

# Estudo Técnico Preliminar 66/2023

## 1. Informações Básicas

Número do processo: 00190.102879/2023-38

## 2. Descrição da necessidade

### Cenário Atual

A Controladoria-Geral da União (CGU) possui 28 datacenters on-premises, um em cada capital do Brasil, além do seu principal datacenter físico localizado na Sede/DF (Serpro). O contrato CGU nº 05/2019 provê a interconectividade de rede e segurança de perímetro para esta infraestrutura on-premises entre todos estes datacenters. Atualmente este contrato está em seu 3º aditivo, sem possibilidade de nova renovação e a sua vigência final é 20/05/2024. O serviço contratado fornece a solução com 28 firewalls físicos (dois Fortinet 1200D com Threat Protection de 4Gbps para alta disponibilidade no datacenter da Sede/DF e um Fortinet 81E/101E com Threat Protection de 250Mbps para cada regional), 1 *appliance* de gerência e 1 *appliance* de análise de logs. Este contrato também provê o serviço de rede “Wide Area Network” (WAN) e “Multiprotocol Label Switching” (MPLS).

A rede WAN tem a finalidade de interligar os datacenters das regionais com os da Sede, além de conectar cada uma das unidades individualmente à Internet. Nas regionais, há um link MPLS que se conecta à Sede e um link de saída para Internet que passam pela análise de segurança do firewall. Há também uma solução de alta disponibilidade, para prover redundância entre estes sites, por meio de balanceamento “Border Gateway Protocol” (BGP). Assim, em caso de queda do link de Internet da regional, o tráfego é direcionado pelo link MPLS até Brasília, de onde segue para a Internet. Do mesmo modo, caso o link MPLS da regional caia, o tráfego com origem-destino à Brasília é encaminhado por meio de um túnel “IPsec” estabelecido pelo link de Internet.

Com a finalidade de ampliar as capacidades com alta disponibilidade e a redundância destes links, é escopo do processo de contratação 00190.103049/2023-28, Plano de trabalho #1066860, contratar 2 (dois) links de Internet, em vez de 1 (um) link MPLS com 1 (um) link de Internet. Para isso, será necessário a utilização de uma solução de “Software Defined WAN” (SD-WAN), cujo principal objetivo é realizar o balanceamento e redundância entre os 2 (dois) links Internet.

Além da ampliação das capacidades dos links, nos datacenters da Sede e Regionais com o intenso uso de aplicações de vídeo e demais tráfego de sistemas e serviços, a equipe de redes tem tratado cenários de picos e congestionamento de tráfego nas interfaces dos equipamentos de rede. Por isso, estão sendo iniciados projetos de expansão da capacidade de tráfego através do incremento das interfaces de todos os equipamentos redes destes ambientes.

Ademais, a solução de firewall provida pelo contrato nº 05/2019 também era utilizada como forma de acesso remoto à rede interna da Organização por meio de “Virtual Private Network” (VPN), que, até meados de 2020, era a única forma de acesso a sistemas e serviços internos da rede não publicados externamente. Porém, esta solução de VPN ainda não utilizava a tecnologia de segundo fator de autenticação (2FA) e o seu uso foi suprimido devido aos riscos de segurança. Para substituir a solução de VPN, foi implantada a solução de “Virtual Desktops Infrastructure” (VDI), contratos nº 34/2020 e nº 35/2020, que trouxe novas funcionalidades de uso, além da maior segurança através da sua autenticação com 2FA.

No final de 2022, a CGU assinou um novo contrato de serviço operação terceirizada de 3º Nível, processo SUPER nº 00190.104832/2020-66, que prevê uma distribuição de suporte ininterrupto de 24x7 remoto e presencial em Brasília, com diversas torres de atuação como: Rede e Conectividade e Segurança de TIC, que são responsáveis pela operação dos serviços de redes e segurança. Desta forma, uma solução de VPN com 2FA, faz-se necessária para alguns casos de uso por servidores internos e para uma forma de acesso administrativos remoto alternativo, principalmente em casos de incidentes da infraestrutura do VDI.

Estas novas equipes de serviço terceirizadas são responsáveis também pela gestão e operação 24x7 dos equipamentos físicos de conectividade e segurança de redes (*Firewall/SD-WAN*) das Regionais, de forma remota, que através de um servidor físico virtualizado oferece os serviços locais de *File/Print Server, Backup, Active Directory, DHCP, Wifi* etc. A tendência de utilização de serviços locais das regionais tem caído com o passar do tempo, no passado havia dois hosts físicos virtualizados para cada regional com dois Active Directorys, File Servers redundantes e todos estes serviços e hardwares foram reduzidos para uma instância apenas. Hoje, existem estudos em andamento pela equipe de Engenharia da Coordenação de Infraestrutura de TI (CGTEC) para migração dos serviços de FileServer para nuvem, que é um dos principais consumidores de recursos deste hospedeiro. Com isso, a tendência é a redução da capacidade do hospedeiro a cada nova contratação.

Adicionalmente à infraestrutura e interconexões tradicionais entre datacenters físicos on-premises, a CGU iniciou a sua jornada para nuvem, por meio do contrato CGU nº 21/2019 com a empresa Claro. Esse contrato fornece os serviços de nuvem da *Amazon Web Services (AWS)* que já abriga os principais sistemas externos críticos da Organização, como FalaBr, Portal da Transparência, SISCOR, e-PAD, SeCI etc. Além desses serviços de nuvem da AWS, a CGU também utiliza os serviços de nuvem da Microsoft do Office 365, por meio do contrato nº 16/2020, para soluções de escritório digital, como correio eletrônico (*Outlook*), armazenamento de arquivos (*Sharepoint*), comunicações (*Teams*) etc.

No ambiente de nuvem na AWS, a proteção de perímetro utiliza basicamente as tecnologias de “*Web Application Firewall*” (WAF) e “*Security Groups*” (SGs), pois o contrato nº 21/2019 não prevê a utilização de serviços adicionais de segurança de perímetro, como *AWS Network Firewall*. Porém, mesmo este serviço oferecido pelo provedor de nuvem da AWS ainda não oferece diversas características de segurança

que temos implementados no ambiente on-premises, como varredura antimalware, ips, ids e demais tecnologias de prevenção de ataques computacionais de próxima geração. Ademais, a utilização de múltiplas contas, como a CGU utiliza hoje na AWS, traz uma complexidade ainda maior na padronização e garantia de compliance de segurança dos diversos ambientes de nuvem como um todo.

