Governo do Distrito Federal
Serviço de Limpeza Urbana do Distrito Federal
Unidade Geral de Tecnologia e Inovação
Gerência de Segurança e Telefonia

Termo de Referência - SLU/PRESI/DTI/UGETI/GESET

TERMO DE REFERÊNCIA

1. **OBJETO**

1.1. Contratação de empresa especializada para fornecer licenciamento de equipamentos de Firewall da marca Fortinet e manutenção, garantia e suporte preventivo e corretivo, de forma contínua, pelo período de 36 (trinta e seis) meses, contados da data de emissão do Termo de Recebimento Definitivo, para que seja possível a continuidade das atividades no setor de segurança.

2. **JUSTIFICATIVA**

2.1. A contratação prevista neste documento demonstra-se indispensável para a segurança, a estabilidade e a funcionalidade dos serviços do SLU para acesso via Internet. A disponibilização de tais serviços devem ser preservadas de forma ativa, com estímulo ao uso de boas práticas e por meio de medidas técnicas compatíveis com os padrões internacionais.

2.1.1. A renovação de licenciamento de Firewall Fortinet Modelo 401E e Aquisição FortiAnalyzer Virtual e Licenciamento com suporte, manutenção e garantia por 36(trinta e seis) meses, treinamento oficial Fortinet NS4 com Voucher de Certificação, conforme especificações e condições estabelecidas pelo SLU, são extremamente necessárias para garantir a confidencialidade e integridade dos sistemas disponibilizados pelo SLU, proporcionando aos serviços públicos, como um todo, melhor segurança nas informações prestadas e melhor desempenho das atividades funcionais.

2.1.2. Renovação das licenças para os Firewalls é essencial, pois o nosso Firewall IP: 10.46.8.1 é utilizado como DATACOM e sem a licença não é possível realizar suporte, manutenção e atualizações de novos softwares e realização de novas políticas na rede do SLU. A renovação do licenciamento visa assegurar que as funcionalidades de segurança estejam atualizadas e alinhadas com as últimas ameaças identificadas.

2.1.3. Ainda, a aquisição do FortiAnalyzer Virtual permitirá uma análise mais abrangente e eficiente dos dados de segurança. Essa ferramenta fornecerá insights detalhados sobre o tráfego de rede, eventos de segurança e comportamento do usuário, contribuindo para uma detecção mais rápida e eficaz de possíveis ameaças.

2.1.4. O treinamento da NSE4 é para a equipe da DTI, responsáveis pelo Firewall, para a utilização tanto do Fortinet Modelo 401E e FortiAnalyzer Virtual, tendo em vista, que é possível a criação de regras para o gerenciamento da rede, bloqueando sites e classificações impróprias para o ambiente de trabalho e a fiscalização e analise pelo FortiAnalyzer. Assim como a empresa é somente para o suporte, manutenção e garantia por 36(trinta e seis) meses, sendo necessário o treinamento da equipe para a realização das atividades..

2.2. Assim sendo, a Diretoria de Tecnologia e Inovação sinaliza a necessidade da contratação do serviço com o intuito de possibilitar conexões seguras, garantindo a confidencialidade e a integridade das informações acessadas pela sociedade.

3. **RESULTADOS ESPERADOS**

3.1. Garantir um ambiente tecnológico adequado e moderno para suportar todas as atividades atuais do SLU;

3.2. Execução contínua das atividades diárias dos Servidores do SLU com maior eficiência e eficácia;

3.3. Equipamentos com garantia e assistência técnica, com meio de permitir um ciclo de vida útil e adequado;

3.4. Potencializar os serviços públicos prestados à sociedade de forma a melhorar qualitativamente e quantitativamente de forma ágil, com eficiência e eficácia, com a aquisição dos novos equipamentos.

4. **CLASSIFICAÇÃO DE BEM COMUM**

4.1. Os objetos a serem adquiridos se enquadram na categoria de bens comuns, nos termos do art. 1º da Lei 10.520/2002, por possuírem padrões de desempenho, qualidade e características gerais usualmente encontradas no mercado.

5. **FUNDAMENTAÇÃO**

5.1. Lei nº 8.666, de 21 de junho de 1993 e alterações;

5.2. Lei nº 10.520, de 17 de julho de 2002 e suas alterações;

5.3. Decreto n° 23.460, de 16 de dezembro de 2002 e suas alterações;

5.4. Lei nº 10.024, de 20 de setembro 2019 e suas alterações;

5.5. Decreto nº 26.851, de 30 de maio de 2006;

5.6. Lei distrital nº 4.770, de 24 de fevereiro de 2012; e

5.7. Decreto nº 36.520, de 28 de maio de 2015 e suas alterações.

6. **COMPOSIÇÃO DO TERMO DE REFERÊNCIA**

6.1. ANEXO I – TERMO DE RECEBIMENTO PROVISÓRIO

6.2. ANEXO II - TERMO DE RECEBIMENTO DEFINITIVO

7. **ESPECIFICAÇÕES**

EQUIPAMENTOS		
Itens	**Descrição do Equipamento**	**Quantidade**
01	Renovação de Licenciamento do Fortigate-401E por período de 3 anos	2
02	Aquisição FortiAnalyzer Virtual e Licenciamento por período de 3 anos	1
03	Treinamento NSE4 + Voucher para prova de certificação	3
	TOTAL	**6**

