.509 para construção de VPNs;
c) Deverá possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Clientto-Site;
d) Deverá possuir suporte a VPN SSL;
e) Deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
f) A VPN SSL deverá possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
g) Deverá possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;
h) A VPN SSL deverá suportar cliente para plataforma Windows, Linux e Mac OS;

i) Deverá permitir a arquitetura de VPN hub and spoke;

j) Deverá possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

- **Funcionalidade de controle de aplicações:**

a) Deverá possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;

b) Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:

a. P2P;

b. Instant Messaging;

c. Web;

d. Transferência de arquivos;

e. VoIP.

c) Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

d) Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;

e) Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

f) Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

g) Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

h) Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

i) Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

j) Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

k) Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

l) Deverá permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos

m) Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

n) Deverá permitir criação de padrões de aplicação manualmente; Deverá ter a capacidade de permitir a criação de perfis de controle de aplicações específicos para tipos de dispositivos identificados automaticamente (funcionalidade essa conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

- **Funcionalidade de cache e otimização de Wan**

a) Deverá implementar otimização do tráfego entre dois equipamentos;

b) Deverá possuir capacidade de armazenamento local;

c) Deverá implementar, no mínimo, as seguintes técnicas de otimização:

a. Otimização de protocolos;

b. Byte caching;

c. Web caching;

d) Deverá otimizar, no mínimo, os seguintes protocolos: CIFS, FTP, HTTP, MAPI e TCP;

e) Deverá permitir criptografar a comunicação entre os appliances envolvidos na otimização do tráfego através de protocolos IPSEC ou SSH;

f) Deverá implementar alta disponibilidade, no mínimo, ativo-passivo;

g) Deverá possuir cache de páginas Web (HTTP);

h) Deverá apresentar gráfico ou relatório que indique a quantidade de tráfego que está sendo otimizada, em porcentagem ou bytes;

- **Funcionalidade de DLP (Data Leak Prevention)**

a) O sistema de DLP (Data Leak Prevention – Proteção contra Vazamento de Informações) de gateway deverá funcionar de maneira que se consiga que os dados sensíveis não saiam da rede e também deverá funcionar de modo que se previna que dados não requisitados entrem na sua rede;
b) Deverá inspecionar, no mínimo, os tráfegos de e-mail, HTTP, NNTP e de mensageiros instantâneos;
c) Sobre o tráfego de e-mail, deverá inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;
d) Sobre o tráfego de mensageiros instantâneos, deverá inspecionar, no mínimo, os protocolos AIM, ICQ, MSN e Yahoo!;
e) Deverá realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS-Word; 4.10.6 Deverá fazer a varredura no conteúdo de um cookie HTTP buscando por determinado texto;
f) Deverá aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;
g) Deverá verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio entrantes/saintes possui um tamanho máximo especificado pelo administrador;
h) Deverá utilizar expressões regulares para composição das regras de verificação dos tráfegos;
i) Deverá tomar minimamente as ações de bloquear, banir usuário e colocar em quarentena a interface sobre as regras que coincidirem com o tráfego esperado pela regra;
j) Deverá permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de e-mail, HTTP e mensageiros instantâneos;
k) Deverá permitir a composição de múltiplas regras de DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o sistema.

- **Funcionalidade de balanceamento de carga**

a) Deverá permitir a criação de endereços IPs virtuais;

b) Deverá permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;
c) Deverá suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;
d) Deverá permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Round Robin, Weighted, First Alive e HTTP host;
e) Deverá permitir persistência de sessão por cookie HTTP ou SSL session ID;
f) Deverá permitir que seja mantido o IP de origem;
g) Deverá suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;
h) Deverá ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;
i) Deverá permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

- **Funcionalidade de virtualização**

a) Deverá suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;
b) Deverá permitir a criação de administradores independentes para cada uma das instâncias virtuais;
c) Deverá permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas;
d) Deverá possuir as seguintes certificações:
   a. Certificação Wi-Fi Alliance;
   b. Certificação ICSA para Firewall; Certificação ICSA para VPN SSL;
   c. Certificação ICSA para VPN IPSec;
   d. Certificação ICSA para IPS;
e) O equipamento de firewall e/ou IPS deverá ter sido aprovado nos testes da NSS Labs e deverá estar na lista de recomendados.