Recentemente, a CGU assinou o contrato 16/2023 de um novo serviço de nuvem, projeto do Plano de Trabalho #1306037, de forma a substituir e ampliar o atual serviço prestado pelo contrato nº 21/2019. Esta contratação marcará o início de novas fases de migração da infraestrutura de sistemas e serviços que ainda residem on-premises na rede interna da CGU, como Super, E-aud, ITSM etc. Adicionalmente, também disponibilizará um maior número de serviços na AWS, além da utilização de serviços multicloud, como serviços de nuvem Azure da Microsoft e *Google Cloud Plataform* (GCP). Este projeto também prevê a contratação de um novo link de alta performance privado/dedicado para comunicação do datacenter da CGU com a nuvem da AWS.

Forma-se então um cenário híbrido on-premises e *multicloud* (AWS, Azure e GCP) de múltiplas contas, que emerge como um novo desafio para segurança de perímetro e gerenciamento de vulnerabilidades, com a utilização de tecnologias diversas, providas por fabricantes distintos, com níveis de proteções diferentes, dependência das limitações das soluções de segurança disponíveis em cada ambiente, e a garantia de compliance nas múltiplas contas de ambientes de nuvens distintos. Nesse tipo de ambiente, as arquiteturas têm se tornado cada vez mais complexas e, por consequência, a necessidade de mão de obra altamente especializada é cada vez maior.

### 3. Área requisitante

Área Requisitante	Responsável
Coordenação-Geral de Infraestrutura Tecnológica (CGTEC /DTI/SE/CGU)	Thiago Guedes Paysan

### 4. Necessidades de Negócio

Esta contratação tem por objetivo substituir as atuais soluções de segurança e interconectividade de redes on-premises, descritas na seção anterior (*firewall* e *SD-WAN*), promovendo a continuidade de serviço essencial para segurança de perímetro da infraestrutura de TI que sustenta todos os sistemas e dados desta Organização, como os sistemas críticos Super, E-aud, e-PAD, SeCI etc.

Além de preservar a continuidade do serviço essencial, este projeto de aquisição também tem por finalidade contratar solução on-premises que seja compatível com tecnologias de nuvem AWS, Microsoft Azure e GCP, de forma a nivelar e centralizar os mecanismos de detecção e prevenção de ameaças de segurança cibernética em toda

a nova infraestrutura híbrida, “on-premises” e “multicloud”, de modo a garantir a modernização da infraestrutura tecnológica da CGU e adequação às constantes evoluções na área de tecnologia da informação.

Funcionalidades básicas de *Web Application Firewall (WAF)* para o ambiente on-premises, foram contratadas pela CGU através do contrato Nº 48/2021. Desta forma, essa funcionalidade não será exigida neste projeto.

Desta forma, este projeto de aquisição deverá encontrar solução que obedeçam aos seguintes requisitos de negócio:

- Solução unificada que promova garantia do mesmo nível de compliance de segurança em toda a infraestrutura híbrida (on-premises e nuvem), fornecendo os mesmos mecanismos de detecção e prevenção de ameaça, com solução de VPN moderna com autenticação de, no mínimo, dois fatores (2FA) para acessos administrativos;
- Serviço de implantação com a migração da solução on-premises atual;
- Repasse de conhecimento para a equipe técnica da CGU;
- Serviço de gerenciamento centralizado;
- Serviço de armazenamento e gerenciamento de logs;
- Horas de consultoria com engenheiro especializado do fabricante, no intuito de sempre ter um apoio especializado que possa orientar, planejar e implantar as melhores recomendações em segurança no desenvolvimento de novas arquiteturas com a solução on-premises ou em nuvem;
- Solução com suporte técnico 24x7 com garantia e direito de atualização do produto pelo fabricante durante a vigência do contrato;

A solução deverá fornecer ferramenta de *Firewall* com *SD-WAN* e ser compatível com o modelo atual da Operação Terceirizada 24x7 contratada pela CGU, conforme mencionado no item Cenário Atual. Dessa forma, deverá possibilitar conectividade para acesso remoto que possibilite atuação em caso de incidentes fora do horário comercial aos serviços *on-premises* disponíveis.

Nas Regionais, os serviços (*fileserver, active directory, dhcp etc.*) são dependentes da infraestrutura de virtualização local (servidor Hyper-V). Para isso, a solução deverá ser independente deste componente virtual. Há a tendência de redução de recursos físicos para implantação de novos serviços neste tipo de ambiente. A última contratação de equipamentos Servidores do Tipo Rack para regionais, resultante do Plano de Trabalho #840918, não levou em consideração utilização deste hardware para suportar appliances de firewall virtuais. Desta forma, os seguintes requisitos de negócio deverão ser observados:

- segurança de perímetro para todos os datacenters “on-premises” (regionais e sede) compatível com solução de interconectividade para garantir a alta disponibilidade dos links de Internet (Firewall + SD Wan); e
- independência do componente de virtualização das regionais.

## 5. Necessidades Tecnológicas

Diante dos requisitos de negócios da seção anterior, faz-se necessário maior aprofundamento nas tecnologias envolvidas para a completa compatibilidade com as peculiaridades dos nossos ambientes de datacenter on-premises e nuvem, além da promoção da modernização tecnológica da infraestrutura da CGU. Para isso, apresentamos o conceito do Gartner para solução moderna de *firewall: Next Generation Firewall (NGFW)*.

*“Next-generation firewalls (NGFWs) are deep-packet inspection firewalls that move beyond port /protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall. An NGFW should not be confused with a stand-alone network intrusion prevention system (IPS), which includes a commodity or nonenterprise firewall, or a firewall and IPS in the same appliance that are not closely integrated.”*

<https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws>

Neste contexto, entendem-se como presentes na solução de NGFW todas as características abaixo:

- possuir as seguintes *características de controle e fluxo de dados*: mecanismos de *Quality of Service (QoS)*, como deduplicação, compressão, cache, marcação de pacotes e “*Traffic Shaping*” para classificação, segmentação, otimização, aceleração, priorização do tráfego de rede;
- possibilitar a criação de túneis criptografados via IPsec (entre sites) ou SSL;
- possuir as seguintes *características de segurança*: *inspeção de tráfego em camada nível 7*; *Intrusion Detection System (IDS)*; *Intrusion Prevention System (IPS)*; *detecção antimalware avançada (Sandbox)*, *Web Filtering*;
- possuir política de roteamento com protocolo Border Gateway Protocol (*BGP*).