7.1. **ITEM-1 APPLIANCE UTM (UNIFIED THREAT MANAGEMENT)**

- A solução deverá ser composta da renovação do licenciamento UTP (FC-10-0401E-950-02-36) para os equipamentos FortiGate-401E (SN: FG4H1E5819900230 e FG4H1E5819900311) do tipo *appliance* e software, de mesmo fabricante, com todas as funcionalidades a seguir listadas, instaladas no mesmo *appliance* que compõe a solução, em alta disponibilidade. Para maior segurança, não serão aceito equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN solaris ou GNU/Linux.
- A solução poderá ser entregue em equipamento único ou com composição de vários equipamentos.
- A solução deverá possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades.
- A solução deverá suportar alta disponibilidade ativo-ativo e ativo-passivo em modo transparente.
- A solução deve possuir interface de administração via web no próprio appliance, permitindo configurá-lo diretamente através de um navegador web.
- O equipamento deverá possuir fonte de alimentação com chaveamento automático 110/220 V – 50-60Hz. A fonte fornecida deve suportar sozinha a operação da unidade com todos os módulos de interface ativos.
- A solução deverá ser fornecida com documentação técnica, bem como manual de utilização, em inglês ou português do Brasil.
- A solução deverá estar licenciada para permitir número ilimitado de estações de rede e usuários e deve incluir licença para todas as funcionalidades solicitadas, pelo período de validade do contrato. A licença do gateway de segurança não deve estar vinculada a nenhum IP configurado em suas interfaces.
- A solução deverá possuir bases de dados, assinaturas e engines de segurança desenvolvidas pelo mesmo fabricante do appliance. Não serão aceitas soluções que utilizem módulos de terceiros.
- A solução deverá permitir a exportação do backup das configurações em formato “texto legível”, de tal maneira que possa ser editado manualmente e posteriormente carregado no equipamento.
- Deverão ser fornecidos 2(dois) tokens que devem integrar-se ao sistema de modo que a autenticação do acesso de administração do appliance possa ser feita com senha e token.
- Deverá possuir Certificação ICSA para o Firewall.
- Deverá possuir Certificação ICSA IPSEC. (VPN IPSec).
- Deverá possuir Certificação ICSA para VPN/SSL.
- Deverá possuir Certificação ICSA para Sistema de Detecção de Intrusão.
- Deverá possuir Certificação ICSA para Antivírus.
- Cada appliance de segurança de redes deverá possuir as seguintes especificações técnicas:
- Throughput de Firewall (UDP 512 bytes): 3 Gbps
- Conexões simultâneas: 3 Milhões
- Novas conexões por segundo: 60 Mil
- Throughput de IPSec: 1.2 Gbps
- Quantidade de túneis LAN to LAN: 2 Mil
- Quantidade de túneis CLIENT TO LAN: 5 Mil
- Throughput de VPN SSL: 400 Mbps
- Quantidade de usuários VPN SSL licenciados: 300
- Throughput de IPS: 1.5 Gbps
- Throughput de Antivírus: 1.5 Gbps
- Quantidade de interfaces 1Gbps: 10
- Quantidade de slots SFP incluídas as interfaces: 8
- Capacidade de armazenamento em disco: 120 GBytes
- Quantidade de Instâncias Virtuais Licenciadas: 5
- Capacidade de Roteamento OSPF, BGP, RIP, RIPng
- Suporte à IPv6
- Deverá suportar a criação de instâncias virtuais no mesmo hardware.
- Deverá permitir a criação de administradores independentes para cada uma das instâncias virtuais.
- Deverá permitir a criação de um administrador global que tenha acesso à todas as configurações das instâncias virtuais criadas.

Firewall:

- Deverá possuir controle de acesso à internet por endereço IP de origem e destino.
- Deverá possuir controle de acesso à internet por sub-rede.
- Deverá suportar tags de VLAN (802.1q).
- Deverá suportar agregação de links, segundo padrão IEEE 802.3ad.
- Deverá possuir ferramenta de diagnóstico do tipo tcpdump.
- Deverá possuir integração com Servidores de Autenticação RADIUS, LDAP e Microsoft Active Directory.
- Deverá possuir métodos de autenticação usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet).
- Deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um, STUN, NAT46, NAT64, PAT e Full Cone NAT.
- Deverá permitir controle de acesso à internet por períodos do dia, mês e ano permitindo a aplicação de políticas por horários e por dia da semana.

- Deverá permitir controle de acesso à internet por tempo de conexão consumido por usuário ou grupo de usuários.
- Deverá permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br
- Deverá possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PA
- Deverá suportar roteamento dinâmico RIP V1, RIP V2, ISIS, OSPF e BGPv4.
- Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay
- Deverá suportar aplicações multimídia como: H.323, SIP.
- Deverá possuir Tecnologia de firewall do tipo Stateful.
- Deverá permitir o funcionamento em modo transparente tipo “bridge”, sem alterar o endereço MAC do tráfego.
- Deverá suportar PBR – Policy Based Routing.
- Deverá possuir conexão criptografada entre estação de gerência e appliance, tanto em interface gráfica quanto em CLI (linha de comando).
- Deverá permitir filtro de pacotes sem controle de estado “stateless” para verificação em camada 2.
- Deverá permitir forwarding de camada 2 para protocolos não IP.
- Deverá suportar forwarding de multicast.
- Deverá suportar roteamento multicast PIM Sparse Mode e Dense Mode.
- Deverá permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP.
- Deverá permitir o agrupamento de serviços.
- Deverá permitir o filtro de pacotes sem a utilização de NAT.
- Deverá permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas.
- Deverá possuir mecanismo de anti-spoofing.
- Deverá permitir criação de regras definidas pelo usuário.
- Deverá permitir o serviço de autenticação para HTTP e FTP.
- Deverá permitir IP/MAC binding, de tal forma que cada endereço IP possa ser associado a um endereço MAC gerando maior controle dos endereços internos e impedindo o IP spoofing.
- Deverá operar como um agente sFlow, para a monitoração de tráfego da rede e envio de datagramas para um sFlow Collector externo.