- **Funcionalidade de SD-WAN**

a) solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web;

b) A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;

c) A solução SD-WAN deve suportar micro-segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN;

d) A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;

e) Solução deve ser capaz de prover Zero Touch provisioning;

f) A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;

g) Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz;

h) A solução deve ser capaz de criar VPN "Full-Mesh" em interface Gráfica, de forma automática, e sem que o administrador precise configurar site por site;

i) A configuração VPN IPSEC deverá oferecer suporte para DH Group: 14 e 15;

j) Reconhecimento em camada 7 totalmente segregado da camada 4;

k) Deve, de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino;

l) O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

m) A solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em

contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc);

n) A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6;

o) A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;

p) A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, no qual seja possível configurar um valor de Theshold para cada um destes itens, será utilizado como fator de decisão nas regras de SD-WAN;

q) A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu Valor de Saúde melhor que o link atual;

r) A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema;

s) A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN

CLAUSULA TERCEIRA - SERVIÇO DE SUPORTE TÉCNICO DAS LICENÇAS DE SOFTWARE ADQUIRIDAS

Durante a vigência do Contrato e da garantia, deverá ser fornecido suporte técnico pela **CONTRATADA** nos termos a seguir descritos:

a) A **CONTRATADA** deverá fornecer serviços de suporte técnico em horário comercial para correção de erros da solução, resolução de dúvidas técnicas pelo telefone;

b) O horário comercial compreende o horário das 08h00min às 18h00min, de 2ª a 6ª feira, em dias úteis;

c) Os pedidos poderão ser registrados através de linha telefônica, correio eletrônico ou serviço equivalente via internet, desde que seja formalizado número de protocolo ou registro de abertura de chamado;

d) O fabricante deverá possuir Centro de Suporte Técnico de 1º nível com atendentes que falem português;

e) A **CONTRATADA** deve fornecer correção de qualquer defeito ou falha que ocorra nos programas que impeçam o seu perfeito funcionamento de acordo com suas características e desempenho especificados em documentação técnica que acompanha cada software;

f) A **CONTRATADA** deve revisar Manuais Técnicos e Guias do Usuário, inclusive documentação, a qualquer tempo, e desde que acompanhada da respectiva atualização/revisão dos softwares;

g) A **CONTRATADA**, após a assinatura do contrato, deve disponibilizar material ou meio de consulta para o **CONTRATANTE** sobre como instalar, configurar e utilizar o objeto adquirido, capacitando o(s) administrador(es) e operador(es) a executar essas atividades com o console central de gerenciamento da solução adquirida;

h) Quaisquer dúvidas técnicas na execução dessas atividades, bem como na instalação, configuração e utilização do Console de Gerenciamento Central deverão ser sanadas por meio do suporte técnico acima descrito;

i) Os serviços de manutenção de software deverão prover suporte aos componentes (licenças de uso); orientações sobre uso, configuração e instalação; orientações para identificação de causas de falhas de software; fornecimento de informações conhecidas sobre defeitos conhecidos e envio de informações sobre falhas não conhecidas para tratamento do fabricante do produto;

j) A **CONTRATADA** deverá prestar suporte técnico às licenças adquiridas durante todo o período de vigência contratual.

CLAUSULA QUARTA - ATUALIZAÇÃO DAS LICENÇAS

a) A **CONTRATADA** deverá prover toda e qualquer atualização ao produto durante a vigência do contrato;

b) Entende-se como atualização o fornecimento de qualquer evolução do produto, incluindo patchs, fixes, correções, updates, service packs e novas versões lançadas;

c) O fornecimento de novas versões e releases não acarretará quaisquer ônus adicionais ao **CONTRATANTE** durante a vigência do contrato;

d) A **CONTRATADA** deverá informar ao **CONTRATANTE** toda e qualquer atualização lançada pelo Fabricante, com detalhamento técnico.

CLÁUSULA QUINTA – DOS PRAZOS

O presente instrumento vigerá pelo prazo de 24 (vinte e quatro) meses, iniciando em 20 de março de 2023, podendo ser prorrogado por conveniência das partes através de Termo Aditivo.

Parágrafo Único – Este Contrato estará integralmente condicionado à vigência do Contrato de Gestão nº 113/2022 celebrado com o Município de Aracaju/SE, devendo durar somente enquanto este último viger.

CLÁUSULA SEXTA – DO VALOR E DAS CONDIÇÕES DE PAGAMENTO

Pela prestação dos serviços objeto deste contrato será pago o valor de R$ 1.784,88 (Hum mil setecentos e oitenta e quatro reais e oitenta e oito centavos) mediante emissão do relatório de evidências e apresentação do boletim de medição e da Nota Fiscal/Fatura mensal, conforme valores extraídos da proposta da **CONTRATADA** anexa, que faz parte deste instrumento independentemente de sua transcrição, referente ao valor mensal da prestação e dos itens locados, descritos de forma unitária na tabela abaixo:

Descrição	Marca/ Modelo	SKU	Qtde	Valor Unitário	Valor Total Mensal
Fornecimento de solução de Gerenciamento de Segurança de Endpoint com Gerência Centralizada, englobando o fornecimento de todo software, subscrições, instalação, configuração e suporte técnico	Fortinet/ Fortigate 80F	FG-80F/ FC-10-0080F-879-02-12	02	R$ 892,44	R$ 1.784,88

Parágrafo Primeiro – Estão inclusos no preço acima, todos os tributos, inclusive ICMxS, ISS e Imposto de Renda, e outros encargos e obrigações trabalhistas e previdenciárias, lucros, fretes e demais despesas incidentes, tais como taxa de administração, suprimentos, enfim, todos os custos necessários para a perfeita execução, assim que nada mais poderá ser cobrado da **CONTRATANTE**.

