CONTRATO N.º 834/2024 - IGESDF

EDITAL DE CHAMAMENTO N.º 034/2024

PROCESSO SEI/GDF N.º 04016-00030943/2024-24

CONTRATO QUE ENTRE SI CELEBRAM O **INSTITUTO DE GESTÃO ESTRATÉGICA DE SAÚDE DO DISTRITO FEDERAL - IGESDF** E A EMPRESA **VOGEL SOLUCOES EM TELECOMUNICACOES E INFORMATICA S.A.**, PARA CONTRATAÇÃO DE **EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS DE CONECTIVIDADE EM SD-WAN PARA INTERLIGAÇÃO DAS UNIDADES DA CONTRATANTE POR MEIO DE UMA REDE DE DADOS, INCLUINDO O GERENCIAMENTO E A SEGURANÇA DA REDE (TODOS POR DEMANDA),** PARA ATENDER ÀS NECESSIDADES DAS UNIDADES DE SAÚDE ADMINISTRADAS PELO INSTITUTO DE GESTÃO ESTRATÉGICA DE SAÚDE DO DISTRITO FEDERAL – IGESDF.

O **INSTITUTO DE GESTÃO ESTRATÉGICA DE SAÚDE DO DISTRITO FEDERAL — IGESDF**, pessoa jurídica de direito privado, inscrito no CNPJ/MF sob o n.º **28.481.233/0001-72**, constituído sob a forma de Serviço Social Autônomo (SSA), instituído pela Lei Distrital n.º 5.899, de 3 de julho de 2017, com nomenclatura alterada pela Lei Distrital n.º 6.270, de 30 de janeiro de 2019, regulamentado por meio do Decreto n.º 39.674, de 19 de fevereiro de 2019, sediado no SHMS — Área Especial — Quadra 101 — Bloco A, Brasília-DF, CEP: 70.335-900, neste ato representado por seu Diretor Presidente - Substituto, o Senhor **CLEBER MONTEIRO FERNANDES**, portador do RG n.º *****.*16 SSP/DF**, inscrito no CPF sob o n.º **144.***.711-**** e seu Diretor de Administração e Logística, o Senhor **RUBENS DE OLIVEIRA PIMENTEL JÚNIOR**, portador do RG n.º **147***3 SSP/DF** e CPF **669.8**.***-87**, doravante denominado **CONTRATANTE**, do outro lado, a empresa **VOGEL SOLUCOES EM TELECOMUNICACOES E INFORMATICA S.A.,** pessoa jurídica de direito privado, inscrita no CNPJ sob o nº **05.872.814/0001-30**, sediada na **AV PROF VICENTE RAO 1262, JARDIM PETROPOLIS, SÃO PAULO/SP**, CEP: **04.636-001,** telefones: **(34) 3256-2961** e **(11) 3512-1212**, e-mail: **cadastro@cscalgar.com.br**, neste ato representada por seus Representantes Legais, o Sr. **AISLAN CARLOS MENDONÇA**, portador do RG n.º **M79****5 - SSP/MG,** inscrito no CPF n.º **057.***.***-02,** e o Sr. **MÁRCIO DE JESUS DA SILVA,** portador do RG n.º **M57****4 - SSP/MG,** inscrito no CPF n.º **755.***.***-87,** doravante denominada **CONTRATADA**, resolvem celebrar o presente **CONTRATO**, conforme condições e especificações constantes no Regulamento Próprio de Compras e Contratações do IGESDF, consoante a Resolução CA-IGESDF Nº 04/2022, e demais ordenamentos legais pertinentes, que aceitam e se obrigam, ratificam e outorgam, por si e seus sucessores, pelas cláusulas a seguir descritas.

1. DO OBJETO

CLÁUSULA PRIMEIRA – Constitui o objeto do presente processo a **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS DE CONECTIVIDADE EM SD-WAN PARA INTERLIGAÇÃO DAS UNIDADES DA CONTRATANTE POR MEIO DE UMA REDE DE DADOS, INCLUINDO O GERENCIAMENTO E A SEGURANÇA DA REDE (TODOS POR DEMANDA),** para atender às necessidades das unidades de saúde administradas pelo Instituto de Gestão Estratégica de Saúde do Distrito Federal – IGESDF, conforme especificação do **EDITAL DO CHAMAMENTO N.º 034/2024 (147209089)** e **ELEMENTO TÉCNICO N.º 5/2024 (135966678)** e na **Proposta Comercial (152173362)** apresentada pela **CONTRATADA**, documentos integrantes e indissociáveis deste instrumento de **CONTRATO**, como se nele estivesse transcrito.

2. DA DESCRIÇÃO DO OBJETO E VINCULAÇÃO

CLÁUSULA SEGUNDA – O presente **CONTRATO** obedece aos termos do **EDITAL DO CHAMAMENTO N.º 034/2024 (147209089)** e **ELEMENTO TÉCNICO N.º 5/2024 (135966678)**, da Declaração de Disponibilidade Orçamentária emitida pela Coordenação de Custos e Orçamento – Despacho – IGESDF/DVP/GGCFC/CCOR (152567927), do Parecer SEI-GDF n.º 268/2024 - IGESDF/DP/GAB/ASJUR/CJPRO (147072456), emitido pela Assessoria Jurídica e encontra-se conforme o que dispõe o Regulamento Próprio de Compras e Contratações do IGESDF.

PARÁGRAFO PRIMEIRO - A solução será composta por **1 ITEM** dispostos da seguinte forma:

Unidade do IGESDF	Velocidade mínima do Link de Internet	QNTD.de NFGW do TIPO 1	QNTD.de NFGW do TIPO 2	LICENÇA
Hospital de Base – HB	1Gbps	2		PREMIUM
Hospital Regional de Santa Maria – HRSM	1Gbps	2		PREMIUM
Hospital Cidade do Sol - HSOL	300 Mbps		1	PREMIUM

PO700	300 Mbps		1	PREMIUM
SIA	300 Mbps		1	PREMIUM
UPA – Ceilândia	100 Mbps		1	PREMIUM
UPA - Núcleo Bandeirante	100 Mbps		1	PREMIUM
UPA - Recanto das Emas	100 Mbps		1	PREMIUM
UPA - São Sebastião	100 Mbps		1	PREMIUM
UPA – Samambaia	100 Mbps		1	PREMIUM
UPA – Sobradinho	100 Mbps		1	PREMIUM
UPA – Brazlândia	100 Mbps		1	PREMIUM
UPA – Ceilândia (Setor O)	100 Mbps		1	PREMIUM
UPA – Gama	100 Mbps		1	PREMIUM
UPA – Paranoá	100 Mbps		1	PREMIUM
UPA – Planaltina	100 Mbps		1	PREMIUM
UPA – Riacho Fundo II	100 Mbps		1	PREMIUM
UPA – Vicente Pires	100 Mbps		1	PREMIUM
Unidade do IGESDF Tipo 1 (sob demanda)	2Gbps	1		PREMIUM
Unidade do IGESDF Tipo 2 (sob demanda)	1Gbps	1		PREMIUM
Unidade do IGESDF Tipo 3 (sob demanda)	600 Mbps		1	PREMIUM
Unidade do IGESDF Tipo 4 (sob demanda)	300 Mbps		1	PREMIUM
Unidade do IGESDF Tipo 5(sob demanda)	100 Mbps		1	PREMIUM

PARÁGRAFO SEGUNDO - DAS INFORMAÇÕES GERAIS:

I - A prestação dos serviços de conectividade abrange circuitos de comunicação, hardwares e softwares, com as respectivas licenças de uso, assim como instalações, desinstalações, dimensionamentos, configurações, testes, operação, monitoração, gerenciamento, suporte técnico e manutenção.

II - O gerenciamento pretendido abrange as funcionalidades do Gerenciamento da Solução SD-WAN e da GNS.

III - A rede interligará as Unidades da CONTRATANTE, distribuídas conforme relação indicada em anexo V, a qual contempla nome da Unidade, endereço completo, CEP, banda em Mbps e Gbps, bem como novas unidades que vierem a ser requisitadas pela CONTRATANTE, dada a possibilidade de expansão da sua estrutura, mediante prévia análise de custos a ser efetuada pela CONTRATADA, tendo como base os valores vigentes à época da assinatura do Contrato.

IV - A prestação dos serviços de conectividade deverá estar **disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, por 365(trezentos e sessenta e cinco) dias do ano**, durante toda a vigência do contrato.

V - A Solução de SD-WAN comtempla a disponibilização de link de internet e equipamento de Next Generation Firewall (NGFW), de forma que as especificações técnicas, suporte técnico, Service Level Agreement (SLA) e referencial de Glosa, estão disponíveis no ANEXO II .

PARÁGRAFO TERCEIRO- DA TOPOLOGIA FÍSICA:

I - A rede deverá prover a interligação entre as Unidades da **CONTRATANTE**, utilizando Solução SD-WAN via Internet Pública, de acordo com a arquitetura que atende às necessidades da Administração Pública contratante.

PARÁGRAFO QUARTO - DA TOPOLOGIA LÓGICA:

I - A rede deverá prover a interligação entre as Unidades da **CONTRATANTE**, utilizando Solução SD-WAN via Internet Pública, de modo a permitir a conectividade dessas unidades, conforme exemplificado na Figura constante no item **27.10** do Elemento Técnico:

II - A rede de dados deverá suportar topologia par full-mesh ou parcial mesh em todas as Unidades da **CONTRATANTE** deverão ter conectividade direta, via túnel VPN, com os N (19) Datacenters referentes a cada unidade do IGESDF.

III - As Unidades da **CONTRATANTE** deverão ter conectividade direta, via tunelamento, com a(s) sua(s) correspondente(s) unidade(s) hierárquica(s).

IV - O limite de atuação da **CONTRATADA**, para cada Unidade da **CONTRATANTE**, é(são) a(s) porta(s) do(s) switch(es) LAN da **CONTRATANTE**, na qual a **CONTRATADA** deverá conectar o(s) cabo(s) proveniente(s) de sua rede e, caso necessário, fornecer a(s) interface(s) e o(s) conversor(es) de mídia.

V - A **CONTRATADA**, disponibilizara informações referente ao SNMP configurado em todos os equipamentos que forem instalados no ambiente da CONTRATANTE para fins de monitoramento dos mesmos.

VI - A **CONTRATANTE** será responsável pela configuração lógica do(s) seu(s) switch(es) e roteador(es) LAN.

VII - A **CONTRATADA** efetivará a **instalação no prazo de até 90 (noventa) dias,** a partir da data da aprovação do Projeto Executivo pelo **CONTRATANTE**.

VIII - Em até **05 (cinco) dias corridos** após a assinatura do contrato, a **CONTRATANTE** deverá realizar reunião inicial do contrato.