O dispositivo deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: BitTorrent, eDonkey, KaZaa, Azureus, ICQ, Facebook Chat e Twitter.

VPN:

- Deverá possuir algoritmos de criptografia para túneis VPN, AES, DES, 3DES.
- Deverá suportar SHA2 tanto para a requisição de assinatura de certificado (CSR) como para a importação de certificado assinado.
- Deverá suportar a certificados PKI X.509 para construção de VPNs
- Deverá possuir suporte a VPNs IPSec site-to-site, VPNs IPSec client-to-site e SSL VPN.
- Deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais.
- A VPN SSL deverá possibilitar o acesso a toda infra-estrutura do órgão de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java.
- Deverá possuir hardware acelerador criptográfico para incrementar o desempenho da VPN.
- A VPN SSL deverá suportar cliente para plataforma Windows, Linux e Mac OS X.
- Deverá permitir a arquitetura de vpn hub and spoke e deverá possuir a funcionalidade de SSL VPN
- Deverá suportar a VPN do tipo PPTP, L2TP
- Deverá suportar a inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

Intrusion Prevention System (IPS):

- Deverá possuir capacidade de detecção de, no mínimo, 3.000 ataques pré-definidos.
- Deverá estar orientado à proteção de redes.
- Deverá permitir funcionar em modo transparente, sniffer e router.
- Deverá possuir tecnologia de detecção baseada em assinatura.
- Deverá possuir integração à plataforma de segurança.
- Deverá possuir capacidade de remontagem de pacotes para identificação de ataques.
- Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web.
- 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.

Deverá possuir os seguintes mecanismos de detecção/proteção de ataques:

- Reconhecimento de padrões
- Análise de protocolos
- Detecção de anomalias
- Detecção de ataques de RPC (Remote procedure call)
- Proteção contra ataques de Windows ou NetBios
- Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol)
- Proteção contra ataques DNS (Domain Name System)

- Proteção contra ataques a FTP, SSH , Telnet e rlogin
- Proteção contra ataques de ICMP (Internet Control Message Protocol).

Deverá possuir os seguintes métodos de notificação:

- Alarmes na console de administração.
- Alertas via correio eletrônico.
- Monitoração do comportamento do appliance mediante traps SNMP. O dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.

Deverá possuir capacidade de resposta/logs ativa a ataques conforme segue:

- Terminação de sessões via TCP resets.
- Armazenamento de logs de sessões.
- Deverá atualizar automaticamente as assinaturas para o sistema de detecção de intrusos.
- Deverá mitigar os efeitos dos ataques de negação de serviços.
- Deverá permitir a criação de assinaturas customizadas.
- Deverá possuir filtros de ataques por anomalias.
- Deverá permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit.
- Deverá permitir filtros de anomalias de protocolos.
- Deverá suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion.
- Deverá suportar verificação de ataque nas camadas de aplicação.
- Deverá possuir as seguintes estratégias de bloqueio: pass, drop, reset.
- Deverá ser capaz de implementar IPsec VPN em modo transparente.
- Deverá suportar VPN em IPv6, assim como tunelar tráfego IPv4 dentro de túneis IPSec IPv6.

Controle de Aplicações:

- Deverá reconhecer, no mínimo, 700 aplicações.
- Deverá possuir pelo menos 10 categorias para classificação de aplicações.

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

- P2P.
- Instant Messaging.
- Web.
- Transferência de arquivos.
- VOIP.
- Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- Deverá permitir o agrupamento de aplicações de, pelo menos, 3 grupos personalizados.
- Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-a apenas pelo comportamento de tráfego da mesma.
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino.

Deverá permitir a inspeção/bloqueio de códigos maliciosos para no mínimo as seguintes categorias:

- P2P.
- Instant Messaging.
- Transferência de arquivos.
- Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.,

Antivírus:

- Deverá possuir funções de Antivírus e Anti-spyware.
- Deverá possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, SMB e FTP.
- Deverá possuir verificação de vírus para aplicativos de mensagens instantâneas (AIM, MSN, Yahoo Messenger, ICQ).
- Deverá permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.).
- Possuir proteção contra conexões a servidores Botnet.
- Deverá permitir o bloqueio de download de arquivos por extensão, nome do arquivo ou tipo.
- Deverá permitir o bloqueio de download de arquivos pelo seu tamanho.

Antispam:

- Deverá possuir verificação de funcionalidade de anti-spam e a verificação do cabeçalho SMTP do tipo MIME.
- Deverá possuir filtragem de e-mail por palavras chaves.
- Deverá permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM.
- Deverá possuir a funcionalidade de RBL.
- Permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico.

Filtro de Conteúdo Web:

- Deverá possuir solução de filtro de conteúdo web integrado a solução de segurança.
- Deverá possuir pelo menos 70 categorias para classificação de sites web.
- Deverá possuir base mínima contendo, 100 milhões de sites internet web já registrados e classificados.
- Possuir a funcionalidade de cota de tempo de utilização por categoria de Filtro de Conteúdo Web.

Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:

- Proxy anônimo.
- Webmail.
- Instituições de saúde.
- Notícias.
- Phishing.
- Hackers.
- Pornografia.
- Comunidades virtuais.
- Compras.

- Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
- Deverá permitir a criação de pelo menos 05 (cinco) categorias personalizadas.
- Deverá permitir a reclassificação de sites web, tanto por URL quanto por endereço IP.
- Deverá prover o funcionamento de todos os serviços de filtragem web de maneira autônoma, sem a necessidade de conexão permanente com o fornecedor.
- 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.
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do Microsoft Active Directory.
- Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem.
- Deverá exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança do órgão.
- 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, activeX através de: base de URL própria atualizável.
- Deverá permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual.
- Deverá permitir o bloqueio de URLs inválidas cujo o campo CN do certificado SSL não contém um domínio válido.
- Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP.
- Deverá permitir o bloqueio de redirecionamento HTTP.
- Deverá implementar roteamento WCCP e ICAP
- Deverá permitir a criação de regras baseadas em tipos de dispositivos identificados automaticamente (funcionalidade normalmente conhecida como BYOD), como por exemplo tablets, smartphones, PCs, Sistemas Operacionais Linux, Windows, Android, Apple, etc.
- Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Áudio, Vídeo e URLs originadas de Spam.
- Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra.
- Filtro de conteúdo baseado em categorias em tempo real.
- Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web.
- Otimização de Rede Wan

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

- Otimização de protocolos.
- Byte caching.
- Web caching.

Deverá otimizar, no mínimo, os seguintes protocolos:

- CIFS.
- FTP.
- HTTP.

- MAPI.
- Deverá criptografar a comunicação entre os appliances envolvidos na otimização do tráfego através de protocolos IPSEC ou SSH.
- Deverá implementar alta disponibilidade no mínimo ativo-passivo.

Qualidade de Serviços:

- 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.
- Deverá permitir modificação de valores DSCP para o DiffServ.
- Deverá permitir priorização de tráfego e suportar ToS.
- Limitar individualmente a banda utilizada por programas tais como peer-to-peer, streaming, chat, VoIP, web, etc.
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino.
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por categoria de aplicações.

7.2. **ITEM 2 - Ferramenta de Gerenciamento e Armazenamento de Logs**

- A solução deverá ser composta da atualização tecnológica do equipamento FAZ-300E de serial FL-3HFTB20900075, para o equipamento FortiAnalyzer-VM para 10 GB/log dia com licenciamento FortiCare.
- A solução deverá ser gerenciada via interface web;
- Suportar o envio de relatórios de forma automática por e-mail;
- Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato PDF:
- Relatório por Protocolo;
- Relatório de utilização de banda total e por usuário/IP;
- Relatório de utilização por aplicações mais usadas;
- Relatório de utilização das aplicações mais bloqueadas;
- Relatório de utilização Web por categoria e site;
- Relatório de bloqueio Web por categoria e site;
- Relatório de utilização de banda da VPN;
- Relatório de ataques identificados e bloqueados pelo IPS;
- Suportar a pesquisa de um determinado LOG baseado em, no mínimo, Endereço IP de Origem, Endereço IP de Destino e Porta de Destino;
- Suportar atualização do sistema pela interface Web;
- Permitir exportar logs para outras fontes de armazenamento;
- Para as funcionalidades de gerenciamento e relatórios poderão ser utilizadas soluções nativas da própria ferramenta, appliances físicos em separado ou ainda máquina virtual. Em qualquer dos casos, deve-se ser garantida a interação entre todas as funcionalidades com as respectivas soluções e entre si.
- Deverá possuir licença para ativação de funcionalidades de segurança UTP contempla Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and FortiCare Premium).
- Deverá possuir licença 24x7 FortiCare Contract contempla garantia de hardware e atualizações de versões de sistema operacional.
- Deverá possuir relatórios pré definidos na solução de relatórios;
- Deverá permitir clonar e posteriormente editar relatórios existentes;
- Deverá permitir criar capas personalizadas para os relatórios;
- Deverá permitir importar e exportar relatórios;
- Deverá permitir criar gráficos dos tipos barra, linha e tabelas para inserção nos relatórios;
- Deverá possibilitar clonar gráficos existentes de relatórios;
- Deverá permitir criar consultas SQL ou equivalente personalizadas para uso nos gráficos e tabelas dos relatórios;
- Permitir criar relatórios nos formatos HTML, PDF, XML e CSV;
- Permitir o envio automático dos relatórios criados por email;
- Permitir definir individualmente para cada relatório os emails que o receberão;
- Permitir o envio automático dos relatórios criados à um servidor FTP ou SFTP externo à solução;
- Permitir criação de relatórios no idioma Português;
- Permitir programar dia e horário para a geração e envio automático dos relatórios;
- Permitir a definição de filtros nos relatórios;
- Permitir definir o layout do relatório, inserir textos e imagens, incluir gráficos, definir fontes, quebras de páginas, cores, alinhamento, entre outros;
- Deverá permitir definir alertas via email, syslog e snmp traps, baseados em eventos tais como ocorrência de determinado log, severidade de log, entre outros;
- A solução de relatórios deve possuir dashboard gráfico, em tempo real, que indique dos dispositivos gerenciados quais as ocorrências de ameaças, ataques, origens, destinos, países, aplicações, websites, serviços e usuários;
- A solução de relatórios deve possuir gráfico em tempo real indicando qual o consumo de disco e taxa de geração de logs dos dispositivos gerenciados;

- Deverá permitir visualizar de forma centralizada os logs detalhados recebidos por um determinado dispositivo e/ou por todos os dispositivos, incluindo capacidade de aplicação de filtros nas pesquisas destes logs;
- Deverá possibilitar efetuar download dos arquivos de logs recebidos;
- Indicar na GUI da solução de relatórios informações do sistema de logs tais como licenças, uso de CPU, memória, disco, taxa de recebimento de logs por segundo, total de logs diários recebidos, alertas gerados entre outros;
- Suportar capacidade mínima de logs diários de 150 GB/Day;
- Suportar capacidade mínima de processamento de 4.500 log's por segundo