Ademais, para compatibilidade com a ampliação da capacidade dos equipamentos de rede citadas na seção do cenário atual, é um requisito tecnológico que os NGFWs tenham interfaces de rede de 25Gbase-sr para Sede e interfaces de 10GBase-sr para as Regionais.

Desta forma, de modo a promover a compatibilidade com o ambiente atual da CGU, as seguintes necessidades tecnológicas são necessárias para este projeto:

- solução deverá ser do tipo NGFW, contendo IPS, IDS, Antimalware (com Sandbox), Inspeção de tráfego camada de aplicação, Web Filtering;
- VPN com autenticação 2FA integrada com aplicativo móvel;
- alta disponibilidade;
- módulo centralizado para gerência, com console única para todo ambiente;
- módulo para análise e armazenamento de logs gerados pela solução, com funcionalidade de envio de logs para repositório central de logs, via protocolo syslog;
- formas de recuperação de backup das configurações em caso de desastre; e
- NGFWs devem possuir interfaces de rede de 25Gbase-sr para Sede e interfaces de 10GBase-sr para as Regionais.

## 6. Demais requisitos necessários e suficientes à escolha da solução de TIC

- Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade - 2022.xlsx (da DTI); e
- Guia do Ministério Economia.

## 7. Estimativa da demanda - quantidade de bens e serviços

### Dimensionamentos dos tamanhos do NFGFW Físicos

O dimensionamento dos equipamentos on-premises está fortemente relacionado ao projeto de contratação da rede WAN, conforme apresentado no item 2 – Cenário Atual, que está em andamento na CGU. Isso se deve ao fato de que um dos fatores mais importantes no dimensionamento dos firewalls é a capacidade de uso (*Throughput*) dos links internet que deverão ser roteados e analisados pelos equipamentos de firewall da Sede e Regionais.

A tabela abaixo apresenta as defasadas capacidades atuais dos links de internet e rede MPLS atuais da CGU.

	FAIXA 1 (Mbps)	FAIXA 2 (Mbps)	FAIXA 3 (Mbps)	FAIXA 4 (Mbps)	FAIXA 5 (Mbps)
MPLS - SEDE	50	100	150	200	250
MPLS - REGIONAL TIPO 1	4	6	8	10	12
MPLS - REGIONAL TIPO 2	6	8	10	12	14
MPLS - REGIONAL TIPO 3	8	10	12	14	16
INTERNET - SEDE	150	200	250	300	350
INTERNET - REGIONAL TIPO 1	6	10	14	18	22
INTERNET - REGIONAL TIPO 2	8	12	16	20	24
INTERNET - REGIONAL TIPO 3	10	14	18	22	26

Tabela 2 – Atuais faixas de velocidade dos links da CGU

Para estas capacidades, considerando os demais tráfegos de rede entre Infovia e redes internas, os atuais equipamentos de Firewall da Sede - Fortinet 1200D com Threat Protection de 4Gbps, e Regionais - Fortinet 81E/101E com Threat Protection de 250Mbps, têm atendido a demanda atual no limite de suas capacidades, por vezes, em algumas unidades da federação, chegando a picos de 100% de uso de processamento e memória.

O novo projeto da rede WAN mapeou a nova expectativa de uso para os próximos 5 anos até a FAIXA 3 da tabela abaixo.

	FAIXA 1 (Mbps)	FAIXA 2 (Mbps)	FAIXA 3 (Mbps)	FAIXA 4 (Mbps)	FAIXA 5 (Mbps)
SEDE	1000	2000	3000	4000	5000
REGIONAL TIPO 1	300	600	900	1200	1500
REGIONAL TIPO 2	500	800	1100	1400	1700

Figura 1: Faixas do contrato da rede WAN

A partir do aumento da capacidade de *throughput* das regionais, estima-se que os próximos Firewalls das regionais deverão, nos próximos 5 anos, prever um *throughput* (com *Threat Protection*) de 1.8 e 2.2 Gbps para as regionais Tipo 1 e Tipo 2, respectivamente. Esses valores consideram a substituição da rede MPLS por mais um link de internet, ou seja, serão dois links internet para cada regional, devendo então multiplicar por 2 a capacidade da FAIXA 3.

Para a Sede, a capacidade atual também será incrementada para os próximos 5 anos, pois é necessário acomodar: os aumentos das capacidades dos links internet do projeto da rede WAN; suportar a previsão de aumento do uso da Infovia (IX + OpenCDN); e comportar o novo canal privado/dedicado de comunicação entre o datacenter da CGU e as nuvens da AWS e Azure (Plano de Trabalho #1306037), que prevê utilização de até 2 links na faixa de 1Gbps, conforme tabela abaixo.

Item (A)	Velocidade do enlace físico/lógico (circuito virtual) (B)	Quantidade mensal inicial de USCN's por enlace físico/lógico (circuito virtual) (C)	Fator percentual de desconto em função da velocidade (D)	Total mensal de USCN's por enlace físico/lógico (circuito virtual) (E) = (C * (1 - D))	Quantidade de enlaces físicos/lógicos (circuitos virtuais) (F)
1	200 Mbps	200	0,00%	200	4
2	500 Mbps	500	35,00%	325	
3	1 Gbps	1000	55,00%	450	
4	2 Gbps	2000	70,00%	600	
5	5 Gbps	5000	80,00%	1000	

Tabela 1 – Total mensal de USCN's a ser considerada para faturamento por enlace físico/lógico em função da velocidade utilizada no circuito.

Desta forma, para o ambiente da Sede/DF, a capacidade do atual *Firewall Fortinet 1200D* com *Threat Protection* de 4Gbps será incrementada em 8Gbps nos próximos 5 anos, conforme a tabela abaixo.

Localidade	Projeto	Capacidade Atual	Incremento da Capacidade Atual	Capacidade Total para 5 anos
Sede/DF	Links WAN	1 Gbps (Faixa 4: MPLS + 2 Links Internet)	5 Gbps	6 Gbps (Faixa 3: 2 links de 3 Gbps)
	Infovia (IX + OpenCDN)	1 Gbps	1.5 Gbps	2.5 Gbps
	Link Privado nuvens	0 Gbps	2 Gbps	2 Gbps
	Tráfego Interno	2 Gbps	0 Gbps	2 Gbps
Total	-	4 Gbps	8 Gbps	12.5 Gbps

## Resumo dos Incrementos de Throuput para Sede/DF para os próximos 5 anos

O modo padrão de uso dos firewalls da CGU é com todas as *features* de segurança habilitadas, mais próxima ao modo de funcionamento com *Threat Protection*, que é a medida de performance calculada na tabela acima. Porém, não há uma forma exata de comparar a medida de *Throughput (Gbps)* entre fabricantes distintos, uma vez que cada um deles especificam condições distintas (% do tráfego de um determinado protocolo, tamanhos de pacotes, modo de análise *flow* ou *proxy* etc.). Desta forma, os fabricantes divulgam, em seus *datasheets*, categorias similares de *Throughput (Gbps)* porém sob condições de análise distintas.