IX - Em até **07 (sete) dias corridos** após a realização da reunião inicial, a **CONTRATADA** deverá entregar um Projeto Executivo, contendo, no mínimo:

a) Definição de topologia física e lógica;

b) Plano de Implantação e Migração da Rede;

c) Cronograma de Implantação da Rede;

d) Plano de Endereçamento;

e) Plano de balanceamento do tráfego;

f) Dimensionamento de enlaces e interfaces de comunicação.

X- A elaboração do Projeto Executivo contará com a participação da **CONTRATADA** e **CONTRATANTE**.

a) **SD-WAN**

I - Todos os itens relacionados no anexo I do Elemento Técnico, serão executados sob demanda da **CONTRATANTE**, podendo ser descontinuados a qualquer momento sem ônus ao IGESDF.

II - A Solução de SD-WAN comtempla a disponibilização de link de internet e equipamento de Next Generation Firewall (NGFW), de forma que as especificações técnicas, suporte técnico, Service Level Agreement (SLA) e **Obrigações da Contratada**, estão disponíveis a seguir:

II.1. Tabela Solução SD-WAN:

Solução de SD-WAN				
Unidade do IGESDF	**Velocidade mínima do Link de Internet**	**QNTD.de NFGW do TIPO 1**	**QNTD.de NFGW do TIPO 2**	**LICENÇA**
Hospital de Base – HB	1Gbps	2		PREMIUM
Hospital Regional de Santa Maria – HRSM	1Gbps	2		PREMIUM
Hospital Cidade do Sol - HSOL	300 Mbps		1	PREMIUM
PO700	300 Mbps		1	PREMIUM
SIA	300 Mbps		1	PREMIUM
UPA – Ceilândia	100 Mbps		1	PREMIUM
UPA - Núcleo Bandeirante	100 Mbps		1	PREMIUM
UPA - Recanto das Emas	100 Mbps		1	PREMIUM
UPA - São Sebastião	100 Mbps		1	PREMIUM
UPA – Samambaia	100 Mbps		1	PREMIUM
UPA – Sobradinho	100 Mbps		1	PREMIUM
UPA – Brazlândia	100 Mbps		1	PREMIUM
UPA – Ceilândia (Setor O)	100 Mbps		1	PREMIUM
UPA – Gama	100 Mbps		1	PREMIUM
UPA – Paranoá	100 Mbps		1	PREMIUM
UPA – Planaltina	100 Mbps		1	PREMIUM
UPA – Riacho Fundo II	100 Mbps		1	PREMIUM
UPA – Vicente Pires	100 Mbps		1	PREMIUM
Unidade do IGESDF Tipo 1 (sob demanda)	2 Gbps	1		PREMIUM
Unidade do IGESDF Tipo 2 (sob demanda)	1 Gbps	1		PREMIUM
Unidade do IGESDF Tipo 3 (sob demanda)	600 Mbps		1	PREMIUM
Unidade do IGESDF Tipo 4 (sob demanda)	300 Mbps		1	PREMIUM
Unidade do IGESDF Tipo 5(sob demanda)	100 Mbps		1	PREMIUM

PARAGRAFO QUINTO: DA ESPECIFICAÇÃO DO LINK DE INTERNET:

I- A solução de Link de Internet, inicialmente deverá ser disponibilizado **sobre demanda** conforme Tabela abaixo:

Tabela - Link de Internet	
Unidade do IGESDF	**Velocidade mínima do Link de Internet**
Hospital de Base – HB	1Gbps
Hospital Regional de Santa Maria – HRSM	1Gbps
Hospital Cidade do Sol - HSOL	300 Mbps
PO700	300 Mbps
SIA	300 Mbps
UPA – Ceilândia	100 Mbps
UPA - Núcleo Bandeirante	100 Mbps
UPA - Recanto das Emas	100 Mbps
UPA - São Sebastião	100 Mbps
UPA – Samambaia	100 Mbps
UPA – Sobradinho	100 Mbps
UPA – Brazlândia	100 Mbps
UPA – Ceilândia (Setor O)	100 Mbps
UPA – Gama	100 Mbps
UPA – Paranoá	100 Mbps
UPA – Planaltina	100 Mbps
UPA – Riacho Fundo II	100 Mbps
UPA – Vicente Pires	100 Mbps
Unidade do IGESDF Tipo 1 (sob demanda)	2 Gbps
Unidade do IGESDF Tipo 2 (sob demanda)	1 Gbps
Unidade do IGESDF Tipo 3 (sob demanda)	600 Mbps
Unidade do IGESDF Tipo 4 (sob demanda)	300 Mbps
Unidade do IGESDF Tipo 5(sob demanda)	100 Mbps

II - O serviço internet deverá ser disponibilizado pela **CONTRATADA** com a utilização de protocolo IP e concessão de 1 (um) bloco cidr/27 para cada hospital , 1 (um) bloco cidr/29 para cada unidade (UPAS, PO700 e SIA), link adicional TIPO 1 e TIPO2 1 (um) bloco cidr/27 para cada link solicitado e link adicional TIPO 3, TIPO 4 e TIPO 5 1 (um) bloco cidr/29 para cada link solicitado.

III - Os Links de Internet deverão ser redundantes e possuir rotas e caminhos distintos.

IV - A **CONTRATADA** deverá fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os equipamentos e recursos que forem necessários para o provimento do serviço telecomunicação do IGESDF, especificado no Elemento Técnico.

V - Os equipamentos serão de propriedade da **CONTRATADA** que deverá ser responsável pelo suporte técnico dos mesmos, cumprindo com os tempos de atendimento estabelecidos no Elemento Técnico;

VI - A **CONTRATADA** deverá fornecer o acesso através de meio físico (fibra ótica) instalado diretamente no local indicado pela **CONTRATANTE**;

VII - O serviço a ser fornecido pela empresa a ser contratada deverá, minimamente:

a) Possuir suporte a DNS (resolução direta e reversa), inclusive ao protocolo DNSSEC.

b) Utilizar exclusivamente fibra óptica desde as instalações da empresa a ser contratada até as instalações da Contratante.

c) Suportar QoS (Quality of Service – Qualidade de Serviço).

d) Suportar Tráfego de Videoconferência e Voz sobre IP (VoIP) em todos os componentes e enlaces da rede e em todos os componentes da Solução.

e) Permitir métodos de priorização de tráfego;

f) Utilizar protocolos e padrões internacionais da IEEE, IETF e ITU.

g) Suportar NAT.

h) Suportar LAN Switching: VLAN.

i) Possibilitar que o equipamento a ser disponibilizado para a perfeita execução dos serviços possa ser instalado em rack de 19" da CONTRATANTE.

j) Fornece todo o material e equipamentos necessários para a instalação e operação dos links, como cabos/fibras, tubulações, sistema de aterramento, sistema de proteção contra descarga elétrica e atmosférica, rádios, modems, roteadores, adaptadores etc.

PARÁGRAFO SEXTO- DA ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO (mínima):

I - Será de responsabilidade da **CONTRATADA** fornecer todos os equipamentos e meios necessários à plena prestação dos serviços, excluindo-se o fornecimento de energia elétrica para alimentação dos equipamentos nas dependências das unidades, o aterramento da rede e a climatização das dependências.

II - **CONTRATADA** deverá garantir que a disponibilidade, a segurança, o desempenho e a qualidade do serviço prestado estejam dentro dos limiares estabelecidos pela **CONTRATANTE**.

III - O serviço deve ter a **disponibilidade de 99,5% (noventa e nove vírgula cinco por cento)**, a ser medido e entregue em relatórios mensalmente.

IV - A **CONTRATADA** deverá fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os equipamentos/recursos que forem necessários para o provimento dos serviços, conforme solicitados nesta especificação. Os equipamentos serão de propriedade da **CONTRATADA**, que deverá ser responsável pelo suporte técnico dos mesmos.

V - Deverá ser feito balanceamento de carga dos links de internet de forma automática para garantir a alta disponibilidade dos links especificados no Elemento Técnico.

VI- A **CONTRATADA** deverá garantir que a disponibilidade, a segurança, o desempenho e a qualidade do serviço prestado estejam dentro dos limites estabelecidos pela **CONTRATANTE**.

VII - Faz parte da prestação do serviço, além da porta de interconexão à Internet global de forma dedicada, o transporte do sinal da **CONTRATADA** até as instalações do **CONTRATANTE**.

VIII - A instalação do ponto de acesso físico no **CONTRATANTE** é de responsabilidade exclusiva da **CONTRATADA** e será cobrada apenas no momento da ativação do link.

IX - A **CONTRATADA** deverá fornecer toda a infraestrutura de rede de telecomunicações necessária para disponibilizar os serviços IP para acesso à Internet global de forma dedicada e exclusiva (não compartilhada), com os circuitos de acesso com a mesma capacidade de tráfego nos dois sentidos.

X - A largura de banda deve sempre estar disponível na totalidade do fluxo contratado, respeitando-se o limiar desse Projeto Básico.

XII - A **CONTRATANTE**, em acordo com a **CONTRATADA**, poderá solicitar adequações da capacidade dos enlaces com acréscimo/decréscimo sem ónus para o IGESDF.

XIII - Caso solicitado, a **CONTRATADA** deverá realizar alterações nas taxas de transmissão contratadas, com a adequação dos recursos necessários (roteadores, enlaces, backbone e outros) garantindo o alto desempenho do serviço sem ónus para o IGESDF.

XIV - O backbone da **CONTRATADA** deverá possuir interligação direta através de canais próprios e dedicados.

XV - A **CONTRATADA** deverá fornecer um bloco de endereçamento Ipv4 ou IPv6 para a **CONTRATANTE.**

XVI - A **CONTRATADA** deverá obedecer às recomendações elaboradas pela ABNT para provimento de serviços de acesso à Internet (ISP).

XVII - Os circuitos empregados pela **CONTRATADA** deverão atender às Normas Técnicas Brasileiras e regulamentações da ANATEL, quando essas não entrarem em conflito com o especificado neste documento.

XVIII - A **CONTRATADA** deverá manter o controle da segurança física e lógica de seus ambientes operacionais, estabelecendo as políticas de segurança a serem aplicadas aos serviços de telecomunicações contratados.

XIX - A **CONTRATADA** deverá aplicar e manter atualizados os patches de segurança nos seus roteadores ou em outros equipamentos de suas redes, exclusivos para a prestação de serviços à **CONTRATANTE**.

XX - A **CONTRATADA** deverá realizar análises de vulnerabilidades periódicas nos seus segmentos da rede relacionados à prestação do serviço objeto desta especificação, visando detectar possíveis falhas de segurança da rede.