7.3. **ITEM 3 - Treinamento Oficial Fortinet para certificação NS4 das soluções com vouncher para prova de certificação:**

- Treinamento e prova de certificação de acordo com programa de treinamento oficial Fortinet para 03 (três) servidores do SLU.
- O treinamento deverá ser ofertado em Brasília – DF em ambiente disponibilizado pela contratada em horário oposto ao expediente do SLU. Caso não seja possível executar o treinamento em Brasília, deverá ser ofertado pela CONTRATADA o local para treinamento incluindo os custos de passagem, transporte, hospedagem e alimentação para os participantes do treinamento e deverá ser apresentado um cronograma do treinamento.
- O treinamento e seu respectivo exame de certificação devem incluir material didático oficial e os mesmos devem ser aplicados em língua Português-Brasil, sempre que a linguagem for disponibilizada pela FORTINET.
- Caso os treinamentos especificados não estejam mais disponíveis no catálogo de treinamentos do Fabricante, serão aceitos os cursos imediatamente substitutos e com conteúdo compatíveis com os anteriores a critério da CONTRATANTE.
- O calendário de treinamento para cada módulo do treinamento deverá ser ajustado conforme a necessidade do SLU.
- Deverá ser fornecido aos servidores acesso ao ambiente virtual do treinamento NSE 4.
- Suporte deverá ser on-site sempre que solicitado

8. **ESTIMATIVA DE CUSTOS**

ITEM	DESCRIÇÃO	UNID. DE MEDIDA	
1	Renovação de Licenciamento do Fortigate-401E por período de 3 anos	Unidade	
2	Aquisição FortiAnalyzer Virtual e Licenciamento por período de 3 anos	Unidade	
3	Treinamento NSE4 + Voucher para prova de certificação	Unidade	

8.1. A planilha acima reflete as quantidades máximas a serem contratadas para atender ao objeto deste Termo de Referência.

8.2. O orçamento estimado em planilha de quantitativos e preços segue os princípios do art. 8º do decreto nº 39.453, de 14 de novembro de 2018, onde o valor de referência de cada item será o menor preço ou o maior percentual de desconto obtido após o cálculo da média final e mediana final dos valores válidos contidos na pesquisa de preços.

8.3. Ressaltamos que foi realizada pesquisa de mercado de preços públicos, como determina a Lei-DF 5.525/2015 e o Decreto-DF 39.453/2018, entretanto, não foram encontradas cotações que pudessem ser aproveitadas, uma vez que os resultados obtidos são bem diferentes do equipamento a ser contratado, devido à especificidade do objeto. Dessa forma, de acordo com o art. 4º do decreto nº 39.453, de 14 de novembro de 2018, realizamos pesquisa de preços junto aos fornecedores.

9. **JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA**

9.1. O critério de julgamento adotado será o de menor preço valor global por lote, em atenção ao Art. 7º, "caput", do Decreto Federal nº 10.024/2019, recepcionado pelo Decreto Distrital nº 40.205, de 30 de outubro de 2019. Objetivando-se, desta forma, agrupar os itens com características semelhantes, garantindo maior celeridade e eficiência às várias etapas procedimentais relativas à licitação, formalização e acompanhamento da execução do serviço, controle dos atos processuais, com reflexos na economia processual e financeira, além de proporcionar uma maior atratividade para as empresas participantes da licitação. Ademais, em atendimento ao princípio da eficiência, tal critério de julgamento será utilizado com o intuito de preservar a elevada qualidade e nível da execução e acompanhamento dos serviços.

9.2. Ressalte-se, ainda, que o agrupamento visa evitar o desinteresse dos licitantes no fornecimento dos produtos e, consequentemente, a falta de oferta na licitação para algum dos itens, haja vista o baixo quantitativo e valor que serão registrados para cada item, fato este que poderia ocorrer se os itens não fossem agrupados, o que prejudicaria o SLU/DF com a não contratação de determinado serviço. Entende-se, também, que a adjudicação agrupada proporcionará vantagens de natureza logística e econômica. Do ponto de vista logístico, o gerenciamento de um número menor de fornecedores traz benefícios operacionais à Administração. Do ponto de vista econômico, acredita-se que o agrupamento proporcionará a obtenção de proposta mais vantajosa para a Administração, uma vez que será possível a ocorrência da economia de escala que, aplicada ao fornecimento de um grupo de determinados serviços, implicará numa redução de preços ofertados. Salienta-se que tal justificativa econômica só é possível por tratar-se de serviços afins.

10. **CONDIÇÕES COMERCIAIS**

10.1. Encargos Sociais, Impostos e/ou tributos inclusos;

10.2. Prazo de entrega e instalação: 45 (quarenta e cinco) dias corridos;

10.3. Forma de pagamento: até 30 (trinta) dias após o recebimento definitivo de equipamentos e/ou serviços

11. **DA DOTAÇÃO ORÇAMENTÁRIA**

11.1. Cobertura das despesas decorrentes da aquisição, objeto constante deste Termo de Referência, ocorrerá a conta dos recursos específicos consignados ao SLU para o exercício de 2023.

12. **GARANTIA E ASSISTÊNCIA TÉCNICA**

12.1. Todo suporte técnico "on-site" dos itens expostos nesse termo de referência é de responsabilidade exclusiva da CONTRATADA.