De forma a tentar minimizar estas variações entre fabricantes, foi selecionada uma medida complementar, *Throughput NGFW (Gbps)*, para ser avaliada em conjunto com *Threat Protection*. Como a medida NGFW geralmente não analisa a parte de malware, ela é bem mais performática. Dessa forma, com base em características de produtos líderes de mercado, consultas Gartner e na tentativa de ampliar a concorrência do certame entre fabricantes distintos, foi estimado um valor de 75% de melhoria de performance do NGFW comparado ao *Threat Protection*.

Abaixo, segue a tabela com as capacidades mínimas de *Throughput com Threat Protection* e *Troughput NGFW* estimadas para cada ambiente físico on-premises.

Categoria	Ambiente	Localidade	Forma	Qtde	Capacidade Mínima / Throughput Threat Protection (Gbps)	Capacidade Mínima / Throughput NGFW (Gbps)	Requisitos mínimos para interfaces
T1	On-premises	Sede/DF	Físico	2	12.5	22	2x25Gbps
T2	On-premises	Regionais	Físico	13	2.2	3.9	4x10Gbps
T3	On-premises	Regionais	Físico	13	1.8	3.2	4x10Gbps

Tabela de Quantitativos e Capacidades dos Equipamentos de Firewalls do ambiente on-premises (Sede e Regionais)

### Quantidade de usuários para uso de VPN (client-to-site) para o NGFW Tipo 1

Para o uso da VPN, estima-se algumas necessidades internas para as equipes de Infraestrutura e Desenvolvimento, além da necessidade de uma forma de acesso redundante para o atendimento do contrato de serviço operação terceirizada de 3º

Nível, processo SUPER nº 00190.104832/2020-66, que prevê uma distribuição de suporte ininterrupto de 24x7 para usuários com perfil de administradores para os diversos serviços de TI tanto para o ambiente on-premises quanto em nuvem.

Além desta necessidade, há também alguns acessos de usuários externos para sistemas específicos da rede da CGU. Hoje existem 4 usuários com este tipo de acesso.

A tabela abaixo apresenta um resumo dos quantitativos de contas administrativas estimadas para as torres de Segurança de TIC (8 pessoas), já ativas no ambiente e as novas prevendo o quantitativo previsto por este novo contrato.

Finalidade	Proporção	Quantidade Total de usuários
Equipes de Desenvolvimento	1 por Equipe da CGSIS	6
Equipes de Engenharia de Aplicações/Banco de Dados e Armazenamento e de Infraestrutura	2 por Equipe da COENG /AUT COENG/SEPAM e COENG/SEMAB	6
Equipe de Engenharia e Conectividade	Todos da CGTEC/SERIM	6
Equipe de Segurança da Informação	Todos da CGTEC/DISEG	6
Usuários externos para acesso a Sistemas Internos	4	4
Contrato Operação Terceirizada CGTEC – Torres Segurança de TIC/VDI/Servidores e Virtualização /Redes e Conectividade.	64	64
<b>Total de usuários VPN</b>	<b>CGU</b>	<b>92</b>

### Quantidade de Dispositivos Gerenciados pela Solução de Gerência Centralizada

para o atendimento dos requisitos de negócio deste projeto, na implementação inicial, serão gerenciados, pela Solução de Gerência Centralizada, 28 dispositivos de *firewall* (2 da Sede e 26 das Regionais). Para o próximo ano, há expectativa de novos projetos, nos ambientes de nuvem AWS e Azure, que ampliarão a quantidade de dispositivos gerenciados.

Por compliance de regulamentação do GSI/PR INº 03, a CGU implantou a sua infraestrutura de datacenter em região de nuvem no Brasil e, para garantir uma alta disponibilidade entre as zonas desta região, toda arquitetura de sistemas e serviços críticos é dividida em 3 zonas de disponibilidade (*Availability Zones - AZ*), ou seja, são suportadas falhas de um até dois datacenters do provedor de nuvem. Para garantir a segurança de perímetro mantendo esta arquitetura de alta disponibilidade, são necessários 3 (três) NGFWs virtuais, um para cada AZ de nuvem da AWS e mais 3 (três) NGFWs virtuais, um para cada AZ de nuvem da Azure, bem como 3 (três) para GCP. Desta forma, a quantidade de dispositivos gerenciados nesses ambientes de nuvem poderá chegar a 9.

Dessa forma, considerando os ambientes on-premisse e nuvem, estima-se um total de 37 dispositivos gerenciados.

Dispositivos Gerenciados pela Solução de Gerência centralizada	
Total	37

### Quantidade de uso da Solução de Armazenamento e Gerenciamento de Logs

Existem diversos parâmetros como tempo de retenção (*on-line/off-line*), quantidade de logs por segundo/por dia e tecnologias de compressão/deduplicação que influenciam numa solução de armazenamento de logs. Para o dimensionamento de recursos necessários, foi considerada uma das principais medidas para mensurar a solução de armazenamento e gerenciamento de logs: a quantidade de logs que é gerada em média por dia (GB/dia).

Desta forma, foi aberto um chamado nº 2023092210005939 para Claro, provedora da solução atual, para mensurar a média de uso da solução atual, para os 28 equipamentos da Sede e Regionais Fortigate 1200D/Fortigate81E/Fortigate101E. O valor médio obtido está próximo a 15 GB/dia.