XXI - A **CONTRATADA** deverá auxiliar a equipe técnica do **CONTRATANTE** na identificação e mitigação de incidentes de segurança que comprometam a disponibilidade do serviço.

XXII - A **CONTRATADA** deverá fornecer roteador CPE com as seguintes características:

a) O roteador CPE deverá ser dimensionado, fornecido, instalado, mantido, gerenciado e operado pela **CONTRATADA** e deverá ser garantido o desempenho e os níveis de serviços contratados;

b) O roteador CPE deverá ser dimensionado para atender o serviço na capacidade máxima de CPU **especificada e de 70% de memória;**

c) O roteador CPE deverá ser fornecido com todos os componentes, módulos e acessórios necessários ao seu perfeito funcionamento;

d) O roteador CPE deverá possuir, no mínimo, **04 (quatro) portas de LAN GigaBit ethernet com conector tipo RJ45 e SFP+ para cabos UTP e fibra ótica** para conexão com a rede local da **CONTRATANTE**;

e) O roteador CPE deverá suportar classificação de tráfego de acordo com, pelo menos, os critérios de IP origem/destino e portas TCP/UDP. Também deverá suportar gerenciamento de filas com base em classes de tráfego.

f) A configuração lógica do roteador CPE será definida pela **CONTRATADA** com a aprovação da **CONTRATANTE**.

XXIII - Em todas as unidades do IGESDF a **CONTRATADA** fornecerá e instalará os roteadores CPEs, equipados com no-break do tipo senoidal on-line com a**utonomia mínima de 30 (trinta) minutos** e quaisquer equipamentos que se façam necessários, os quais ficarão fisicamente instalados nas mesmas dependências das redes locais.

XXIV - Os roteadores CPE deverão ser fornecidos, instalados, mantidos, gerenciados e operados pela **CONTRATADA** e deverá ser garantido o desempenho e os níveis de serviços contratados.

XXV- Cada roteador CPE será fornecido com todos os acessórios e programas necessários à sua instalação, operação e monitoração (cabo de console, cabo de alimentação, cabo V35 e outros cabos e acessórios se fizerem necessários.

XXVI - Todos os roteadores suportarão, além dos protocolos básicos para operação em uma rede IP, Frame Relay e PPP, com compressão de dados e o protocolo de roteamento OSPF. Com opção de security telnet e IP security (IPSec).

XXVII - Os roteadores terão facilidades de configuração através de porta serial e da console de monitoramento.

XXVIII - O roteador de acesso à Internet deverá ter a seguinte configuração mínima:

a) Possuir, **no mínimo, 04 (quatro) portas de LAN GigaBit ethernet sendo 02 (duas) portas com conector tipo RJ45 para cabos UTP e 02 (duas) portas com conector tipo SFP+ para fibra ótica** que seja compatível com o padrão IEEE 802.3;

b) Possuir opção de boot local e permitir armazenamento de firmware e configuração em memória compact flash que deverá ser fornecida caso seja necessário;

c) Possuir no mínimo 256 MB de memória flash ou similar e 2048 MB de memória DRAM, permitindo que o equipamento atenda a todas as funcionalidades exigidas nesta especificação, em conformidade com as recomendações do fabricante;

d) Possuir seu firmware e sistema operacional em versão que atenda a todos os requisitos mínimos necessários (memória, flash, dentre outros) para suportá-lo;

e) Suportar o protocolo de rede IP sobre ATM, compatível com a RFC 2684;

f) Suportar portas seriais Síncronas, Assíncronas, ATM OC3 e Gigabit;

g) Implementar os protocolos de roteamento OSPF (Open Shortest Path First) e BGP 4;

h) Implementar o protocolo de distribuição de endereços IP - DHCP Relay, Server, Client;

i) O protocolo IGMPv1, v2 e v3 (Internet Grouping Message Protocol), PIM-SM e PIM-DM;

j) Implementar, no mínimo, 32 VLAN (Virtual Local Area Network), com base em portas, endereços MAC e Padrão IEEE 802.1q;

k) Implementar NAT (Network Address Translation) e PAT (Port Address Translation);

l) Deverá suportar os padrões QoS (Quality-of-Service), 802.1p e 802.1q;

m) Disponibilizar , no mínimo, dois níveis de senha de acesso;

n) Deve possuir arquitetura modular, permitindo a substituição de interfaces e do módulo de processamento central;

o) Capacidade de comutação mínima de 1.400 (mil e quatrocentos) kbps disponível no equipamento;

p) Permitir a criação de funções de filtragem baseada em listas de controle de acesso com capacidade de filtrar através de endereços de origem e destino e porta UDP e TCP de origem e destino (ACL Básicas e Estendidas - Lista de controle de acesso) 3 mil linhas;

q) Deverá ser do mesmo fabricante e compartilhar a mesma sintaxe de comandos dos demais roteadores fornecidos;

r) Deve possuir interfaces com velocidades iguais ou superiores às especificadas para os links fornecidos;

s) Permitir a configuração remota através de TELNET, SSH e por porta console RJ-45. O equipamento deverá possuir, além da porta console, porta auxiliar que permita a ligação de modem externo;

t) Deverá ser compatível com, pelo menos, um dos protocolos a seguir: NetFlow, NetStream ou IPFIX, de forma a permitir estatísticas mais apuradas do tráfego;

u) Implementar IPSEC com criptografia em hardware. Devem ser suportados 1500 túneis externos IPSEC simultâneos, com capacidade mínima de 8 Mbps de tráfego criptografado em 3DES/MD5, considerando-se pacotes de 1400 bytes;

v) Deve implementar a criação de tuneis VPN dinamicamente, de forma a garantir que escritórios remotos criem túneis entre si sob demanda, mesmo quando associados a endereços IP dinâmicos.

PARÁGRAFO SÉTIMO- DO Anti-DDOS:

I - A **CONTRATADA** deverá disponibilizar em seu backbone proteção contra-ataques de negação de serviços, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DOS e DDoS de acordo considerando os requisitos mínimos a seguir:

a) Serviços deverão ter proatividade para solução e prevenção de incidentes e ataques;

b) Monitorar disponibilidade e desempenho de todos os links de dados existentes no elemento técnico em **regime de 24 (vinte e quatro) horas por dia, nos 7 (sete) dias da semana, durante os 365 (trezentos e sessenta e cinco) dias do ano** utilizando profissionais de forma dedicada;

c) Tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento do mesmo pela contratada.

d) A solução deve possuir a capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações própria, gerada durante a filtragem de ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.

e) A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes malformados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP, dentre outras.

II - A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, incluindo, mas não se restringindo aos seguintes:

a) Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;

b) Ataques à pilha TCP, incluindo mal-uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;

c) Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;

d) Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);

e) Ataques à camada de aplicação, incluindo protocolos HTTP e DNS.

f) A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um determinado período considerado seguro pela **CONTRATADA**.

g) A **contratada** deve mitigar ataques por **3 horas**, caso o ataque ultrapasse o SLA de mitigação contratado.

h) Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole,

i) As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques.

j) A **CONTRATADA** deve disponibilizar um Centro Operacional de Segurança (ou SOC – Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone 0800, correio eletrônico, em idioma português brasileiro, **durante as 24 (vinte e quatro) horas por dia, nos 7 (sete) dias da semana, durante os 365 (trezentos e sessenta e cinco) dias do ano**, no período de vigência contratual.

k) A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento.

l) Em momentos de ataques DOS e DDoS, todo tráfego limpo deve ser reinjetado na infraestrutura da contratante através de túneis GRE (Generic Routing Encapsulation), configurado entre a plataforma de DOS e DDoS da contratada e o CPE do contratante.

m) Para a mitigação dos ataques não será permitido o encaminhamento do tráfego para limpeza fora do território brasileiro.

n) As funcionalidades de monitoramento, detecção e mitigação de ataques devem ser mantidas em operação ininterrupta **durante as 24 (vinte e quatro) horas por dia, nos 7 (sete) dias da semana, durante os 365 (trezentos e sessenta e cinco) dias do ano, no período de vigência contratual.**

o) Em nenhum caso será aceito bloqueio de ataques de DOS e DDoS por ACLs em roteadores de bordas da contratada.

p) A contratada deve iniciar a mitigação de ataques de DDoS em pelo menos **15 minutos.**

q) Cada alerta deverá ter um número de identificação que facilite sua consulta.

r) Informar a data de início e fim do acompanhamento do alerta.

s) Volume de ataques sumarizados por hora, dia, semana e mês.

t) Relatório por tipos de ataques.

u) O Portal de monitoração da **CONTRATADA** deverá possuir uma interface única para acesso às suas funcionalidades, independentemente dos equipamentos ou tecnologias empregadas para a prestação dos serviços.

v) O Portal de Gerência deverá permitir o acesso simultâneo a, pelo menos, um administrador de rede da **CONTRATANTE**.

PARÁGRAFO OITAVO- DA ESPECIFICAÇÕES NEXT GENERATION FIREWALL - NFGW (POR DEMANDA):

I - A solução NFGW será distribuída em TIPO 1 e TIPO 2 contemplando licença PREMIUM para todos os equipamentos, conforme Tabela a abaixo:

Tabela - Next Generation Firewall (NFGW)			
Unidade do IGESDF	**QNTD.de NFGW do TIPO 1**	**QNTD.de NFGW do TIPO 2**	**LICENÇA**
Hospital de Base – HB	2		PREMIUM
Hospital Regional de Santa Maria – HRSM	2		PREMIUM
Hospital Cidade do Sol - HSOL		1	PREMIUM
PO700		1	PREMIUM
SIA		1	PREMIUM
UPA – Ceilândia		1	PREMIUM
UPA - Núcleo Bandeirante		1	PREMIUM
UPA - Recanto das Emas		1	PREMIUM
UPA - São Sebastião		1	PREMIUM
UPA – Samambaia		1	PREMIUM
UPA – Sobradinho		1	PREMIUM
UPA – Brazlândia		1	PREMIUM
UPA – Ceilândia (Setor O)		1	PREMIUM
UPA – Gama		1	PREMIUM
UPA – Paranoá		1	PREMIUM
UPA – Planaltina		1	PREMIUM
UPA – Riacho Fundo II		1	PREMIUM
UPA – Vicente Pires		1	PREMIUM
Unidade do IGESDF Tipo 1 (sob demanda)	1		PREMIUM
Unidade do IGESDF Tipo 2 (sob demanda)	1		PREMIUM
Unidade do IGESDF Tipo 3 (sob demanda)		1	PREMIUM
Unidade do IGESDF Tipo 4 (sob demanda)		1	PREMIUM
Unidade do IGESDF Tipo 5(sob demanda)		1	PREMIUM

II - Solução de NFGW Principais (TIPO 1) devem ser compostas deve ser composta por 2 equipamento configurados em Cluster, já a Solução de NFGW Secundaria (TIPO 2) deve ser composta por 1 equipamento.