Parágrafo Segundo – O pagamento dar-se-á em até 30 (trinta) dias após a entrega da Nota Fiscal/Fatura, através de transferência em conta fornecida pela **CONTRATADA** na Nota Fiscal/Fatura.

Parágrafo Terceiro – As Notas Fiscais deverão ser emitidas em favor do CNPJ informado no preâmbulo entre o dia 1º ao dia 20 do mês seguinte à prestação dos serviços, contendo o número do contrato de prestação de serviços e os dados bancários para depósito, devendo a conta estar vinculada ao CNPJ de titularidade da **CONTRATADA.**

Parágrafo Quarto – Os pagamentos descritos acima estarão condicionados ao recebimento, por parte do **CONTRATANTE**, dos recursos previstos no Contrato de Gestão nº 113/2022 celebrado com o Município de Aracaju/SE.

Parágrafo Quinto – Na hipótese de atraso no repasse dos valores do Contrato de Gestão nº 113/2022 celebrado com o Município de Aracaju/SE, a **CONTRATADA** declara, desde este momento, que não terá direito a qualquer remuneração compensatória, a qualquer título, isentando o **CONTRATANTE** de qualquer ônus sobre as parcelas atrasadas.

Parágrafo Sexto – A superveniência na majoração de alíquotas ou a criação de novos Tributos, Contribuições Sociais instituídos com vinculação a existência de contrato de trabalho dos empregados inerentes a este contrato, ocorridos na vigência deste, constituirão custos para a **CONTRATADA**.

Parágrafo Sétimo – O valor relativo a eventuais serviços extras não previstos neste Contrato, quando solicitados e/ou autorizados expressamente pelo **CONTRATANTE**, será previamente ajustado por escrito mediante Termo Aditivo.

Parágrafo Oitavo - As isenções específicas deverão ser comprovadamente apresentadas ao **CONTRATANTE**, bem como declaração firmada pela **CONTRATADA** justificando a sua isenção.

Parágrafo Nono - Ocorrendo atraso na apresentação da Nota Fiscal/Fatura, o vencimento ficará automaticamente prorrogado por período equivalente, sem ônus ao **CONTRATANTE.**

Parágrafo Décimo - Caso seja constatado algum erro na Nota Fiscal/Fatura, será a mesma devolvida e o respectivo pagamento suspenso até a sua efetiva correção, sem que isso implique na paralisação dos serviços, bem assim a incidência de juros, reajuste ou multa.

Parágrafo Décimo Primeiro - Os pagamentos referentes ao presente contrato estão condicionados à apresentação da Nota Fiscal/Fatura de serviços que deverão ser apresentadas junto com as seguintes certidões negativas de débitos ou positivas com efeito negativa, abrangendo a data de pagamento da Nota Fiscal/Fatura:

a) Certidão Negativa de Débitos relativos aos Tributos Federais e à Dívida Ativa da União -Federal e INSS;

b) Certidão Negativa de Débitos Tributários - Estadual;

c) Certidão Negativa de Débitos Mobiliários – Municipal;

d) Fundo de Garantia por Tempo de Serviço – FGTS, mediante apresentação de Certificado de Regularidade de Situação – CRF;

e) Certidão Negativa de Débitos Trabalhistas – CNDT.

CLÁUSULA SÉTIMA – OBRIGAÇÕES DA CONTRATADA

Caberá a **CONTRATADA**, dentre outras obrigações legais e constantes do presente contrato:

a) Executar os serviços contratados através da fixação de parâmetros técnicos e a tempo certo, obedecendo as condições e prazos estipulados entre as partes;
b) Submeter ao **CONTRATANTE**, para prévia aprovação escrita, todo serviço que se fizer necessário à sua participação;
c) Respeitar e fazer com que sejam respeitadas as normas atinentes ao bom funcionamento dos serviços prestados pelo **CONTRATANTE** e aquelas relativas ao objeto do Contrato;
d) Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, o objeto do presente Termo, nem subcontratar quaisquer das prestações a que está obrigada sem prévio consentimento, por escrito, do **CONTRATANTE**;
e) Manter, durante todo o período de vigência do Contrato, todas as condições que ensejaram a contratação, particularmente no que tange à regularidade fiscal, qualificação técnica e cumprimento do Processo Seletivo;
f) Cuidar da regularidade obrigacional derivada do vínculo e subordinação com o pessoal envolvido direta ou indiretamente na execução do Contrato, adimplindo com toda e qualquer obrigação fiscal e trabalhista decorrente da prestação de serviços dos seus cooperados/funcionários;