12.2. Deverá ser entregue garantia pelo período de 36 (trinta e seis) meses junto ao Fabricante, a contar do momento da assinatura do contrato, para a possibilidade de abertura de chamados e atualização de versão.

12.3. Suporte on-site por período de 36 (trinta e seis) contemplando as seguintes atividades e características:

12.3.1. Serviços de suporte técnico compreendem o atendimento para identificação e correção de falhas ou inconsistências detectadas nos produtos, inclusive nas suas configurações e parametrizações, também se aplica na prestação de informações necessárias ao esclarecimento de dúvidas, de forma a garantir o perfeito funcionamento e utilização dos softwares, de acordo com o estabelecido nos manuais que acompanham o produto.

12.4. A CONTRATADA deverá disponibilizar uma central de atendimento, com números de telefone 0800, e-mail de correio eletrônico e endereço web para abertura de chamados online.

12.5. Toda e qualquer solicitação feita pela CONTRATANTE deverá ser registrada pela CONTRATADA, em sistema informatizado para acompanhamento e controle da execução dos serviços.

12.6. A CONTRATADA deverá comunicar a CONTRATANTE sobre a descoberta de erros (bugs) no software durante toda a vigência do contrato. A descrição destes erros e seus possíveis impactos devem ser divulgados para a CONTRATANTE, tão logo sejam identificados.

12.7. Implementação e configuração da solução no ambiente da CONTRATANTE, conforme as melhores práticas do fabricante da solução.

12.8. Suporte na modalidade remoto e presencial, de acordo com a demanda da CONTRATANTE.

12.9. Resolução de dúvidas e esclarecimentos relativos à utilização e configuração das funcionalidades de hardware e software.

12.10. Resolução de problemas de desempenho de hardware e software.

12.11. Resolução de problemas do software que limitem ou impeçam o desenvolvimento e/ou execução das aplicações da CONTRATANTE que façam uso efetivo das suas funcionalidades.

12.12. O serviço de suporte será prestado em idioma Português do Brasil.

12.13. A CONTRATANTE poderá efetuar um número ilimitado de chamados de suporte durante a vigência da garantia para suprir suas necessidades de utilização do software.

12.14. **NÍVEIS MÍNIMOS DE SERVIÇOS**

12.14.1. A equipe que atuará no projeto deverá ser composta por profissionais treinados e certificados nos produtos ofertados. Ao final das atividades deverá ser entregue toda documentação do projeto em formato Gerencial, em meio impresso e digital.

12.14.2. Os serviços de suporte e assistência técnica deverão atender os seguintes requisitos:

Severidade	Indicador	Prazo de Atendimento	Solução de Contorno	Solução Definitiva
Baixa	Operando normalmente	Imediato via telefone	08 (oito) horas	72 (setenta e duas) hrs
Média	Operando parcialmente	Imediato via telefone e 02 (duas) hora presencial	06 (seis) horas	48 (quarenta e oito) hrs
Alta	Parado	Imediato via telefone e 1 (uma) hora presencial	04 (quatro) horas	24 (vinte e quatro)hrs

13. **QUALIFICAÇÃO TÉCNICA**

13.1. As empresas interessadas deverão comprovar aptidão no desempenho de atividade pertinente compatível em características com o objeto deste Termo de Referência, por meio da apresentação de atestado(s) de aptidão técnica, fornecido(s) por pessoa jurídica de direito público ou privado, declarando ter a empresa licitante fornecido ou estar fornecendo material(is) pertinente(s) e compatível(eis) em características e prazos com objeto deste Termo de Referência.

13.2. Posteriormente, caso haja dúvidas com relação ao conteúdo dos atestados, o SLU poderá, em qualquer fase da licitação, promover diligência destinada a esclarecer ou a complementar a instrução do processo.

14. **OBRIGAÇÕES DA CONTRATANTE**

14.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos.

14.2. Prestar as informações e os esclarecimentos solicitados pela CONTRATADA.

14.3. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente e definitivamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivos;

14.4. Efetuar o pagamento no prazo previsto.

14.5. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da fornecedora, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior, falhas na execução de serviços técnicos e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 21 de junho de 1993.

14.6. Rejeitar, no todo ou em parte, o produto entregue pela CONTRATADA fora das especificações deste Termo de Referência.

14.7. Notificar, formal e tempestivamente, a CONTRATADA sobre quaisquer irregularidades observadas na prestação dos serviços.

15. **OBRIGAÇÕES DA CONTRATADA**

15.1. Indicar formalmente preposto apto a representa-la junto à CONTRATANTE, que deverá responder pela fiel execução do contrato.

15.2. O serviço deverá ser realizado por pessoal técnico treinado e habilitado visto tratar-se de equipamento elétrico e de precisão;

15.3. Efetuar a entrega dos bens nas condições, no(s) prazo(s) e no(s) local(is) indicados pelo SLU, em estrita observância das especificações do Edital e da proposta, acompanhado da respectiva nota fiscal eletrônica constando detalhadamente o preço, as indicações da marca, fabricante, número de série de cada equipamento, modelo, tipo, procedência e prazo de garantia;

15.4. Os bens devem estar acompanhados, ainda, quando for o caso, do manual do usuário, com uma versão em português, e da relação da rede de assistência técnica autorizada;

15.5. Atender prontamente a quaisquer exigências da Administração, inerentes ao objeto do presente Termo de Referência;

15.6. Comunicar ao SLU, com antecedência mínima de 48 (quarenta e oito) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação, o que será analisado pela autoridade competente que somente autorizará a prorrogação nas hipóteses previstas no § 1º, art. 57 da Lei nº 8.666/93.