PARÁGRAFO NONO- DETALHAMENTO TÉCNICO PARA SOLUÇÃO DE NFGW DO TIPO 1: (modelo de referencia Fortigate 401F, modelo atual Fortigate 500E).

I - 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.

II - A solução deve suportar a configuração de cluster de alta disponibilidade no modo ATIVO-ATIVO e ATIVO-PASSIVO.

III - 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, desde que ocupem até 4U, no máximo.

IV - Deve possuir e estar licenciado durante a vigência do contrato, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention e contextos virtuais.

V - Deve possuir fonte de alimentação com chaveamento automático 110/220V.

VI - Deve possuir firewall com capacidade mínima de processamento de 79 (setenta e nove) Gbps;

VII - Deve possuir IPS com capacidade mínima de processamento de 12 (doze) Gbps;

VIII - Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 9 (nove) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas, podendo evoluir para até 10 (dez) Gbps durante a vigência do contrato, caso haja necessidade técnica.

IX - Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 3 (tres) Gbps;

X - Deve possuir VPN com capacidade de, pelo menos, 50 (cinquenta) Gbps de tráfego IPSec;

XI - Deve suportar 7.000.000 (sete milhões) conexões simultâneas;

XII - Deverão ser licenciados para suportar, pelo menos, 5.000 (cinco mil) usuários de VPN SSL.

XIII - Deve suportar, pelo menos, 450.000 (quatrocentos e sessenta mil) novas conexões por segundo;

XIV - Deve suportar, pelo menos, 2.000 (dois mil) túneis de VPN Site-Site.

XV - Deve suportar, pelo menos, 45.000 (quarenta e cinco mil) túneis de VPN Client- Site;

XVI - Deve possuir, pelo menos, 16 (dezesseis) interfaces RJ 45.

XVII - Deve possuir, pelo menos, 8 (oito) interfaces Gigabit SFP.

Deve possuir, pelo menos, 2 (quatro) interfaces 10 Gigabit SFP+.

XVIII - Deve incluir licença para a funcionalidade de VPN SSL.

XIX - Deve estar licenciado para 10 (dez) instâncias de firewalls virtuais.

XX - Deve possuir armazenamento interno minimo de 2x 480 (quatrocentos e oitenta) Gbps SSD;

XXI - Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.

XXII - Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

PARÁGRAFO DÉCIMO- DETALHAMENTO TÉCNICO PARA SOLUÇÃO DE NFGW DO TIPO2: (modelo de referencia Fortigate 61F, modelo atual não possuímos).

I - 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.

II - A solução deve suportar a configuração de cluster de alta disponibilidade no modo ATIVO-ATIVO e ATIVO-PASSIVO.

III - 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, desde que ocupem até 4U, no máximo.

IV - Deve possuir e estar licenciado durante a vigência do contrato, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention e contextos virtuais.

V - Deve possuir fonte de alimentação com chaveamento automático 110/220V.

VI - Deve possuir firewall com capacidade mínima de processamento de 10 (dez) Gbps.

VII - Deve possuir IPS com capacidade mínima de processamento de 1 (um) Gbps.

VIII - Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 700 (seiscentos) Mbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.

IX - Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 700 (setecentos) Mbps.

X - Deve possuir VPN com capacidade de, pelo menos, 6 (seis) Gbps de tráfego IPSec.

XI - Deverão ser licenciados para suportar, pelo menos, 200 (duzentos) usuários de VPN SSL.

XII - Deve suportar, pelo menos, 35.000 (trinta e cinco mil) novas conexões por segundo.

XIII-Deve suportar, pelo menos, 150 (cento e cinquenta) túneis de VPN Site- Site.

XIV - Deve suportar, pelo menos, 500 (quinhentos) túneis de VPN Client-Site.

XV - Deve possuir, pelo menos, 10 (dez) interfaces RJ45.

XVI - Deve incluir licença para a funcionalidade de VPN SSL.

XVII - Deve estar licenciado para 10 (dez) firewalls virtuais.

XVIII - Deve possuir armazenamento interno minimo de 128 (cento e vinte oito) Gbps SSD;

XIX - Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.

XX - Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

XXI - Caso a empresa ganhadora esteja ofertando todos os produtos do lote sendo do mesmo fabricante será permitido a Solução de Gerenciamento e Controle dos itens deste lote, desde que todas as características sejam atendidas;

PARÁGRAFO DÉCIMO PRIMEIRO- DOS REQUISITOS GERAIS DE FUNCIONALIDADES E LICENCIAMENTOS COMUNS para NGFW do TIPO 1 e TIPO 2

1 - FUNCIONALIDADES DE FIREWALL:

a) Deve possuir controle de acesso à internet por endereço IP de origem e destino;

b) Deve possuir controle de acesso à internet por sub-rede;

c) Deve suportar tags de VLAN (802.1q);

d) Deve possuir ferramenta de diagnóstico do tipo tcpdump;

e) Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

f) Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

g) Deve suportar single-sign-on para Active Directory, RADIUS;

h) Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

i) Deve 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) Deve permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

l) Deve permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;

m) Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

n) Deve suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

o) Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;

p) Deve suportar aplicações multimídia, como: H.323 e SIP;

q) Deve possuir tecnologia de firewall do tipo Statefull;

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

s) Deve permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;

t) Deve suportar PBR – Policy Based Routing;

u) Deve permitir a criação de VLANS no padrão IEEE 802.1q;

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

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

z) Deve permitir forwarding de camada 2 para protocolos não IP;

aa) Deve suportar forwarding multicast;

ab) Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;

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

ad) Deve permitir o agrupamento de serviços;

ae) Deve permitir o filtro de pacotes sem a utilização de NAT;

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

ag) Deve possuir mecanismo de anti-spoofing;

ah) Deve permitir criação de regras definidas pelo usuário;

ai) Deve permitir o serviço de autenticação para tráfego HTTP e FTP;

aj) Deve 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;

al) Deve possuir a funcionalidade de balanceamento e contingência de links;

am) Deve suportar sFlow;

an) O dispositivo deve ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas.

ao) Deve 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;

ap) Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

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

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

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

at) Deve 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;

au) Deve suportar SIP, H.323 e SCCP NAT Traversal;

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

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

2 - FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

a) Deve 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) Deve permitir modificação de valores DSCP para o DiffServ;

c) Deve permitir priorização de tráfego e suportar ToS;

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

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

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

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

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

i) Deve controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;

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

3- FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY

a) Deve permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;

b) Deve possuir filtragem de e-mail por palavras chaves;

c) Deve permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;

d) Deve possuir, para a funcionalidade de anti-spam, o recurso de RBL;

e) Deve permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;

4- FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

a) Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança;

b) Deve possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;

c) Deve possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;

d) Deve possuir a funcionalidade de cota de tempo de utilização por categoria;

e) Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo; Webmail; Instituições de saúde; Notícias; Phishing; Hackers; Pornografia; Racismo; Websites pessoais; Compras;

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

g) Deve permitir a criação de, pelo menos, 07 (sete) categorias personalizadas;

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

i) Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado;

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

l) Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

m) Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

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

o) Deve 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;

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

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

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

s) Deve filtrar o conteúdo baseado em categorias em tempo real;

t) Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;

u) Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

v) Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

x) Deve permitir a criação de regras para acesso/bloqueio por sub-rede de origem;

z) Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;

aa) Deve permitir o bloqueio de redirecionamento HTTP;

ab) Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;

ac) Deve possuir Proxy Explícito e Transparente;

ad) Deve implementar roteamento WCCP e ICAP;

5- FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

a) Deve 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) Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;

c) Deve estar orientado à proteção de redes;

d) Deve permitir funcionar em modo transparente, sniffer e router;

e) Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

f) Deve permitir a criação de padrões de ataque manualmente;

g) Deve possuir integração à plataforma de segurança;

h)Deve possuir capacidade de remontagem de pacotes para identificação de ataques;

i) Deve 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;

j) Deve 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;

l) Deve possuir mecanismos de detecção/proteção de ataques;

m) Deve possuir reconhecimento de padrões;

n) Deve possuir análise de protocolos;

o) Deve possuir detecção de anomalias;

p) Deve possuir detecção de ataques de RPC (Remote Procedure Call);

q) Deve possuir proteção contra-ataques de Windows ou NetBios;

r)Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);

s) Deve possuir proteção contra-ataques DNS (Domain Name System);

t) Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;

u) Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);

v) Deve possuir métodos de notificação de detecção de ataques;

x) Deve possuir alarmes na console de administração;

z) Deve possuir alertas via correio eletrônico;

aa) Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

ab) Deve ter a capacidade de resposta/logs ativa a ataques;

ac) Deve prover a terminação de sessões via TCP resets;

ad) Deve armazenar os logs de sessões;

ae) Deve atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

af) Deve mitigar os efeitos dos ataques de negação de serviços;

ag) Deve permitir a criação de assinaturas personalizadas;

ah) Deve possuir filtros de ataques por anomalias;

ai) Deve permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

aj) Deve permitir filtros de anomalias de protocolos;

al) Deve suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

am) Deve suportar verificação de ataque na camada de aplicação;

an) Deve suportar verificação de tráfego em tempo real, via aceleração de hardware;

ao) Deve possuir as seguintes estratégias de bloqueio: pass, drop e reset.

6- FUNCIONALIDADE DE VPN

a) Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

b) Deve possuir suporte a certificados PKI X.509 para construção de VPNs;

c) Deve possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to- Site;

d) Deve possuir suporte a VPN SSL;

e) Deve possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

f) A VPN SSL Deve possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;

g) Deve possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;

h) A VPN SSL Deve suportar cliente para plataforma Windows, Linux e Mac OS X;

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

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

7- FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

a) Deve reconhecer, no mínimo, 2.000 (duas mil) aplicações;

b) Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;

c) Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging; Web client; Transferência de arquivos; VoIP;

d) Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

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

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

g) Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

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

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

j) Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

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

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

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

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

p) Deve permitir criação de padrões de aplicação manualmente;

8- FUNCIONALIDADE DE DLP (DATA LEAK PREVENTION)

a) O sistema de DLP (Data Leak Prevention – Proteção contra Vazamento de Informações) de gateway, deve funcionar de maneira que se consiga que os dados sensíveis não saiam da rede e também Deve funcionar de modo que se previna que dados não requisitados entrem na sua rede;

b) Deve inspecionar, no mínimo, os tráfegos de e-mail, HTTP;

c) Sobre o tráfego de e-mail, deve inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;

d) Deve realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS-Word;

e) Deve fazer a varredura no conteúdo de um cookie HTTP buscando por determinado texto;

f) Deve aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;

g) Deve verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio entrantes/saintes possui um tamanho máximo especificado pelo administrador;

h) Deve utilizar expressões regulares para composição das regras de verificação dos tráfegos;

i) Deve 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) Deve 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;

l) Deve 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.