g) Atuar conforme as normas estabelecidas pelos Órgãos de fiscalização profissional de sua especialidade e obedecer às normas legais vigentes na ANVISA e Ministério da Saúde, bem como atender todas as resoluções normativas pertinentes ao objeto do Contrato;

h) Dar esclarecimentos sobre qualquer procedimento, o mais breve possível, a contar do recebimento de notificação para tal mister;

i) Submeter-se à fiscalização a ser realizada pelo **CONTRATANTE**, ou qualquer Órgão fiscalizador, relativa à prestação dos serviços pactuados, conforme regras estabelecidas nos protocolos internos e padronização do **CONTRATANTE** e do nosocômio onde será prestado os serviços;

j) Comunicar, por escrito, imediatamente, a impossibilidade de execução de qualquer obrigação contratual, para adoção das providências cabíveis;

k) Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em decorrência da espécie, forem vítimas os seus empregados quando da prestação dos serviços, sendo defeso invocar o Contrato para eximir-se de qualquer responsabilidade ou obrigação, bem como transferir o ônus financeiro decorrente dessas obrigações ao **CONTRATANTE**;

l) Executar os serviços com o máximo de zelo, bem como seguir rigorosamente as especificações e normas pertinentes em vigência;

m) Responder, integralmente, por perdas e danos que vier a causar ao **CONTRATANTE** ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus funcionários, independentemente de outras cominações contratuais ou legais a que estiver sujeita, sendo defeso invocar o Contrato para eximir-se de qualquer responsabilidade ou obrigação, bem como transferir o ônus financeiro decorrente dessas obrigações ao **CONTRATANTE**;

n) Dar ciência ao **CONTRATANTE**, imediatamente e por escrito, de qualquer anormalidade que verificar durante a execução dos serviços;

o) Atender a qualquer convocação do **CONTRATANTE** para esclarecimentos a respeito dos serviços prestados.

CLAUSULA OITAVA - DAS OBRIGAÇÕES DA CONTRATANTE

Caberá ao **CONTRATANTE**, as suas expensas, dentre outras obrigações legais e ou constantes do presente contrato:

a) Exercer o acompanhamento e a fiscalização dos serviços quanto as quantidades, prazos e especificações, notificando a **CONTRATADA** por escrito para que tome as providências necessárias caso observado não conformidade para o efetivo cumprimento do Contrato, bem como rejeitar todo e qualquer material que não atendam as especificações contidas no presente contrato. Caso não sejam corrigidas as não conformidades em tempo hábil, cabe ao **CONTRATANTE** aplicar as devidas sanções;

b) Prestar as informações e os esclarecimentos em tempo hábil, que venham a ser solicitados pela **CONTRATADA** para o melhor cumprimento do Contrato;

c) Editar normas complementares para o gerenciamento da execução do Contrato em razão de exigência dos órgãos de controle e fiscalização aos quais o Contrato de Gestão que a Unidade esteja vinculada ou subordinada;

d) Glosar do valor do Contrato eventuais prejuízos causados pela **CONTRATADA**, de qualquer natureza, bem como valores decorrentes de passivos trabalhistas e fiscais, gerada e não adimplidos pela **CONTRATADA**.

Parágrafo Único – O presente contrato não implica em qualquer vínculo de solidariedade entre os contratantes, ficando cada qual responsável pelas obrigações derivadas de suas respectivas atividades, sejam elas de caráter fiscal, trabalhista, previdenciário, sem exclusão de qualquer outra.

CLÁUSULA NONA – RESPONSABILIDADE TRABALHISTA

A prestação de serviços ora contratada não enseja qualquer tipo de vínculo, inclusive trabalhista, entre a **CONTRATADA**, seus propostos, prestadores de serviço e empregados, com o **CONTRATANTE**; respondendo aquele por todas as obrigações decorrentes de sua posição de empregador e contratante dos profissionais porventura contratados para lhe auxiliar na execução deste pacto - não se estabelecendo entre estes e o **CONTRATANTE** ou entre esta e o **CONTRATADO**, qualquer tipo de solidariedade em relação aos mesmos.

CLÁUSULA DÉCIMA – RESCISÃO

O presente Contrato poderá ser rescindido de pleno direito, em caso de rescisão do no Contrato de Gestão nº 113/2022 celebrado com o Município de Aracaju/SE, apenas para formalização, sem qualquer indenização cabível, como também poderá ser rescindido, por quaisquer das partes, a qualquer tempo, mediante envio de notificação com antecedência

mínima de 30 (trinta) dias, sem que lhe caiba qualquer indenização, porém sem prejuízo do pagamento proporcional dos serviços já realizados.