The screenshot shows a log management interface with the following elements:

- Usage Statistics:**
  - Today: 13.14 GB
  - Sep 24, 2023: 7.21 GB
  - Sep 23, 2023: 7.54 GB
  - Sep 22, 2023: 14.22 GB
  - Sep 21, 2023: 14.31 GB
  - Sep 20, 2023: 14.88 GB
  - Sep 19, 2023: 14.18 GB
- Retention Settings:**
  - A retenção está conforme print
  - Keep Logs for Analytics: 120 Days
  - Keep Logs for Archive: 150 Days

Medição do uso atual da Solução de Armazenamento e Gerenciamento de Logs

Conforme apresentado no item sobre dimensionamento dos NGFW físicos, estão em andamento os projetos de ampliação de links nos firewalls on-premises para comportar aumento de serviços. Além disso, projetos futuros que incluirão novos dispositivos nos ambientes de nuvem também demandarão maior capacidade de armazenamento e análise de logs. Com essas demandas, estima-se triplicar a quantidade de logs gerados por dia.

<b>Expectativa do crescimento do uso da Solução de Armazenamento e Gerenciamento de Logs para os próximos 5 anos em Gb/dia</b>	
<b>Demanda Atual</b>	<b>Demanda Atual + projetos de expansão links/nuvem</b>
15 GB/dia	45 GB/dia

#### **Quantidade de horas para consultoria especializada do fabricante**

Para consultoria, planejamento ou implantação de futuros projetos de soluções (on-premises ou em nuvem, Azure e AWS) de novas arquiteturas, funcionalidades no ambiente da CGU, são estimadas 300 horas de utilização sob demanda, conforme quadro abaixo.

<b>Estimativa de Demandas para uso de Horas</b>	
<b>Demanda Futura</b>	<b>Horas</b>
Estudo de Arquitetura e Implantação de solução em nuvem AWS	120h
Estudo de Arquitetura e Implantação de solução em nuvem Microsoft Azure	120h
Revisões e Implantação de novas funcionalidades de segurança no ambiente híbrido (on-premises + nuvem)	60h

Total	300h
-------	------

## Resumo dos Requisitos

Requisitos		
#ID	Nome Curto	Descrição
1	NGFW	<p>A Solução deverá ser composta por solução de Firewall do tipo NGFW com as características abaixo:</p> <ul style="list-style-type: none"> <li>• Possuir as seguintes <i>características de controle e fluxo de dados</i>: mecanismos de <i>Quality of Service (QoS)</i>, como deduplicação, compressão, cache, marcação de pacotes e “<i>traffic shaping</i>” para classificação, segmentação, otimização, aceleração, priorização do tráfego de rede;</li> <li>• Possibilitar a criação de túneis criptografados via IPSec (entre sites) ou SSL;</li> <li>• Possuir as seguintes <i>características de segurança</i>: <i>inspeção de tráfego em camada de aplicação</i>; <i>Intrusion Detection System (IDS)</i>; <i>Intrusion Prevention System (IPS)</i>; <i>deteção antimalware avançada (sandbox)</i>, <i>Web Filtering</i> e <i>técnicas avançadas de detecção de ameaça baseadas em Inteligência Artificial</i>.</li> <li>• possuir política de roteamento com protocolo Border Gateway Protocol (<i>BGP</i>).</li> <li>• VPN com autenticação 2FA integrada com aplicativo móvel, para no mínimo 92 usuários.</li> </ul>
2	Solução Híbrida Unificada com Alta Disponibilidade	<p>Solução unificada que promova garantia do mesmo nível de compliance de segurança em toda a infraestrutura híbrida (on-premises e nuvem), fornecendo os mesmos mecanismos de detecção e prevenção de ameaça. Deverá garantir também:</p> <ul style="list-style-type: none"> <li>• alta disponibilidade na Sede e ambientes de nuvem;</li> <li>• módulo centralizado para gerência, com console única para todo ambiente;</li> <li>• módulo centralizado de armazenamento e análise de logs, com funcionalidade de envio de logs para solução centralizadora de logs via protocolo syslog;</li> <li>• formas de recuperação de backup das configurações em caso de desastre.</li> </ul>

3	Garantia e Suporte 24x7	Solução com suporte técnico 24x7 com garantia e direito de atualização do produto pelo fabricante durante a vigência do contrato.
4	Serviços de Implantação com Repasse de Conhecimento	Deverá conter o Serviço de implantação com a migração da Solução atual com repasse de conhecimento para a equipe técnica da CGU.
5	SD-WAN	A solução deverá prover função de SD-WAN: <ul style="list-style-type: none"> <li>• segurança de perímetro para todos os datacenters “on-premises” (regionais e sede) compatível com solução de interconectividade para garantir a alta disponibilidade dos links de Internet (Firewall + SD Wan).</li> </ul>
6	Independente de camada de Virtualização	A solução deverá ser independente do componente de virtualização das regionais.
7	Horas de Consultoria Especializada	A solução deverá fornecer horas de consultoria com engenheiro especializado do fabricante.

## 8. Levantamento de soluções

### Software Público

Não foram encontradas soluções de software no Portal de Software Público Brasileiro. O acesso ao site <https://www.gov.br/governodigital/pt-br/software-publico> foi feito no dia 16/04/2023 e foram utilizadas as seguintes palavras-chave no campo de busca: “firewall”, “sd-wan” e “ngfw”.

### Soluções Identificadas

**Solução 1:** Contratação de Subscrição com entrega de equipamento de NGFW com SD-WAN Físico, compatível com solução de Ambiente de Nuvem com contratação de NGFW Virtual.

Este é o cenário atual da solução atual, hoje existem 28 equipamentos físicos de firewall implantados na CGU (dois para Sede e um para cada regional, com capacidades diferentes de acordo com o tamanho do datacenter), através do contrato

CGU nº 05/2019 com a empresa Claro. A CGU não detém os equipamentos, em vez disso ela paga pela sua utilização com o serviço.

**Solução 2:** Contratação de Subscrição com entrega de Licenciamento de Solução de Firewall com SD-WAN Virtual, compatível com solução de Ambiente de Nuvem com contratação de NGFW Virtual.

Este é um cenário que também é ofertado no mercado pelos principais fabricantes, onde em vez de ter uma entrega de hardware (equipamento físico) há entrega de licenciamento de software, que poderá ser usado para subir máquinas virtuais em hospedeiros e software de virtualização adquiridos em outros contratos pela CGU. Assim como o cenário anterior o pagamento também é por subscrição mensal ou anual pela utilização das licenças.

**Solução 3:** Contratação de Equipamento de NGFW com SD-WAN Físico, compatível com solução de Ambiente de Nuvem com contratação de NGFW Virtual.

Este é o mesmo cenário da Solução 1, com a diferença que em vez do pagamento de subscrição do serviço mensal ou anual, é feito um investimento para aquisição do equipamento físico com garantia e suporte do fabricante. Desta forma, a CGU estria adquirindo os equipamentos físicos da solução.