9-FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

a) Deve permitir a criação de endereços IPs virtuais;

b) Deve permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;

c) Deve suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

d) Deve permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Static, Round Robin, Weighted, First Alive e HTTP host, Least Session, Least RTT;

e) Deve permitir persistência de sessão por cookie HTTP ou SSL session ID;

f) Deve permitir que seja mantido o IP de origem;

g) Deve suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;

h) Deve 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) Deve permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

10- FUNCIONALIDADE DE VIRTUALIZAÇÃO

a) Deve suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;

b) Deve permitir a criação de administradores independentes para cada uma das instâncias virtuais;

c) Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

11- FUNCIONALIDADE DE SD-WAN

a) 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 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 ou CLI, de forma automática, e sem que o administrador precise configurar site por site.

i) A configuração VPN IPSEC Deve oferecer suporte para DH Group: 14 e 15.

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

l) 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.

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

n)Ainda sobre o reconhecimento de Aplicações, 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).

o) A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a Ipv4 ou IPv6.

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

q) A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.

r) 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.

s) 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.

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

12-FUNCIONALIDADE DE GERENCIAMENTO DO NGFW

a) A solução deve ser baseada em máquina virtual ou appliance físico do mesmo fabricante da solução de NGFW e SD-WAN, e ter como objetivo gerenciar de modo centralizado todos os equipamentos a partir de uma única console de administração;

b) Poderá ser entregue em formato de appliance físico ou appliance virtual;

c) Para appliance virtual, deve ser compatível com VMWare 7.0 e superiores, Hyper-V 2016 e superiores, e KVM. Deverá estar devidamente licenciada para:

c.1) Gerenciar, no mínimo, o total de NGFWs/Clusters unidades (NGFW, SD-WAN ou Sistemas Virtuais) dos equipamentos da solução de NGFW e SD-WAN de forma simultânea;

c.2) Não deverá existir limite para o número de vCPUs no appliance virtual;

c.3) Não deverá existir limite para a expansão da memória RAM no appliance virtual;

d) Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.

e) A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;

f) Deverá garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;

g) Permitir acesso concorrente de administradores, permitindo ainda que seja definida uma cadeia de aprovação das alterações realizadas;

h) Possibilitar a criação e administração de políticas de firewall, controle de aplicação, sistema de prevenção a intrusão (IPS – Intrusion Prevention System), antivírus, filtro de URL e SD-WAN;

i) Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do link, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido;

j) Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de uma única console, além de exibir sua localização geográfica em um mapa;

l) Permitir usar palavras chaves ou cores para facilitar identificação de regras;

m) Permitir localizar em quais regras um objeto (ex. computador, serviço, etc.) está sendo utilizado;

n) Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;

o) Permitir criação de regras que fiquem ativas em horário definido;

p) Permitir criação de regras com data de expiração;

q) Realizar o backup das configurações para permitir o retorno de uma configuração salva;

r) Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso.

s) Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas

t) Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;

u) Garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota de maneira centralizada;

v) Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

x) Deve suportar a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

z) Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, TACACS+ e PKI.

aa)Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;

ab) A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato.

13- FUNCIONALIDADE DE GERENCIAMENTO DE LOGS DO NGFW (online e off-line)

a) Deve ser do mesmo fornecedor das soluções ofertadas, suportando nativamente todos os recursos listados.

b) Deve considerar o volume de equipamentos ofertados, considerando todo o licenciamento necessário para a correta gestão dos elementos de rede;

c) Deve ser fornecido com licenciamento perpétuo, cabendo apenas a renovação de suporte, caso seja de interesse do órgão;

e) Deve suportar a recepção de 100% dos logs com armazenamento mínimo de 6 (seis) meses consecutivos para cada appliance;

f) A **CONTRATADA** deverá no final dos 6 meses entregar o arquivo de Log para **CONTRATANTE**;

g) O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

h) Deve ser fornecido em software que suporte

i) O sistema deverá suportar contas de usuário/senha estáticas;

j) Definição de perfis de acesso à console com permissões granulares como: acesso de escrita e acesso de leitura;

l) O sistema deverá suportar o método de autenticação externo usuário/conta do servidor Radius;

m) A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC;

n) Deve possuir integração nativa com Microsoft Teams;

o) Deve possuir integração via Fluentd, permitindo o streaming de logs para multiplos destinos;

p) Essas comunicações deverão ser protegidas e criptografadas;

q) Deverá permitir que todos os alarmes e eventos sejam registrados na console de Gerência.

r) Deve permitir a correlação de eventos, provendo dashboards diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança;

s) O portal deve permitir uma visão geral do tráfego de rede e da postura de segurança, incluindo widgets intuitivos com informações como principais países, principais ameaças, principais origens de tráfego, principais destinos, principais aplicativos e hits de políticas, bem como gráficos para mostrar logins de administrador, eventos do sistema, e uso de recursos;

t) O portal deve suportar a sua configuração possibilite seu uso via multi-tenant, ou seja, com a possibilidade de se criarem vários portais de acesso independentes entre si para fins de administração distribuída;

u) Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;

v) Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;

x) Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

z) Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

aa)Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

ab) Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

ac) Deve possuir mecanismos de remoção automática para logs antigos;

ad) Permitir importação e exportação de relatórios;

ae) Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;

af) Deve permitir exportar os logs no formato CSV;

ag)Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

ah) Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;

ai) A solução deve ter relatórios predefinidos;

aj) Deve permitir o envio automático dos logs para um servidor FTP externo a solução;

al) Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

am) Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

an) Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

ao) Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

ap) Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;

aq) Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

ar) Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

as) Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

at) Permitir o envio por e-mail relatórios automaticamente;

au) Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;

av) Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

ax) Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;

az) Deve permitir o uso de filtros nos relatórios;

ba)Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

bb)Permitir especificar o idioma dos relatórios criados;

bc)Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;

bd)Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;

be) Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

bf)Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

bg) Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

bh)Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

bi) Deve permitir visualizar em tempo real os logs recebidos;

bj) Deve permitir o encaminhamento de log no formato syslog;

bl) Deve permitir o encaminhamento de log no formato CEF (Common Event Format);

bm) Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;

bn) Deve permitir gerar alertas de eventos a partir de logs recebidos;

bo)Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados, o monitoramento de computadores que estão potencialmente comprometidas ou usuários com uso de rede suspeito;

bp)Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados pelos computadores, atribuição de pontuações de risco que definem os vereditos dos níveis de comprometimento como baixo, médio ou alto;

bq)Deve suportar a análise detalhada dos computadores comprometidos e exibir os detalhes das ameaças detectadas;

br) Deve suportar recursos de automação (playbooks) que, por meio de integrações com soluções de firewall, endpoint, Email, ITSM e eventos pré-determinados, possa tomar ações automáticas visando mitigar riscos;

bs)Deve evidenciar o consumo de banda do SD-WAN ao longo do tempo;

bt) Deve mostrar a utilização de banda por interface e aplicação;

bu)Deve mostrar a performance para uma aplicação especifica de acordo com a latência, jitter, perda de pacote e banda consumida;

bv) Deve mostrar o MOS (Mean Opinion Score) por interface, bem como a qualidade da chamada de voz;

bx) Deve criar automaticamente um gráfico para cada health check criado na solução de SD-WAN, indicando parâmetros como latência, jitter e perda de pacote de acordo com o tempo selecionado;

bz)Deve mostrar o status do ambiente de SD-WAN para, pelo menos: maiores problemas de rede, aplicações mais usadas, elementos que mais consomem banda e MOS;

ca) Deve possuir relatórios nativos de SD-WAN;

cb) Permitir para reconstruir o banco de dados, gerando relatórios a partir de logs arquivados (offline):

cb.1) Permitir reimportar os arquivos de log que foram exportados.

cb.2) A importação deve acionar automaticamente com a inserção dos logs no banco de dados SQL no gerenciador de logs de produção.

cb.3) Sendo possível, em outro gerenciador de logs, se necessário para esta ação, estar licenciado dedicado para esta função, permitir extrair dados de log mais antigos que atendam aos critérios filtrados, evitando assim, a duplicação de logs e a necessidade de alterar repetidamente a Política de Retenção de Logs no Gerenciador de produção.

3. **DO VALOR**

CLÁUSULA TERCEIRA – O **valor mensal estimado** deste **CONTRATO** é de **R$ 102.500,00 (cento e dois mil e quinhentos reais)** e o **valor total estimado** é de **R$ 3.075.000,00 (três milhões setenta e cinco mil reais)**, compreendendo todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação, conforme tabela abaixo:

Unidade do IGESDF	**Velocidade mínima do Link de Internet**	**QNTD.de NFGW do TIPO 1**	**QNTD.de NFGW do TIPO 2**	**LICENÇA**	**Valor Unitário**	**Valor Mensal**	**Valor Global para 30 meses**
Hospital de Base – HB	1Gbps	2		PREMIUM	R$ 16.000,00	R$ 16.000,00	R$ 480.000,00
Hospital Regional de Santa Maria – HRSM	1Gbps	2		PREMIUM	R$ 16.000,00	R$ 16.000,00	R$ 480.000,00
Hospital Cidade do Sol - HSOL	300 Mbps		1	PREMIUM	R$ 3.000,00	R$ 3.000,00	R$ 90.000,00
PO700	300 Mbps		1	PREMIUM	R$ 3.000,00	R$ 3.000,00	R$ 90.000,00