Parágrafo Primeiro – O presente contrato será considerado rescindido por justa causa, além dos previstos em lei, independente de aviso, notificação ou interpelação judicial:

a) Falência, recuperação judicial ou extrajudicial, dissolução ou liquidação de qualquer das partes;

b) Inadimplência, por uma das partes, de quaisquer obrigações previstas no contrato, salvo em decorrência de caso fortuito ou força maior;

c) Subcontratação ou cessão parcial ou total deste contrato a terceiros, sem autorização expressa da outra parte;

d) Descumprimento de qualquer das cláusulas e condições estabelecidas neste instrumento.

Parágrafo Segundo – Na ocorrência de sucessão da **CONTRATADA**, o presente Contrato poderá prosseguir ou ser rescindido, a critério exclusivo da **CONTRATADA**.

Parágrafo Terceiro – Rescindido o presente contrato por quaisquer motivos previstos nesta cláusula, a **CONTRATANTE** entregará a execução dos serviços a quem julgar conveniente, respondendo a **CONTRATADA**, na forma legal e contratual, pela infração ou execução inadequada que der causa à rescisão.

CLÁUSULA DECIMA PRIMEIRA - GLOSAS

O **CONTRATANTE** poderá efetuar a retenção ou glosa do pagamento de qualquer documento de cobrança, no todo ou em parte, nos seguintes casos:

a) Inexecução total ou execução defeituosa ou insatisfatória dos serviços que resulte na perda total do trabalho;
b) Não utilização de materiais e recursos humanos exigidos para execução dos serviços, ou utilização ou em qualidade ou em quantidade inferior a demanda;
c) Descumprimento de obrigação relacionada ao objeto do ajuste que possa ensejar a responsabilização solidária ou subsidiária da **CONTRATANTE**, independente da sua natureza.

CLÁUSULA DECIMA SEGUNDA – RESPONSABILIDADES FISCAIS

A **CONTRATANTE** se responsabiliza pela retenção que lhe impuser a legislação vigente, das taxas e impostos incidentes sobre as faturas mensais da prestação de serviços ora locados, bem como pelo recolhimento das mesmas aos respectivos órgãos credores.

CLÁUSULA DÉCIMA TERCEIRA – RESPONSABILIDADE CIVIL

A **CONTRATADA** responderá por todos os danos causados à **CONTRATANTE**, aos empregados, prestadores de serviços, prepostos, representantes ou terceiros, a que venha a dar causa, por ação ou omissão, em razão da execução do objeto deste contrato.

CLÁUSULA DÉCIMA QUARTA – DA TOLERÂNCIA

Todas as obrigações decorrentes deste instrumento, se vencerão independentemente de qualquer notificação, interpelação ou aviso judicial ou extrajudicial. Qualquer tolerância no recebimento dos encargos em atraso, por qualquer das partes, não implicará em novação, permanecendo exigíveis as sanções contratuais independentemente de reforço.

CLÁUSULA DÉCIMA QUINTA – COMPROMISSO DA CONTRATADA

A CONTRATADA, neste ato, compromete-se a:

a) Não utilizar mão de obra infantil, ressalvado o menor aprendiz nos termos lei;

b) Não utilizar trabalho forçado ou equivalente;

c) Respeitar a legislação ambiental.

CLÁUSULA DÉCIMA SEXTA – DOS CASOS OMISSOS

Fica estabelecido que, caso venha a ocorrer algum fato não previsto no instrumento, os chamados casos omissos, estes deverão ser resolvidos entre as partes, respeitados o objeto deste Contrato o código civil vigente, supletivamente, os princípios da teoria geral dos contratos e as disposições de direito privado, não se constituindo em novação ou renúncia ao direito de aplicar as sanções previstas neste contrato ou decorrentes de lei.

CLÁUSULA DÉCIMA SÉTIMA – DA CONFIDENCIALIDADE

As partes reconhecem que todas as informações confidenciais são essenciais para seus sucessos e negócios, e por isso se obrigam entre si, por seus empregados e prepostos, a manter sigilo sobre os dados, fotos, documentos, especificações técnicas ou comerciais e demais informações de caráter confidencial, de que venham a ter conhecimento em virtude deste Contrato, mesmo após a sua vigência, não podendo divulgá-las de forma alguma, salvo autorização prévia por escrito do **CONTRATANTE**.

CLÁUSULA DÉCIMA OITAVA – DAS DECLARAÇÕES E GARANTIAS ANTICORRUPÇÃO

As partes declaram, neste ato, que estão cientes, conhecem e entendem os termos das leis anticorrupção brasileira e de quaisquer outras leis antissuborno ou anticorrupção aplicáveis ao presente contrato; assim como das demais leis aplicáveis sobre o objeto do presente contrato. Em especial a Lei nº 12.846/13, suas alterações e regulamentações, que dispõe sobre a responsabilização objetiva administrativa e civil de pessoas jurídicas, pela prática de ato contra a administração pública nacional ou estrangeira, também chamada de Lei Anticorrupção, comprometendo-se a abster-se de qualquer atividade que constitua uma violação das disposições destas Regras Anticorrupção.