**Solução 4:** Contratação de Licenciamento perpétuo Solução de NGFW com SD-WAN Virtual, compatível com solução de Ambiente de Nuvem com contratação de NGFW Virtual.

Este é o mesmo cenário da Solução 3, com a diferença que é feito um investimento para aquisição do licenciamento perpétuo do software com garantia e suporte do fabricante. Desta forma, a CGU estaria adquirindo as licenças de software da solução e ao fim do término do suporte ou garantia, perde-se o direito de atualização do produto, porém a solução virtual continua em funcionamento caso ocorra algum atraso na contratação de uma nova solução ao fim do contrato.

### **Necessidades similares em outro órgão ou entidade da Administração Pública**

#### **PREGÃO ELETRÔNICO nº 108/2022 (DPU)**

Contratação de empresa especializada no fornecimento de ativos de segurança de rede do tipo Next Generation Firewall (NGFW), com SD-WAN integrada, instalação, treinamento e suporte técnico, para a Defensoria Pública da União em âmbito nacional, com garantia de 36 (trinta e seis meses).

#### **PREGÃO ELETRÔNICO nº 25/2022 (CEAGESP)**

“Contratação de empresa especializada na prestação de serviço de segurança de rede perimetral com solução de firewall de próxima geração (NGFW), contemplando instalação, configuração, gerenciamento, monitoramento, armazenamento de logs e suporte técnico especializado”

#### **PREGÃO ELETRÔNICO nº 02/2021 (CONAB)**

“Contratação de solução de comunicação de dados composta por SD-WAN (Software-defined Networking in a Wide Area Network) capaz de prover a interconexão da Matriz da CONAB, suas superintendências regionais, suas unidades armazenadoras e as bolsas de mercadoria, entre si e com a Internet, em âmbito nacional, e acesso redundante à Internet, na Matriz”

### **PREGÃO ELETRÔNICO Nº 02/2022 (CFP)**

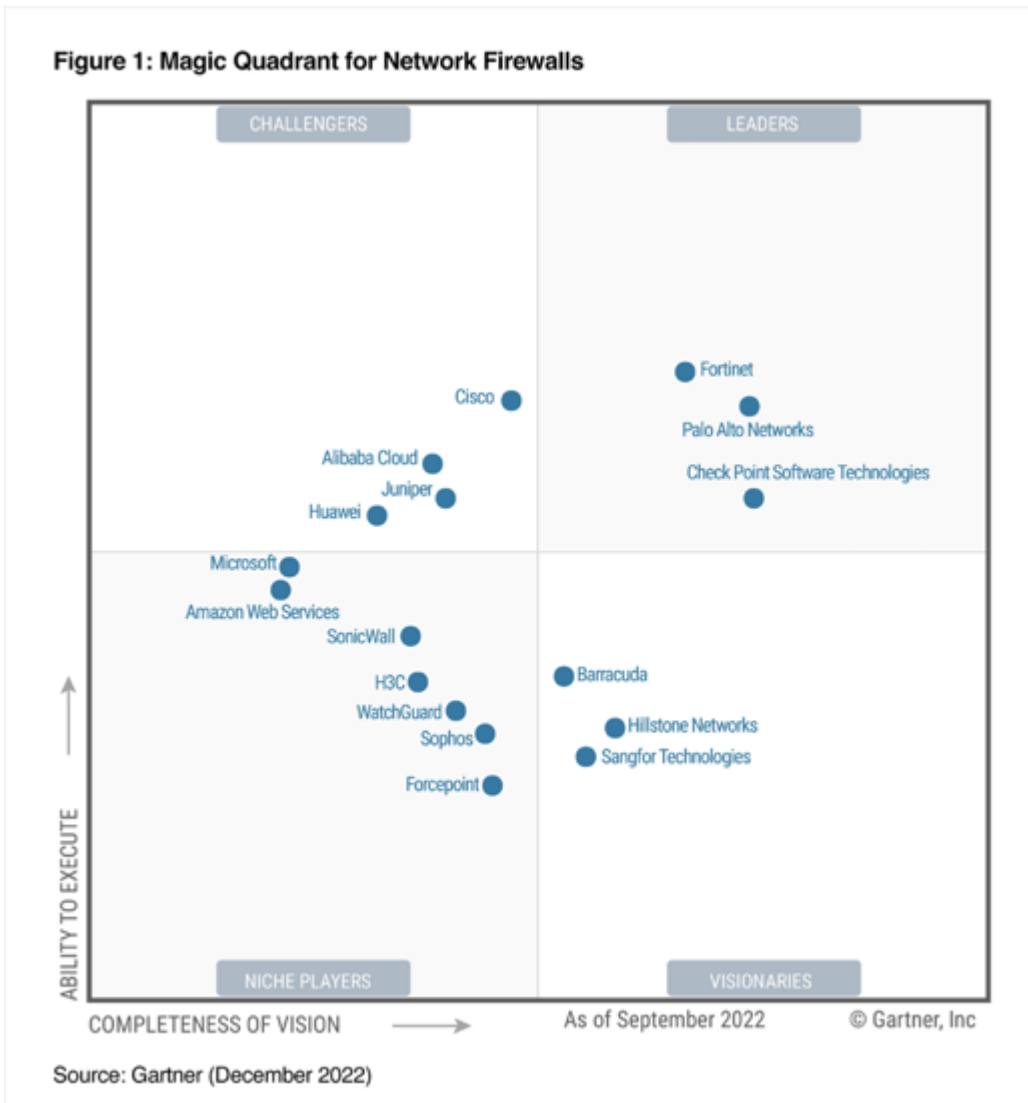
“Contratação de pessoa jurídica especializada para o fornecimento de renovação de subscrição da solução do *firewall*, incluindo garantia de hardware, atualização de versões e assinaturas de proteção, manutenção e suporte técnico.”

### **PREGÃO ELETRÔNICO Nº 37/2020 (ANAC)**

“registro de preço para a aquisição de solução de aceleração/otimização de tráfego WAN, implementação e configuração de rede definida por software (SD-WAN) e serviços de instalação, treinamento, suporte técnico e garantia de 60 meses.”

### **Alternativas do mercado**

Existem diversos fabricantes no mercado que trabalham com a fabricação de equipamentos e software de *NGFW* e *SD-WAN*. Ssegue abaixo o Quadrante mágico do Gartner para *Network Firewalls*, publicado em setembro de 2022.