SIA	300 Mbps		1	PREMIUM	R$ 3.000,00	R$ 3.000,00	R$ 90.000,00
UPA – Ceilândia	100 Mbps		1	PREMIUM	R$ 2.200,00	R$ 2.200,00	R$ 66.000,00
UPA - Núcleo Bandeirante	100 Mbps		1	PREMIUM	R$ 2.200,00	R$ 2.200,00	R$ 66.000,00
UPA - Recanto das Emas	100 Mbps		1	PREMIUM	R$ 2.200,00	R$ 2.200,00	R$ 66.000,00
UPA - São Sebastião	100 Mbps		1	PREMIUM	R$ 2.200,00	R$ 2.200,00	R$ 66.000,00
UPA – Samambaia	100 Mbps		1	PREMIUM	R$ 2.200,00	R$ 2.200,00	R$ 66.000,00
UPA – Sobradinho	100 Mbps		1	PREMIUM	R$ 2.200,00	R$ 2.200,00	R$ 66.000,00
UPA – Brazlândia	100 Mbps		1	PREMIUM	R$ 2.200,00	R$ 2.200,00	R$ 66.000,00
UPA – Ceilândia (Setor O)	100 Mbps		1	PREMIUM	R$ 2.200,00	R$ 2.200,00	R$ 66.000,00
UPA – Gama	100 Mbps		1	PREMIUM	R$ 2.200,00	R$ 2.200,00	R$ 66.000,00
UPA – Paranoá	100 Mbps		1	PREMIUM	R$ 2.200,00	R$ 2.200,00	R$ 66.000,00
UPA – Planaltina	100 Mbps		1	PREMIUM	R$ 2.200,00	R$ 2.200,00	R$ 66.000,00
UPA – Riacho Fundo II	100 Mbps		1	PREMIUM	R$ 2.200,00	R$ 2.200,00	R$ 66.000,00
UPA – Vicente Pires	100 Mbps		1	PREMIUM	R$ 2.200,00	R$ 2.200,00	R$ 66.000,00
Unidade do IGESDF Tipo 1 (sob demanda)	2 Gbps	1		PREMIUM	R$ 12.500,00	R$ 12.500,00	R$ 375.000,00
Unidade do IGESDF Tipo 2 (sob demanda)	1 Gbps	1		PREMIUM	R$ 10.600,00	R$10.600,00	R$ 318.000,00
Unidade do IGESDF Tipo 3 (sob demanda)	600 Mbps		1	PREMIUM	R$ 4.600,00	R$ 4.600,00	R$ 138.000,00
Unidade do IGESDF Tipo 4 (sob demanda)	300 Mbps		1	PREMIUM	R$ 3.000,00	R$ 3.000,00	R$ 90.000,00
Unidade do IGESDF Tipo 5(sob demanda)	100 Mbps		1	PREMIUM	R$ 2.200,00	R$ 2.200,00	R$ 66.000,00
VALOR MENSAL DA CONTRATAÇÃO: R$ 102.500,00 (cento e dois mil e quinhentos reais). **VALOR TOTAL PARA 30 MESES: R$ 3.075.000,00 (três milhões setenta e cinco mil reais).**							

4. **DO PRAZO DE VIGÊNCIA**

CLÁUSULA QUARTA – A vigência deste Instrumento Contratual **será de 30 (trinta) meses**, a contar de sua assinatura, podendo ser prorrogado, por igual período, mediante a Termo Aditivo até o limite máximo de 60 (sessenta) meses, conforme preconiza o Regulamento Próprio de Compras e Contratações do IGESDF.

PARÁGRAFO ÚNICO - A referida vigência não exonera o fornecedor do cumprimento da garantia mínima do(s) produto(s), contados a partir da data do termo de recebimento definitivo do objeto.

5. **DO PRAZO DE ENTREGA**

CLÁUSULA QUINTA – O prazo de início e demais eventos relativos à execução do objeto seguirão os critérios definidos no cronograma a seguir:

ID	EVENTO	DESCRIÇÃO
01	Reunião de alinhamento	A primeira reunião de alinhamento, será realizada após 5 dias após assinatura do contrato.
02	*Reunião inicial*	*Em até 07 (sete) dias corridos após a realização da reunião inicial, a CONTRATADA deverá entregar um Projeto Executivo, contendo, no mínimo:* Definição de topologia física e lógica; a) Definição de topologia física e lógica; b) Plano de Implantação e Migração da Rede; c) Cronograma de Implantação da Rede; d) Plano de Endereçamento; e) Plano de balanceamento do tráfego;

		f) Dimensionamento de enlaces e interfaces de comunicação.
03	Entrega	Os equipamentos e acessórios devem ser entregues no prazo de até 60 (sessenta) dias corridos, a contar da assinatura do contrato.
04	Instalação	*A CONTRATADA efetivará a instalação no prazo de até 90 (noventa) dias, a partir da data da aprovação do Projeto Executivo pelo CONTRATANTE*

6. **DA MANUTENÇÃO E SUPORTE TÉCNICO**

CLÁUSULA SEXTA - Manutenção e Suporte Técnico referente a prestação de serviços de SDWAN, devem estar de acordo com o especificado a seguir:

I - O suporte e a manutenção deverão ser providos durante toda vigência do contrato;

II - Deverá monitorar o quantitativo instalado. A **CONTRATANTE**, deve ter acesso de leitura a planilha de monitoração para fins de acompanhamento e auditoria;

III- Dentro do contrato, deverá estar incluída a atualização de softwares, drivers e hardware ou novos releases sem custos adicionais a **CONTRATANTE**.

IV - A **CONTRATADA** deve emitir relatório sempre que ocorrer atualizações de softwares, driver e hardware ou novos releases sem custos adicionais a CONTRATANTE, contendo:

a) Descrição do procedimento que será executado;

b) Cronograma de Atividades;

c) Impacto e eventuais procedimentos de contingência;

d) Bem como relatório posterior sobre os resultados obtido.

V- O Suporte deverá ser prestado com disponibilidade **24 (vinte e quatro)** horas por dia, **7 (sete) dias** na semana, durante os **365 (trezentos e sessenta e cinco)** do ano.

VI- Deverá ser disponibilizado pela **CONTRATADA**, os meios necessários para que os técnicos especialistas executem suas atividades (equipamentos, ferramentas e transporte) sem ônus para **CONTRATANTE**.

VII- A **CONTRATADA**, deverá utilizar a ferramenta de ITSM da **CONTRATANTE**, para registro de chamados, acompanhamento dos chamados e emissão de relatórios.

VIII- Todo chamado deve ser registrado em ITSM próprio da **CONTRATANTE**, em que haja possibilidade de visualização por parte da **CONTRATADA**.

IX - Para finalizar os chamados registrados devem ser inseridos os registros das tratativas adotadas.

X Todo e qualquer problema detectado nos itens/serviços descritos no Elemento Técnico, deverão ser, de forma imediata, ser relatados à equipe de Fiscais do **CONTRATANTE**.

XI - Todas as mudanças adotadas por iniciativa da **CONTRATADA** nas configurações, deverão ser efetuadas mediante aprovação do **CONTRATANTE**, por se tratar de ambiente Hospitalar.

XII -A **CONTRATADA** deverá emitir uma declaração prévia, com **antecedência mínima de 48 (quarenta e oito) horas**, contendo:

a) Descrição do procedimento que será executado;

b) Cronograma de Atividades;

c) Impacto e eventuais procedimentos de contingência;

d) Bem como relatório posterior sobre os resultados obtido.

XIII- suporte deverá incluir resposta a chamados críticos **em tempo inferior a 60 (sessenta) minutos e permitir a comunicação por meio de e-mail, whatsapp ou telefone** (devendo a **CONTRATADA** fornecer um número telefônico para contato direto da **CONTRATANTE** com a **CONTRATADA**). No momento do aceite de cada ordem de serviço, a CONTRATADA deverá comprovar está em operação o suporte técnico descrito neste item.

XIV- Os serviços de Suporte Técnico compreendem todos os chamados rela vos aos itens referenciados no Elemento Técnico, com serviço previamente planejado e executado pela **CONTRATADA**, bem como todos os chamados que objetivem esclarecer dúvidas na utilização dos serviços prestados diretamente pelo provedor, independentemente de esses serviços terem sido provisionados pela **CONTRATADA** ou pela **CONTRATANTE.**

XV- Os serviços de suporte técnico deverão ser prestados pela **CONTRATADA** sem qualquer ônus adicional para a **CONTRATANTE**.

XVI- Os chamados de suporte técnico serão classificados por Criticidade, de acordo com o impacto no ambiente computacional da **CONTRATANTE.**

XIVII- Serão utilizados **3 (três) níveis**, com prazo de início do atendimento e prazo para conclusão **conforme Tabela 01 – SLA de atendimento**.

a) **Criticidade Alta** - Deveremos entender como criticidade ALTA um serviço totalmente fora de operação, co**m SLA de 20 minuto**s para captura de chamado e início de atendimento, e **até 04 horas** para resolução do problema.

b) **Criticidade Média** - Deveremos entender como Severidade Média incidentes que não impeçam o uso do equipamento, serviços e/ou consultas em geral, com SLA de **20 minutos** para captura de chamado e início de atendimento e **até 06 horas** para resolução do problema;

c) **Criticidade Baixa** - Deveremos entender como Severidade Baixa os testes funcionais e consultas gerais do equipamento, com SLA de **20 minutos** para captura de chamado e início de atendimento e **até 08 horas** para resolução do problema.

XVIII- Para fins de verificação do atendimento, os chamados serão agrupados por nível de severidade e seus prazos de atendimento serão contabilizados mensalmente, conforme **Tabela 01 – SLA de atendimento:**

Tabela 1 – SLA de Atendimento				
Criticidade	**Descrição**	**Prazo para início do atendimento**	**Prazo para conclusão do atendimento**	**Desconto por não atendimento no prazo**

Alta	Deveremos entender como criticidade ALTA um serviço totalmente fora de operação	20 minutos para captura de chamado	Até 04 horas para resolução do problema	1,5%
Média	Deveremos entender como Severidade Média incidentes que não impeçam o uso do equipamento, serviços e/ou consultas em geral	20 minutos para captura de chamado	Até 06 horas para resolução do problema	1,0%
Baixa	Deveremos entender como Severidade Baixa os testes funcionais e consultas gerais do equipamento	20 minutos para captura de chamado	Até 08 horas para resolução do problema	0,5%
Observação	Troca de equipamentos	30 minutos após abertura do chamado	A CONTRATADA deverá providenciar equipamento reserva de falhas e este equipamento deverá estar disponível em até 1 (um) dia corridos. Obs: Podendo ser negociado com a Gestão	2,0% por dia em atraso

7. **DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA**

CLÁUSULA SÉTIMA- A **Contratada** se obriga a:

I - Prestar os serviços com pessoal adequadamente qualificado e capacitado para suas atividades.

II - Cumprir rigorosamente todas as programações e atividades do objeto do contrato.

III - Prestar os serviços de acordo com o especificado neste instrumento.

IV - Levar imediatamente ao conhecimento da Fiscalização qualquer fato extraordinário ou anormal que ocorra durante a execução dos serviços a fim de que sejam adotadas medidas cabíveis, bem como comunicar por escrito e de forma detalhada todo tipo de incidente que venha a ocorrer.

V - Prestar todos os esclarecimentos que forem solicitados pela Fiscalização, atendendo de imediato as solicitações.

VI - Responder pelos danos causados ao IGESDF ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução dos serviços.

VII - Arcar com despesas decorrentes de infrações relacionadas ao disposto no objeto deste instrumento, durante o desempenho das funções, ainda que fora das dependências do IGESDF.

VIII - Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às recomendações aceitas pela boa técnica, normas e legislação. Garantir a supervisão permanente dos serviços de forma a obter uma operação correta e eficaz.