Parágrafo Primeiro – As partes, por si e por seus administradores, sócios, diretores, funcionários e agentes ou outra pessoa ou entidade que atue, por qualquer tempo, em seu nome ou de qualquer outrem, se obrigam, no curso de suas ações ou em nome do seu respectivo representante legal, durante a consecução do presente Contrato, agir de forma ética e em conformidade com os preceitos legais aplicáveis.

Parágrafo Segundo – Na execução deste Contrato, nenhuma das partes, por si e por seus administradores, sócios, diretores, funcionários e agentes ou outra pessoa ou entidade que atue, por qualquer tempo, em seu nome ou de qualquer de suas afiliadas, tomando ou prestando serviços uma a outra, devem dar, prometer dar, oferecer, pagar, prometer pagar, transferir ou autorizar o pagamento de, direta ou indiretamente, qualquer dinheiro ou qualquer coisa de valor a qualquer funcionário ou empregado ou a qualquer autoridade governamental, concursados ou eleitos, em exercício atual de sua função ou a favor de sua nomeação, seus subcontratados, seus familiares ou empresas de sua propriedade ou indicadas, consultores, representantes, parceiros, ou quaisquer terceiros, com finalidade de: influenciar qualquer ato ou decisão de tal Agente Público em seu dever de ofício; induzir tal Agente Público a fazer ou deixar de fazer algo em relação ao seu dever legal; assegurar qualquer vantagem indevida;

ou induzir tal Agente Público a influenciar ou afetar qualquer ato ou decisão de qualquer Órgão Governamental.

Parágrafo Terceiro – Para os fins da presente Cláusula, as partes declaram neste ato que:

a) Não violaram, violam ou violarão as Regras Anticorrupção estabelecidas em lei;

b) Têm ciência de que qualquer atividade que viole as Regras Anticorrupção é proibida e que conhece as consequências possíveis de tal violação.

Parágrafo Quarto – Qualquer descumprimento das regras Anticorrupção pelas partes, em qualquer um dos seus aspectos, ensejará a rescisão motivada imediata do presente instrumento, independentemente de qualquer notificação.

Parágrafo Quinto – "Órgão Governamental", tal como empregado na presente disposição, denota qualquer governo, entidade, repartição, departamento ou agência mediadora desta, incluindo qualquer entidade ou empresa de propriedade ou controlada por um governo ou por uma organização internacional pública.

CLÁUSULA DÉCIMA NONA – DAS NORMAS DE CONDUTA

A parte **CONTRATADA** declara, neste ato, que está ciente, conhece e entende os termos do Código de Conduta de Terceiros da **CONTRATANTE**, obrigando-se por si e por seus administradores, sócios, diretores, funcionários e agentes ou outra pessoa ou entidade que atue, por qualquer tempo, em seu nome, a cumprir os seus termos, sob pena da aplicação das sanções contratuais previstas.

Parágrafo Primeiro – No exercício da sua atividade, a parte **CONTRATADA** obriga-se a cumprir com as leis de privacidade e proteção dos dados relacionados ao processo de coleta, uso, processamento e divulgação dessas informações pessoais.

Parágrafo Segundo – A parte **CONTRATADA** obriga-se a manter sigilo de todas e quaisquer informações da **CONTRATANTE** que venham a ter acesso, como documentos, projetos e quaisquer materiais arquivados e registrados de qualquer forma, sejam originais ou copias, de quaisquer formas (gráficas, eletrônica ou qualquer outro modo), protegendo-as e não divulgando para terceiros.

Parágrafo Terceiro – A parte **CONTRATADA** declara, neste ato, que está ciente, conhece e irá cumprir a Política Antissuborno e a Política de Brindes, Presentes e Hospitalidades da **CONTRATANTE,** que podem ser acessadas através do site: http://ints.org.br/.

CLÁUSULA VIGÉSIMA – DA LEI GERAL DE PROTEÇÃO DE DADOS

O presente contrato será regido e interpretado em relação as leis de proteção de dados conforme a Legislação vigente de Proteção de Dados (LGPD - Lei Geral de Proteção de Dados) de acordo com as leis da República Federativa do Brasil (13.709/2018 e suas atualizações), além das demais normas e políticas de proteção de dados de cada país onde houver qualquer tipo de tratamento dos dados dos clientes, valendo-se para este contrato e incluindo também dados anteriores que possam já existir em nossa base de informações para proteção.