**Avaliação das soluções identificadas frente aos requisitos**

Requisito		Soluções			
#ID	Nome curto	Solução 1 - Subscrição com NGFW Físico	Solução 2 - Subscrição com NGFW Virtual	Solução 3 - Aquisição de Equipamento com NGFW Físico	Solução 4 - Licenciamento Perpétuo NGFW Virtual
1	NGFW	Atende	Atende	Atende	Atende
2	Solução Híbrida Unificada com Alta Disponibilidade	Atende	Atende	Atende	Atende

3	Garantia e Suporte durante a vigência do contrato.	Atende	Atende	Atende	Atende
4	Serviços de Implantação com Repasse de Conhecimento	Atende	Atende	Atende	Atende
5	SD-WAN	Atende	Atende	Atende	Atende
6	Independência de camada de Virtualização	Atende	<b>Não Atende</b>	Atende	<b>Não Atende</b>
7	Horas de consultoria especializadas	Atende	Atende	Atende	Atende

## 9. Análise comparativa de soluções

### Análise comparativa de soluções

**Solução 1:** Licitação Pública para Contratação como Serviço através de Subscrição com entrega de equipamento de Firewall com SD-WAN Físico, compatível com solução de Ambiente de Nuvem com contratação de NGFW Virtual.

- Descrição da Solução: consiste na subscrição de uso de 28 NGFWs físicos (2 para Sede e 26 para regionais) com funcionalidade de SD-WAN de mesmo fornecedor compatível com NGFW Virtual para o ambiente de nuvem da AWS e Azure, um serviço de implantação e migração da solução atual com repasse de conhecimento, garantia e suporte 24/7 com direito de atualização do produto durante a vigência do contrato, 300 horas de serviço de consultoria especializada do fabricante, solução de gerência centralizada e solução de gerenciamento e armazenamento de logs.
- Fornecedores da solução: Alguns dos principais fornecedores do quadrante de Líderes do Gartner são Palo Alto, CheckPoint, Fortinet, entre outros.
- Quem utiliza e valor pago: MPU e MPDFT (R\$ 1.410.000,00); TJ MG (R\$ 1.203.382,78); Justiça SP (R\$ 538.020,00); MCOM (R\$ 560.000,00), etc.
- Diferentes formas de contratação:
  - Aluguel/Serviço: contrata-se o direito de usar o equipamento/software por um tempo determinado no contrato, após o término do direito de uso o equipamento/software é interrompido.

- Diferentes Métricas:
  - Serviços de implantação, repasse de conhecimento são pagos em sua totalidade e estimados por quantidade/horas;
  - Demais itens são pagos após comprovação da prestação mensal do serviço.
- Diferentes formas de pagamento:
  - Por se tratar de subscrição, a forma usual de pagamento é mensal.
- Requisitos da solução:
  - Capacitação: serviço de repasse de conhecimento.
  - Legais: Decreto nº 7.174, de 12 de maio de 2010; Diretrizes para a Aquisição de Ativos de Tecnologia da Informação e Comunicação contidas no documento “BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC – Versão 4”; publicado em 23/03/2017, disponível em [https://www.gov.br/governodigital/pt-br/contratacoes/orientacoes\\_ativos-de-tic-v-4.pdf](https://www.gov.br/governodigital/pt-br/contratacoes/orientacoes_ativos-de-tic-v-4.pdf).
  - Garantia e Manutenção: Suporte e Garantia do Fabricante com direito a atualização do produto durante a vigência do contrato;
  - Temporais: deverá estar implantada até a data de 01/04/2024, data final do contrato da solução atual.
  - Segurança e privacidade: inspeção de tráfego em camada nível 7; Intrusion Detection System (IDS); Intrusion Prevention System (IPS); detecção antimalware avançada (sandbox), Web Filtering e técnicas avançadas de detecção de ameaça baseadas em Inteligência Artificial, VPN com 2FA.
  - Sociais, ambientais e culturais: Linguagem da interface deve ser em inglês ou português.
  - Sustentabilidade: deverá adotar, no que couber, práticas de sustentabilidade e de natureza ambiental no fornecimento, conforme requisitos constantes na Instrução Normativa SLTI/MPOG nº01, de 19 de janeiro de 2010.
  - Arquitetura Tecnológica: Não se aplica, uma vez que a demanda trata de fornecimento de equipamentos.
  - Projeto, Implementação e Implantação: migração da solução atual com repasse de conhecimento.
  - Experiência e formação de equipe: não há.
  - Metodologia de Trabalho: remoto e presencial para fase de implantação e repasse de conhecimento.
- Atendimento aos padrões e modelos do Governo Eletrônico:
  - ePing: Não se aplica
  - eMag: Não se aplica
  - ePwg: Não se aplica
  - ICP-Brasil: Não se aplica
  - e-ARQ: Não se aplica
- Necessidade de adequação do ambiente para implantação e operação da solução:
  - **Recursos materiais:** Não há. Todos os materiais e acessórios necessário para a correta instalação e funcionamento deverão ser entregues pela contratada.

- **Recursos humanos:** Disponibilidade das equipes de engenharia, segurança e operação terceirizada para dar suporte na fase de implantação /migração da solução atual.
- Mecanismos de continuidade da solução (caso o contrato se encerre): como a contratação por subscrição de serviço, caso o contrato se encerre, a solução de continuidade seria uma tentativa de prorrogação emergencial do contrato atual para suprir o tempo necessário da nova solução a ser contratada.
- Critérios de comparação das soluções, pensando também no alcance dos objetivos da contratação:
  - **Critério 1:** Forma de pagamento
    - Vantagens:
      - Contratar como serviço exige orçamento de custeio, o que é mais flexível e imune às contingências orçamentárias quando comparado ao orçamento de investimento.
      - Pagamento parcelado do contrato, de forma mensal ou anual, durante a prestação do serviço, mitiga o risco de prejuízo por descontinuidade de fornecimento do serviço, caso empresa de tecnologia descontinue o suporte e atualização de suas licenças.
    - Desvantagens:
      - Geralmente o custo é um pouco mais elevado, por não conseguir desconto no pagamento único.

**Solução 3:** Licitação Pública para Contratação de Equipamento de Firewall com SD-WAN Físico, compatível Ambiente de Nuvem com contratação de NGFW Virtual.