IX - Manter suporte inerente aos serviços a serem executados, garantindo um serviço de alto padrão, sem nenhum custo adicional para o IGESDF.

X - Atender prontamente quaisquer exigências do representante do IGESDF inerentes ao objeto do Contrato.

XI - Fornecer, na forma solicitada pelo IGESDF, o demonstrativo de utilização dos serviços, objeto do Contrato.

XII - Comunicar ao IGESDF, por escrito, qualquer anormalidade, sobretudo de caráter urgente, e prestar os esclarecimentos julgados necessários.

XIII - Manter, durante toda a execução do Contrato, em compatibilidade com as obrigações a serem assumidas, todas as condições de qualificação exigidas na contratação, inclusive por meio da atualização dos seus profissionais.

XIV - Indicar um preposto para acompanhar a execução do contrato e responder perante o **CONTRATANTE**.

XV - A **CONTRATADA** deve manter Matriz, Filial ou Escritório de Representação no Distrito Federal, durante toda a vigência do Contrato, com condições adequadas para gerenciar a prestação dos serviços, com linha telefônica, em virtude da necessidade do IGESDF manter contato com o preposto indicado pela empresa.

XVI - A **CONTRATADA** deve fornecer, no ato da assinatura contratual, endereço da matriz, filial ou escritório no Distrito Federal, bem como número de telefone comercial fixo, móvel, fax, também no Distrito Federal, e endereço eletrônico (e-mail), devendo atualizar todos os dados sempre que houver alterações.

XVII - Dar cumprimento a todas as determinações e especificações estabelecidas neste instrumento e assumir inteira responsabilidade pela execução dos serviços contratados, nos termos da legislação vigente.

XVIII - Manter arquivo com toda a documentação relativa à execução do contrato.

XIX - A **contratada se obriga a manter o fornecimento de bens e serviços**, nas mesmas condições estabelecidas no Elemento Técnico e no preço pactuado, **caso exista risco a vida dos pacientes**, **por, no mínimo, 90 dias ou até a celebração de contrato com outro fornecedor.**

8. **DAS OBRIGAÇÕES E RESPONSABILIDADES DO CONTRATANTE**

CLÁUSULA OITAVA - O CONTRATANTE se obriga a:

I - Indicar os locais e horários em que deverá ser entregue o produto.

II - Autorizar o pessoal da **CONTRATADA**, acesso ao local da entrega desde que observadas às normas de segurança do IGESDF.

III - Rejeitar no todo ou em parte, o produto entregue em desacordo com as obrigações assumidas pelo fornecedor.

IV - Garantir o contraditório e ampla defesa.

V - Efetuar o pagamento à Contratada nas condições estabelecidas neste Instrumento Contratual.

VI - Acompanhar e fiscalizar a execução do instrumento contratual, bem como atestar na nota fiscal/fatura a efetiva execução do objeto.

VII - Notificar a **Contratad**a, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na execução da entrega deste Contrato, para que sejam adotadas as medidas corretivas necessárias.

9. **DO PAGAMENTO**

CLÁUSULA NONA - Para efeito de pagamento, a **CONTRATADA** deverá observar as disposições do Edital e seus Anexos

PARÁGRAFO PRIMEIRO – Os pagamentos serão efetuados mediante apresentação de nota fiscal, conforme segue:

I - Nota Fiscal;

II - A empresa deverá emitir uma nota fiscal específica para cada pedido e respectiva entrega efetuada, ou pagamento na forma do cronograma desembolso, na forma abaixo:

NOME: INSTITUTO DE GESTÃO ESTRATÉGICA DE SAÚDE DO DISTRITO FEDERAL - IGESDF.

CNPJ: 28.481.233/0001-72.

ENDEREÇO: SMHS, ÁREA ESPECIAL, QUADRA 101, BLOCO A, CEP: 70.335-900 - BRASÍLIA/DF.

III - Na nota fiscal ou fatura deverá constar obrigatoriamente o número de referência deste instrumento, o nome do Banco, e o número da Agência e da Conta Corrente da **CONTRATADA**, para realização do pagamento obrigatoriamente por meio de depósito/transferência bancária, a critério do **CONTRATANTE**.

IV - Caso as notas fiscais ou faturas tenham sido emitidas com incorreções ou em desacordo com a legislação vigente, serão devolvidas e o prazo para pagamento passará a ser contado a partir da reapresentação.

V - Caso algum item constante na nota fiscal seja impugnado, o **CONTRATANTE** liberará a parte não sujeita à contestação, retendo o restante do pagamento até que seja sanado o problema.

VI - Deverá conter o número do instrumento contratual de referência.

PARÁGRAFO SEGUNDO – O pagamento será realizado **em até 30 (trinta) dias corridos**, por meio de depósito/transferência bancária em conta corrente, contados do recebimento da Nota Fiscal devidamente atestada pela unidade responsável.

PARÁGRAFO TERCEIRO – Em razão de o pagamento ser realizado mediante depósito/transferência bancária, a **CONTRATADA** não deverá fazer a emissão de boleto bancário, sob pena de haver cobrança indevida.

PARÁGRAFO QUARTO – Havendo necessidade de providências complementares a serem realizadas por parte da **CONTRATADA**, o decurso do prazo de pagamento será interrompido, reiniciando sua contagem a partir da data em que estas forem cumpridas, hipótese em que não será devida atualização financeira.

PARÁGRAFO QUINTO – O atraso do pagamento, pelo prazo de até 30 dias, após o determinado no Parágrafo Segundo, não implica no direito da suspensão da empresa **CONTRATADA** ao cumprimento de suas obrigações, até que seja normalizada a situação.

PARÁGRAFO SEXTO – Os pagamentos ficam condicionados à manifestação de conformidade pelo Fiscal do contrato, observando as regularidades exigidas no instrumento convocatório original.

10. **DO REAJUSTE E DO REEQUILÍBRIO FINANCEIRO**

CLÁUSULA DÉCIMA - O presente **CONTRATO** somente poderá ser reajustado, por ocasião de prorrogação do mesmo, respeitando os valores de mercado adequados ao caso, que se apresentam nos meios de pesquisa dos quais o **CONTRATANTE** se utilize.

PARÁGRAFO PRIMEIRO – Em nenhuma hipótese, os valores cotados em moeda estrangeira, especificamente Dólares Americanos, serão considerados o da entrega do bem, tomando-se como marco inicial, o valor no Contrato e/ou Termo Aditivo pactuado à sua época.

PARÁGRAFO SEGUNDO – O presente **CONTRATO** poderá ser revisado ou reequilibrado, por meio de Termo Aditivo, conforme disposições contidas no art. 38, parágrafo primeiro do Regulamento Próprio de Compras e Contratações do IGESDF, inclusive levando em consideração o prazo de vigência estabelecido na Cláusula Quarta deste Instrumento.

PARÁGRAFO TERCEIRO – No reajuste do Contrato, objetivando a recomposição do valor monetário do contrato, utilizar-se-á o índice IGPM ou o índice IPCA, optando pelo mais vantajoso ao IGESDF no momento da celebração do termo aditivo, em observância ao Regulamento Próprio de Compras e Contratações do IGESDF.

I - Excepcionalmente e em casos específicos, não serão aplicados os índices do **Parágrafo Terceiro** cabendo aplicação do valor em moeda estrangeira conforme **Parágrafo Primeiro,** vedada sua cumulação com os índices supracitados.

11. **DA ALTERAÇÃO CONTRATUAL**

CLÁUSULA DÉCIMA PRIMEIRA - O presente **CONTRATO** poderá ser alterado, por meio de Termo Aditivo, nos casos previstos nos arts. 37 do Regulamento Próprio de Compras e Contratações do IGESDF, consoante a Resolução CA-IGESDF Nº 04/2022, desde que haja interesse do **CONTRATANTE**, com a apresentação das devidas justificativas, e não haja modificação de seu objeto, conforme legislação vigente

PARÁGRAFO ÚNICO – A **CONTRATADA**, na forma prevista no art. 38 do Regulamento Próprio de Compras e Contratações do IGESDF, fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nas obras, serviços ou compras, até 50% (cinquenta por cento) do valor inicial atualizado do contrato.

12. DAS PENALIDADES

CLÁUSULA DÉCIMA SEGUNDA - Nos termos do artigo 49, 50, 51, 52 e 53 do Regulamento Próprio de Compras e Contratações do IGESDF, sem prejuízo da rescisão unilateral do contrato e da responsabilidade civil e penal cabíveis a **CONTRATADA**, o descumprimento do contrato poderá acarretar as seguintes penalidades, precedido do devido processo legal, ampla defesa e o contraditório:

I – advertência;

II – Multa nos seguintes percentuais:

a) 0,1% (um décimo por cento) ao dia, sobre o valor total da aquisição, até o limite de 30 (trinta) dias, no caso de atraso injustificado;

b) 10% (dez por cento), cumulativamente, sobre o valor total da aquisição, após 30 (trinta) dias de atraso injustificado;

c) O atraso injustificado de entrega dos itens superior a 30 (trinta) dias corridos será considerado como inexecução total do objeto, devendo o instrumento respectivo ser rescindido, salvo razões de interesse público devidamente explicitadas no ato da autoridade competente do IGESDF;

d) 10% sobre o valor da parcela em caso de inexecução parcial ou infração contratual;

e) 20% sobre o valor global do contrato, em caso de inexecução total ou quando ficar caracterizada a recusa do cumprimento das obrigações.

f) Multa de 5% (cinco por cento) sobre o valor total da contratação, quando for constatado o descumprimento de qualquer obrigação prevista no **EDITAL DO CHAMAMENTO N.º 034/2024 (147209089)** e no **ELEMENTO TÉCNICO N.º 5/2024 (135966678**), ressalvadas aquelas obrigações para as quais tenham sido fixadas penalidades específicas.

g) Multa indenizatória, a título de perdas e danos, na hipótese da **CONTRATADA** ensejar a rescisão das obrigações assumidas e/ou sua conduta implicar em gastos ao **CONTRATANTE** superiores aos registrados.

III – suspensão de participação em Seleção de Fornecedores e impedimento de contratar com o IGESDF, por prazo não superior a 2 (dois) anos;

IV – solicitação aos órgãos governamentais competentes da caracterização de inidoneidade;

V – perda da caução em dinheiro ou execução das demais garantias oferecidas, sem prejuízo de outras penalidades no instrumento convocatório.

PARÁGRAFO PRIMEIRO - Caso haja uma situação que se enquadre em dois ou mais casos de multa, o IGESDF poderá utilizar a multa mais elevada.

PARÁGRAFO SEGUNDO - O atraso superior a **30 (trinta) dias corridos** autoriza o **CONTRATANTE**, a seu critério, a não aceitar o fornecimento dos itens solicitados, de forma a configurar inexecução total da obrigação assumida pela **CONTRATADA** e, podendo ainda, promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas.