Parágrafo Primeiro – A **CONTRATADA**, por si e por seus colaboradores, obriga-se a atuar no presente Contrato em conformidade com a Legislação vigente sobre Proteção de Dados Pessoais e as determinações de órgãos reguladores/fiscalizadores sobre a matéria, em especial a Lei 13.709/2018, tratando os dados pessoais a que tiver acesso apenas de acordo com as instruções da **CONTRATANTE**.

Parágrafo Segundo – A **CONTRATADA** se compromete a acessar os dados dentro de seu escopo e na medida abrangida por sua permissão de acesso (autorização) e que os dados pessoais não podem ser lidos, copiados, modificados ou removidos sem autorização expressa e por escrito da **CONTRATANTE.**

Parágrafo Terceiro – Na assinatura desse contrato, a **CONTRATADA** autoriza e consente o tratamento de seus dados pessoais de acordo com a LGPD e da Política de Proteção de Dados da **CONTRATANTE**.

Parágrafo Quarto – A **CONTRATANTE** poderá tratar os dados da **CONTRATADA** de acordo com seu legítimo interesse, podendo inclusive prestar informações à autoridade de proteção de dados, ou terceiros que solicitarem informações da **CONTRATADA** relativas ao tratamento de dados pessoais, observando a legalidade do pedido, sem necessidade de novo consentimento.

Parágrafo Quinto – A **CONTRATADA**, na assinatura desse contrato, dá consentimento e cede espontaneamente o uso gratuito do direito de sua imagem, voz, nome e dados, para a

CONTRATANTE, que poderá utilizar esses dados em gravações audiovisuais internas e externas. Os dados serão armazenados por tempo indeterminado ou por determinação da autoridade nacional de proteção de dados, podendo ser utilizados para criação e divulgação de conteúdos institucionais em mídias sociais e em mídias impressas.

Parágrafo Sexto – A qualquer momento a **CONTRATADA** poderá solicitar informações, correções, anonimização, bloqueio ou eliminação, portabilidade dentre outras, de acordo com a LGPD, sobre seus dados pessoais mediante requisição formal ao departamento pessoal. Pedidos de exclusão observarão os prazos e as obrigações decorrentes desse contrato de prestação de Serviços Autônomos.

Parágrafo Sétimo – A **CONTRATADA** será integralmente responsável pelo pagamento de perdas e danos de ordem moral e material, bem como pelo ressarcimento do pagamento de qualquer multa ou penalidade imposta à **CONTRATANTE** e/ou a terceiros diretamente resultantes do descumprimento pela **CONTRATANTE** de qualquer das cláusulas previstas neste capítulo quanto a proteção e uso dos dados pessoais.

CLÁUSULA VIGÉSIMA PRIMEIRA – DA REALIZAÇÃO DE *DUE DILIGENCE* DE INTEGRIDADE

Para atender aos padrões de integridade da **CONTRATANTE**, a parte **CONTRATADA** obriga-se a fornecer informações sobre sua estrutura organizacional, relacionamento com agentes públicos, histórico de integridade, relacionamento com terceiros e seus controles de integridade.

CLÁUSULA VIGÉSIMA SEGUNDA – DAS SANÇÕES

Em caso de descumprimento das obrigações assumidas através deste Contrato, a parte transgressora, estará sujeita às sanções de advertência formal, aplicação de multa contratual, no percentual de até 5% (cinco por cento) do valor global do Contrato, bem como a rescisão do contrato e/ou a sua inclusão na Lista Restrita da **CONTRATANTE**.

Parágrafo Único – A **CONTRATADA** declara, neste ato, que está ciente e consente com as penalidades previstas neste Contrato, obrigando-se por si e por seus administradores, sócios ou outra pessoa ou entidade que atue, por qualquer tempo, em seu nome.

CLÁUSULA VIGÉSIMA TERCEIRA – COMUNICAÇÕES

Todas as comunicações e entrega de documentos realizados em razão deste contrato deverão ser feitas por escrito, através de correspondência:

a) Entregue pessoalmente, contrarrecibo;
b) Enviada por carta registrada com Aviso de Recebimento - AR;
c) Enviada por e-mail ou outro meio eletrônico amplamente aceito;
d) Enviada por Cartório de Títulos e Documentos ou por via judicial;
e) Dirigidas e/ou entregues às partes nos endereços constantes do preâmbulo ou encaminhadas para outro endereço que as partes venham a fornecer, por escrito.

Parágrafo Primeiro – Qualquer notificação será considerada como tendo sido devidamente entregue na data da:

a) Assinatura na 2ª (segunda) via da correspondência entregue pessoalmente ou encaminhada mediante protocolo;

b) Assinatura do Aviso de Recebimento - AR;

c) Confirmação expressa da outra parte referente ao recebimento da comunicação via e-mail;

d) Entrega da notificação judicial ou extrajudicial.