15.7. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

15.8. Responsabilizar-se pelas despesas dos tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução do contrato.

15.9. Para a instalação e a prestação da garantia, disponibilizar equipe técnica qualificada com responsável, devendo a qualificação ser comprovada conforme legislação vigente quando da assinatura deste contrato.

16. **FORMA DE PAGAMENTO**

16.1. Os pagamentos serão efetuados em 1 (uma) única parcela, mediante apresentação da documentação fiscal e técnica, conforme estabelecido a seguir:

16.1.1. Apresentação de Nota Fiscal pela CONTRATADA, devidamente atestada pelo CONTRATANTE.

16.1.2. Apresentação do Termo de Recebimento Provisório, conforme modelo constante no Anexo III deste Termo de Referência, emitido pelo CONTRATANTE, referente à entrega do equipamento e sua respectiva conferência. O prazo para emissão do Termo será de até 5 (cinco) dias úteis.

16.1.3. O prazo para pagamento após a entrega da documentação fiscal e técnica será de, até, 30 (dez) dias corridos.

16.1.4. Apresentação do Termo de Recebimento Definitivo (TARD), conforme modelo do Anexo II deste Termo de Referência, emitido pelo CONTRATANTE, referente à conclusão desta etapa.

17. **INFRAÇÕES E SANÇÕES ADMINISTRATIVAS**

17.1. Na hipótese de descumprimento parcial ou total pela CONTRATADA das obrigações assumidas, ou de infringência de preceitos legais pertinentes, a CONTRATANTE poderá, garantida a ampla defesa e o contraditório, aplicar, segundo a gravidade da falta cometida, as penalidades de natureza pecuniária e restritiva de direitos previstas no Decreto Distrital nº 26.851, de 30 de maio de 2006 e suas alterações;

17.2. A CONTRATADA responderá solidariamente com seus agentes empregados, prepostos, sujeitando-se a arcar com indenização por perdas e danos patrimoniais e morais e/ou lucros cessantes decorrentes de atrasos na entrega dos equipamentos e ou inexecução dos serviços, salvo se ficar comprovado que ocorreram por motivo de caso fortuito ou de força maior, obrigação legal ou inexistência de culpa ou dolo.

18. **CONDIÇÕES DE ACEITE**

18.1. Provisoriamente, para efeito de verificação da conformidade, em até 5 (cinco) dias úteis após a entrega será elaborado o TERMO DE RECEBIMENTO PROVISÓRIO.

18.1.1. Para verificação técnica dos itens do termo de referência, o SLU fará análise física e lógica do equipamento. Nesta fase, caso a análise não comprove a especificação técnica solicitada neste termo, a licitante será convocada para comprovar o item solicitado através de seu corpo técnico.

18.2. Definitivamente, após a verificação da conformidade com as especificações constantes no Edital e da proposta, e sua consequente aceitação, que se dará em até 15 (quinze) dias após o recebimento provisório.

18.3. No caso de reprovação do objeto, a substituição deverá ocorrer no prazo máximo de 5 (cinco) dias da notificação.

19. **GESTÃO DO CONTRATO**

19.1. **Da coordenação das atividades:**

19.1.1. A coordenação geral, programação, controle, medição, fiscalização e liberação das atividades; toda e qualquer alteração de quantitativos e qualitativos das atividades; toda e qualquer aceitação e aprovação de orçamentos e autorização das atividades não previstas no presente Termo de Referência; todo e qualquer atestado de realização de atividades caberá, única e exclusivamente, ao Diretor-Presidente do SLU, ou a quem por ele for delegado.

19.2. A gestão de contrato é uma atividade crítica e estratégica para garantir o correto funcionamento, manutenção e desempenho desses sistemas essenciais. Nesta função, o contrato tem por garantir que todos os aspectos contratuais sejam cumpridos, bem como o alinhamento contínuo com os objetivos e requisitos estipulados deste Termo de Referência.

19.3. O serviço deverá ser realizado por pessoal técnico treinado e habilitado visto tratar-se de equipamento elétrico e de precisão;

19.4. Atender prontamente a quaisquer exigências da Administração, inerentes ao objeto do presente Termo de Referência;

19.5. A CONTRATADA será responsável pelas despesas dos tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução do contrato.

20. **VIGÊNCIA DE CONTRATO**

20.1. O contrato terá vigência de 36 (trinta e seis) meses, a contar da data de sua assinatura, persistindo as obrigações decorrentes da garantia, quando houver, sendo seu extrato publicado no DODF.

20.2. Tendo em vista que existe contrato com vigência e licença dos equipamentos previsto para encerramento em 31/03/2024, a nova contratação só deverá ser formalizada para vigência a partir de 01/04/2024.

20.3. Na assinatura do contrato será exigida a comprovação das condições de habilitação consignadas neste edital, que deverão ser mantidas pelo contratado durante a vigência contratual.

20.4. O prazo para assinatura do contrato será de **até 5 (cinco) dias úteis** contados a partir da disponibilização do documento para acesso externo via SEI-GDF, podendo ser prorrogado uma vez por igual período, desde que ocorra motivo justificado e aceito pela Administração.

20.5. **Da Garantia Contratual:**

20.5.1. Para garantia deste ajuste, a contratada recolherá no Núcleo de Tesouraria (NUTES) do SLU/DF, em qualquer uma das modalidades previstas no art. 56, § 2º da Lei nº 8.666/1993: "A garantia a que se refere o caput deste artigo não excederá a cinco por cento do valor do contrato e terá seu valor atualizado nas mesmas condições daquele, ressalvado o previsto no parágrafo 3º deste artigo", no percentual de **5% (cinco por cento)** do valor total do contrato.