PARÁGRAFO TERCEIRO - A multa eventualmente imposta à **CONTRATADA** será automaticamente descontada da fatura a que fizer jus.

PARÁGRAFO QUARTO - Caso a **CONTRATADA** não tenha nenhum valor a receber do IGESDF, ser-lhe-á concedido o prazo de 05 (cinco) dias úteis contados de sua notificação para efetuar o pagamento da multa.

PARÁGRAFO QUINTO - Não ocorrendo o pagamento no prazo previsto, proceder-se-á a cobrança judicial da mesma.

PARÁGRAFO SEXTO - As sanções previstas no contrato poderão ser aplicadas cumulativamente.

PARÁGRAFO SÉTIMO - Em caso de risco iminente, o IGESDF poderá motivadamente adotar providências acauteladoras, sem prévia manifestação da **CONTRATADA**.

PARÁGRAFO OITAVO - A recusa injustificada em assinar o contrato, o instrumento de registro de preços ou instrumento equivalente, dentro do prazo fixado, caracterizará o descumprimento total da obrigação assumida e poderá acarretar ao participante do Chamamento as seguintes penalidades:

I - Perda da contratação, sem prejuízo à indenização ao IGESDF por danos causados pela recusa;

II - Suspensão do direito de participar de Seleção de Fornecedores ou contratar com o IGESDF, por prazo não superior a 2 (dois) anos.

PARÁGRAFO NONO – A dosimetria da penalidade a ser aplicada, deverá seguir rito próprio do IGESDF, levando-se em consideração agravamento da penalidade, considerando o impacto econômico, social e institucional da **CONTRATANTE**.

13. DA RESCISÃO

CLÁUSULA DÉCIMA TERCEIRA - Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurados o contraditório e a ampla defesa.

PARÁGRAFO PRIMEIRO - **UNILATERALMENTE**:

I - Em caso de inadimplemento total ou parcial das obrigações contratuais assumidas, sem prejuízo de outras penalidades previstas no **EDITAL DO CHAMAMENTO N.º 034/2024 (147209089)**, neste **CONTRATO** e no Regulamento Próprio de Compras e Contratações do IGESDF.

PARÁGRAFO SEGUNDO - **AMIGAVELMENTE**, por mútuo acordo entre as partes envolvidas.

PARÁGRAFO TERCEIRO - Caso exista risco à vida dos pacientes, a **CONTRATADA** se obriga a manter o fornecimento de bens e serviços por, no mínimo, 90 (noventa) dias, ou até a celebração de contrato com outro fornecedor, conforme o disposto no Regulamento Próprio de Compras e Contratações do IGESDF, consoante a Resolução CA-IGESDF Nº 04/2022.

I - O descumprimento do **Parágrafo Terceiro** confere ao **CONTRATANTE** hipótese de aquisição emergencial com outro fornecedor, podendo cobrar judicial ou extrajudicialmente a diferença de valores entre o pactuado no presente instrumento e o que efetivamente foi adquirido emergencialmente.

14. DA FISCALIZAÇÃO

CLÁUSULA DÉCIMA QUARTA - Fiscalização e o atesto da Nota Fiscal serão realizados pelo fiscal do contrato ou colaborador designado.

PARÁGRAFO PRIMEIRO – A fiscalização não exclui, nem reduz a responsabilidade da **CONTRATADA**, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade do **CONTRATANTE** ou de seus agentes prepostos.

PARÁGRAFO SEGUNDO – A fiscalização do instrumento contratual será realizada por colaborador designado, quanto ao objeto contratado, sendo responsável pelo recebimento e controle.

PARÁGRAFO TERCEIRO - A execução do Contrato será realizada conforme análise de histórico de consumo fornecido pelo sistema de gestão de estoque.

PARÁGRAFO QUARTO – Na ausência de histórico de consumo, as execuções serão realizadas conforme dados de capacidade do serviço, fornecido pela área técnica.

PARÁGRAFO QUINTO – Todas as atividades realizadas na execução dos serviços deverão ser supervisionadas por mecanismos de controle de qualidade incidentes em três momentos, a saber:

a) Preliminarmente, ao início da execução;

b) Durante a execução; e

c) Ao término da execução.

15. DA PUBLICAÇÃO E DO REGISTRO

CLÁUSULA DÉCIMA QUINTA - A **CONTRATANTE** providenciará a publicação do extrato/resumo deste instrumento no sítio eletrônico do IGESDF na rede mundial de computadores, em observância ao Princípio da Publicidade previsto no inciso I do art. 2º do Regulamento Próprio de Compras e Contratações do IGESDF, consoante a Resolução CA-IGESDF Nº 04/2022.

16. DA FRAUDE E CORRUPÇÃO

CLÁUSULA DÉCIMA SEXTA - Os **CONTRATOS** firmados com o IGESDF pautam-se pela ética e transparência, evitando-se condutas que possam suscitar conflitos de interesses.

PARÁGRAFO PRIMEIRO – O IGESDF exige que as **CONTRATADAS** observem o mais alto padrão de ética durante toda a execução dos instrumentos contratuais, nos termos da legislação vigente.

PARÁGRAFO SEGUNDO – A **CONTRATADA** declara conhecer o inteiro teor da Lei Federal nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e do Decreto Distrital nº 37.296, de 29 de abril de 2016 que disciplina, no âmbito da Administração Pública do Distrito Federal, a aplicação da Lei nº 12.846/2013, e compromete-se a não praticar atos lesivos, assim como em face do IGESDF.

PARÁGRAFO TERCEIRO – A **CONTRATADA** se obriga, sob as penalidades previstas neste **CONTRATO** e na legislação aplicável, ao estrito cumprimento da legislação cabível, incluindo a legislação brasileira anticorrupção, bem como as normas e exigências previstas nas Políticas internas da **CONTRATANTE**, incluindo, naquilo que couber, o Código de Ética e Conduta do IGESDF.

PARÁGRAFO QUARTO – A violação comprovada das obrigações previstas relacionadas à fraude e corrupção constitui causa para a rescisão unilateral deste **CONTRATO**, sem quaisquer ônus ou penalidade para a parte idônea, sem prejuízo da cobrança de perdas e danos a quem lhe der causa.

17. **DO SIGILO E DA CONFIDENCIALIDADE**

CLÁUSULA DÉCIMA SÉTIMA - A **CONTRATADA** compromete-se a guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do presente **CONTRATO**, observando que os termos e condições contidos neste instrumento, o escopo de execução dos trabalhos e todos os documentos que o instruem, assim como aqueles que vierem a instruí-lo e que venham a ser trocados entre as Partes ou por elas produzidos na vigência deste **CONTRATO**, são de caráter estritamente confidencial e não poderão ser revelados, divulgados ou cedidos a terceiros, integral ou parcialmente.

18. **DA RESCISÃO OU NÃO RENOVAÇÃO**

CLÁUSULA DÉCIMA OITAVA - A **CONTRATADA** declara neste ato que tem ciência de que o IGESDF executa sua atividade mediante Contrato de Gestão firmado com ente público e que sua rescisão ou não renovação importará em rescisão automática do instrumento firmado para as contratações e aquisições, sem que caiba, a qualquer das partes, direito a multa, indenização, retenção, compensação, perdas e danos então decorrentes do mencionado encerramento contratual, sem qualquer ônus para as partes.

PARÁGRAFO ÚNICO - Caso seja de interesse do poder público, os contratos vigentes no momento da rescisão ou não renovação do contrato de gestão poderão ser sub-rogados em seu favor.

19. **DO APOSTILAMENTO**

CLÁUSULA DÉCIMA NONA - A **CONTRATANTE** se reserva ao direito de proceder com apostilamento nos autos do processo do qual se verifica inserto este instrumento contratual, para fins de correção de erro material, equívocos e demais anotações pertinentes a boa execução e esclarecimentos do presente contrato.

20. **DOS CASOS OMISSOS**

CLÁUSULA VIGÉSIMA – Os casos omissos serão resolvidos pela Diretoria Executiva do Instituto de Gestão Estratégica de Saúde do Distrito Federal, com prévia comunicação formal ao **CONTRATADO**.

21. **DOS FUNDAMENTOS**

CLÁUSULA VIGÉSIMA PRIMEIRA - O presente **Contrato** fundamenta-se:

- Nos autos do processo SEI nº **04016-00030943/2024-24, EDITAL DO CHAMAMENTO N.º 034/2024 (147209089)** e no **ELEMENTO TÉCNICO N.º 5/2024 (135966678).**
- Nas disposições do Regulamento Próprio de Compras e Contratações do IGESDF vigente e
- Nos princípios do Direito Público e supletivamente, nos princípios da Teoria Geral dos Contratos e nas disposições do Direito Privado.

22. **DO FORO**

CLÁUSULA VIGÉSIMA SEGUNDA - Fica eleito o foro da Circunscrição Especial Judiciária de Brasília/DF, para dirimir todas e quaisquer dúvidas oriundas da execução deste Instrumento, renunciando a qualquer outro por mais privilegiado que seja.

E, para firmeza e validade do que foi pactuado, lavrou-se o presente instrumento, o qual, após de lido, será assinado pelos representantes das partes.

CONTRATANTE:

CLEBER MONTEIRO FERNANDES Diretor Presidente - Substituto
Instituto de Gestão Estratégica de Saúde do Distrito Federal - IGESDF

RUBENS DE OLIVEIRA PIMENTEL JÚNIOR Diretor de Administração e Logística
Instituto de Gestão Estratégica de Saúde do Distrito Federal - IGESDF

CONTRATADA:

AISLAN CARLOS MENDONÇA Representante Legal
VOGEL SOLUCOES EM TELECOMUNICACOES E INFORMATICA S.A.

MÁRCIO DE JESUS DA SILVA Representante Legal
VOGEL SOLUCOES EM TELECOMUNICACOES E INFORMATICA S.A.

Documento assinado eletronicamente por **Aislan Mendonça**, **Usuário Externo**, em 30/10/2024, às 16:50, 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 **Márcio de Jesus da Silva**, **Usuário Externo**, em 30/10/2024, às 18:05, 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 **RUBENS DE OLIVEIRA PIMENTEL JUNIOR - Matr.0001587-0**, **Diretor(a) Executivo(a)**, em 30/10/2024, às 18:53, 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 **CLEBER MONTEIRO FERNANDES - Matr. 0001938-1**, **Diretor(a) Vice-Presidente**, em 31/10/2024, às 10:16, 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= **154830875** código CRC= **C50CBC1A**.

Criado por 00018669, versão 3 por 00018669 em 30/10/2024 14:29:30.