Parágrafo Segundo – As partes obrigam-se a comunicar uma à outra, por escrito, toda e qualquer alteração de seu endereço, telefones e e-mails para contato, sob pena de, não o fazendo, serem reputadas válidas todas as comunicações enviadas para o endereço e e-mail constantes de sua qualificação no presente instrumento.

CLÁUSULA VIGÉSIMA QUARTA – DAS DISPOSIÇÕES GERAIS

Parágrafo Primeiro – O presente Contrato rescinde e substitui todos os outros contratos, negócios, ajustes verbais ou escritos referentes ao objeto ora pactuado, eventualmente efetuados pelas partes anteriormente à presente data.

Parágrafo Segundo – As partes contratantes concordam em rever as condições estabelecidas no presente contrato, sempre que alterações supervenientes na legislação vigente ou na conjuntura socioeconômica venham afetar as condições contratuais definidas no presente instrumento.

Parágrafo Terceiro – O presente instrumento somente poderá ser alterado mediante Termo Aditivo firmado entre as partes, sob pena de nulidade da cláusula.

Parágrafo Quarto – Este contrato obriga as partes e seus sucessores a qualquer título.

Parágrafo Quinto – Se porventura existir divergência entre as disposições deste Contrato e a Proposta apresentada pela **CONTRATADA**, prevalecerá o aqui disposto, especialmente pela natureza bilateral desta avença.

CLÁUSULA VIGÉSIMA QUINTA – DO FORO

Fica eleito o Foro da Comarca de Salvador/Bahia, para dirimir as questões oriundas da execução deste instrumento, renunciando as partes a qualquer outro, por mais privilegiado que seja.

E, por estarem justas e contratadas, firmam o presente instrumento, em 02 (duas) vias de igual teor e forma, na presença de duas testemunhas, para que produza seus efeitos legais e jurídicos.

Salvador/BA, 20 de março de 2023.

Assinado eletronicamente por:
José Jorge Urpia
CPF: 123.126.815-87
Data: 22/03/2023 10:25:47 -03:00
MUNDO DIGITAL

INSTITUTO NACIONAL DE TECNOLOGIA E SAÚDE – INTS

Assinado eletronicamente por:
Ricardo Luiz de Oliveira
CPF: 684.548.135-00
Data: 22/03/2023 15:09:19 -03:00
MUNDO DIGITAL

TLD TELEDATA COMERCIO E SERVICOS LTDA

TESTEMUNHAS

Assinado eletronicamente por:
Marcelle Hora
CPF: 006.418.855-80
Data: 22/03/2023 10:35:38 -03:00
MUNDO DIGITAL

NOME:

CPF:

Assinado eletronicamente por:
Luciana Torres Peixoto
CPF: 942.484.945-15
Data: 22/03/2023 10:50:07 -03:00
MUNDO DIGITAL

NOME:

CPF:

MANIFESTO DE ASSINATURAS

Código de validação: NXCHE-68Y4P-4XVWK-3Z97G

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

✔ José Jorge Urpia (CPF 123.126.815-87) em 22/03/2023 10:25 - Assinado eletronicamente

Endereço IP	Geolocalização
189.39.7.228	Não disponível

Autenticação jorgeurpia@ints.org.br

Email verificado

lrtMNpHZ25Ea8P/+qASR6WZEPjV3i9Y2eDx18KSydoc=

SHA-256

✔ Marcelle Hora (CPF 006.418.855-80) em 22/03/2023 10:35 - Assinado eletronicamente

Endereço IP	Geolocalização
189.89.171.194	Lat: -12,983296 Long: -38,453436 Precisão: 13559 (metros)

Autenticação marcelle@tld.com.br

Email verificado

pcDoYuNsLmeIzxTSGlFQMQFhIlweS9tTBp8KxC0Byao=

SHA-256

✔ Luciana Torres Peixoto (CPF 942.484.945-15) em 22/03/2023 10:50 - Assinado eletronicamente

Endereço IP	Geolocalização
191.162.225.127	Não disponível

Autenticação lucianapeixoto@ints.org.br (Verificado)

Login

eJxxogf5HwdaEmMRhWzvoSkiZJRmMUPmlzHZoiCA3Ao= SHA-256

✔ Ricardo Luiz de Oliveira (CPF 684.548.135-00) em 22/03/2023 15:09 - Assinado eletronicamente

Endereço IP	Geolocalização
189.89.171.194	Lat: -12,980124 Long: -38,451947 Precisão: 12 (metros)

Autenticação ricardo@tld.com.br

Email verificado

T5KxzhvFOY+0xYqnDqrg9s18qgA5RG1EGX77PFF8jPs= SHA-256

Para verificar as assinaturas, acesse o link direto de validação deste documento:

https://mundo.easydocmd.com.br/validate/NXCHE-68Y4P-4XVWK-3Z97G

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

https://mundo.easydocmd.com.br/validate