20.5.2. O total caucionado será liberado ou restituído, após a execução do contrato, desde que não haja obrigação civil ou criminal cominada à contratada, decorrente direta ou indiretamente deste contrato, depois de verificada a quitação de eventuais multas e débitos contratuais.

20.5.3. A garantia do contrato terá validade durante a execução do contrato e 3 (três) meses após o término da vigência contratual.

20.5.4. No caso de garantia prestada em dinheiro, o valor a ser restituído será atualizado monetariamente.

21. **PRAZOS E LOCAIS DE ENTREGA**

21.1. A entrega será efetuada em remessa única com prazo de entrega de até 45 (quarenta e cinco) dias corridos, contados a partir da assinatura do instrumento de contrato.

21.2. Os bens deverão ser entregues na sede do SLU, no endereço: Quadra 08 Bloco “B50” 6º andar Edifício Venâncio 2000 - CEP: 70.333-900. Telefone: 3213-0139/3213-140

22. **DAS DISPOSIÇÕES FINAIS**

22.1. Esclarecimentos relativos ao Termo de Referência serão prestados pela Diretoria de Tecnologia e Inovação – DTI, no horário de 09:00 às 12:00 e 14:00 às 18:00, no SCS Quadra 08 Edifício Venâncio 2000, bloco b-50 6º andar, CEP 70.333-900. Brasília - Distrito Federal, Telefone: (61) 3213-0139.

FABIANO MAGALHÃES SILVA
Membro da Equipe de Planejamento da Contratação

RAFAEL DA SILVA MARCELINO
Membro da Equipe de Planejamento da Contratação

SANSÃO RODRIGO DE SOUZA
Membro da Equipe de Planejamento da Contratação

ANEXOS

ANEXO I - TERMO DE RECEBIMENTO PROVISÓRIO

INTRODUÇÃO
O Termo de Recebimento Provisório declarará formalmente a Contratada que os serviços foram prestados ou os bens foram recebidos para posterior análise das conformidades de qualidade, baseadas nos critérios de aceitação definidos em contrato.

IDENTIFICAÇÃO					
Contrato nº [XXXXXXX] Contratada: [XXXXXX] Contratante: [XXXXXX]					
Ordem de Serviço Nº: <XXXXXXXX>		Data da Emissão: <dia> **de** <mês> **de** <ano>.			
Solução de TI					
ESPECIFICAÇÃO DOS PRODUTOS / SERVIÇOS E VOLUMES DE EXECUÇÃO					
Item	Descrição de Produto e Serviço		Métrica	Quantidade	Total
1.	<Descrição igual da OS de abertura>		<PF ou outra>		
...					
TOTAL DOS ITENS					

Por este instrumento, atestamos para fins de cumprimento do disposto no art. 34, inciso VIII, da Instrução Normativa nº 4/2014 SLTI/MP, que os serviços e/ou bens integrantes da **OS/OFB** acima identificada, ou conforme definido no Modelo de Execução do contrato supracitado, atendem às exigências especificadas no Termo de Referência / Projeto Básico do Contrato acima referenciado.

DE ACORDO	
Gestor do Contrato	**Fiscal Requisitante do Contrato**
_____ <nome do gestor do contrato> Matr.: <nº da matrícula> Local, <dia> de <mês> de <ano>.	_____ <nome do fiscal requisitante do contrato> <Qualificação> Local, <dia> de <mês> de <ano>.

ANEXO II - TERMO DE RECEBIMENTO DEFINITIVO

INTRODUÇÃO	
O Termo de Recebimento Definitivo declarará formalmente a Contratada que os serviços foram prestados ou os bens foram recebidos em conformidade com os critérios de aceitação definidos em contrato.	

IDENTIFICAÇÃO

Contrato nº [XXXXXXX] Contratada: [XXXXXX] Contratante: [XXXXXX]						
Ordem de Serviço Nº: <XXXXXXXX>			Data da Emissão: <dia> **de** <mês> **de** <ano>.			
Solução de TI						
ESPECIFICAÇÃO DOS PRODUTOS / SERVIÇOS E VOLUMES DE EXECUÇÃO						
Item	Descrição de Produto e Serviço			Métrica	Quantidade	Total
1.	<Descrição igual da OS de abertura>			<PF ou outra>		
...						
TOTAL DOS ITENS						

Por este instrumento, atestamos para fins de cumprimento do disposto no art. 34, inciso VIII, da Instrução Normativa nº 4/2014 SLTI/MP, que os serviços e/ou bens integrantes da **OS/OFB** acima identificada, ou conforme definido no Modelo de Execução do contrato supracitado, atendem às exigências especificadas no Termo de Referência / Projeto Básico do Contrato acima referenciado.

DE ACORDO	
Gestor do Contrato	**Fiscal Requisitante do Contrato**
_____ <nome do gestor do contrato> Matr.: <nº da matrícula> Local, <dia> de <mês> de <ano>.	_____ <nome do gestor do contrato> Matr.: <nº da matrícula> Local, <dia> de <mês> de <ano>.

Documento assinado eletronicamente por **RAFAEL DA SILVA MARCELINO - Matr.0277562-X**, **Gerente de Segurança e Telefonia**, em 27/12/2023, às 15:37, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **FABIANO MAGALHÃES SILVA - Matr.0280246-5**, **Gerente de Suporte e Operações**, em 27/12/2023, às 15:39, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **SANSÃO RODRIGO DE SOUZA - Matr.0276334-6**, **Gestor em Políticas Públicas e Gestão Governamental**, em 27/12/2023, às 15:42, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **130024018** código CRC= **FF7736FA**.