- Descrição da Solução: consiste na aquisição de 28 NGFW físicos (2 para Sede e 26 para regionais) com funcionalidade de SD-WAN de mesmo fornecedor compatível com NGFW Virtual para o ambiente de nuvem da AWS e Azure, um serviço de implantação e migração da solução atual com repasse de conhecimento, garantia e suporte 24/7 com direito de atualização do produto durante a vigência do contrato, 300 horas de serviço de consultoria especializada do fabricante, solução de gerência centralizada e solução de gerenciamento e armazenamento de logs.
- Fornecedores da solução: Alguns dos principais fornecedores do quadrante de Líderes do Gartner são Palo Alto, CheckPoint, Fortinet, entre outros.
- Quem utiliza e valor pago: UFF (R\$ 1.023.884,80); MP/MS (Lote I - R\$ 6.699.999,20); TRF 1ª (R\$ 5.469.612,65); DPU (R\$ 4.765.500,00).
- Diferentes formas de contratação:
  - Aluguel/Serviço: via marketplace para o ambiente de nuvem.
  - Bens/Compra: aquisição dos equipamentos físicos para o ambiente on-premises.
- Diferentes Métricas:
  - Serviços de repasse de conhecimento são consumidos por horas;
  - Serviços de VPN segura são adquiridos por quantidade de usuários;
  - Demais itens são pagos por uso de forma única, mensal ou anual.
- Diferentes formas de pagamento:

- Ambiente de nuvem, por se tratar de subscrição, a forma usual de pagamento é mensal ou anual.
- Ambiente on-premises, por se tratar de equipamento físico, a forma usual de pagamento é única.
- Requisitos da solução
  - Capacitação: serviço de repasse de conhecimento.
  - Legais: Decreto nº 7.174, de 12 de maio de 2010; Diretrizes para a Aquisição de Ativos de Tecnologia da Informação e Comunicação contidas no documento “BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC – Versão 4”; publicado em 23/03/2017, disponível em [https://www.gov.br/governodigital/pt-br/contratacoes/orientacoes\\_ativos-de-tic-v-4.pdf](https://www.gov.br/governodigital/pt-br/contratacoes/orientacoes_ativos-de-tic-v-4.pdf).
  - Garantia e Manutenção: Suporte e Garantia do Fabricante com direito a atualização do produto durante a vigência do contrato;
  - Temporais: deverá estar implantada até a data de 01/04/2024, data final do contrato da solução atual.
  - Segurança e privacidade: inspeção de tráfego em camada nível 7; *Intrusion Detection System* (IDS); *Intrusion Prevention System* (IPS); detecção antimalware avançada (sandbox), *Web Filtering* e técnicas avançadas de detecção de ameaça baseadas em Inteligência Artificial, VPN com 2FA.
  - Sociais, ambientais e culturais: Linguagem da interface deve ser em inglês ou português.
  - Sustentabilidade: deverá adotar, no que couber, práticas de sustentabilidade e de natureza ambiental no fornecimento, conforme requisitos constantes na Instrução Normativa SLTI/MPOG nº01, de 19 de janeiro de 2010.
  - Arquitetura Tecnológica: Não se aplica, uma vez que a demanda trata de fornecimento de equipamentos.
  - Projeto, Implementação e Implantação: migração da solução atual com repasse de conhecimento.
  - Experiência e formação de equipe: não há.
  - Metodologia de Trabalho: remoto e presencial para fase de implantação e repasse de conhecimento.
- Atendimento aos padrões e modelos do Governo Eletrônico:
  - ePing: Não se aplica
  - eMag: Não se aplica
  - ePwg: Não se aplica
  - ICP-Brasil: Não se aplica
  - e-ARQ: Não se aplica
- Necessidade de adequação do ambiente para implantação e operação da solução:
  - **Recursos materiais:** Não há. Todos os materiais e acessórios necessário para a correta instalação e funcionamento deverão ser entregues pela contratada.
  - **Recursos humanos:** Disponibilidade das equipes de engenharia, segurança e operação terceirizada para dar suporte na fase de implantação /migração da solução atual.

- Mecanismos de continuidade da solução (caso o contrato se encerrado): no ambiente on-premises, como a solução é aquisição de equipamento físico, caso o contrato se encerre, o serviço continua em funcionamento no ambiente perdendo apenas o direito ao suporte e garantia de atualização do produto.
- Critérios de comparação das soluções, pensando também no alcance dos objetivos da contratação:
  - **Critério 1:** Forma de pagamento
    - Vantagens:
      - Geralmente o pagamento antecipado gera menor preço;
    - Desvantagens:
      - Há necessidade da disponibilidade total orçamentária para investimento já no início do contrato.
      - Pagamento total na assinatura do contrato para serviço, aumenta o risco de inexecução contratual, caso empresa de tecnologia descontinue o suporte e atualização de suas licenças.

### Comparação das alternativas:

Critérios/Opção	Solução 1	Solução 3
Critério 1	5	3
Critério Custo	1	5
<b>Pontuação Final</b>	<b>6</b>	<b>8</b>

### Descrição dos Critérios:

- **Critério 1:** Forma de pagamento;
- **Critério Custo:** Solução de menor preço;

### Classificação dos Critérios:

Classificação dos Critérios	Pontuação
<b>Melhor</b>	5
<b>Bom</b>	4
<b>Médio</b>	3

Ruim	2
Pior	1

## 10. Registro de soluções consideradas inviáveis

As soluções 2 e 4 mostram-se inviáveis pelo não atendimento ao requisito de negócio nº 6.

## 11. Análise comparativa de custos (TCO)

**Solução 1:** Licitação Pública para Contratação como Serviço através de Subscrição com entrega de equipamento de Firewall com *SD-WAN* Físico, compatível com solução de Ambiente de Nuvem com contratação de *NGFW* Virtual.

### Pregões

- Pregão Justiça SP (14/04/2023) – Item 1;

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
1	NGFW Tipo 1 - Suporte 24/7 por 60 meses <i>(equipamento similar)</i>	un	2	R\$ 538.020,00	R\$ 1.076.040,00

- Pregão MPU/DFT (13/12/2022) – Item 1;

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
1	NGFW Tipo 1 - Suporte 24/7 por 60 meses <i>(equipamento similar)</i>	un	1	R\$ 1.410.000,00	R\$ 1.410.000,00

- Pregão TCE/SE (12/08/2022) – Item 2 e 3;

--	--	--	--	--	--

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
2	NGFW Tipo 2 - Suporte 24/7 por 60 meses <i>(equipamento similar)</i>	un	13	R\$ 219.987,00	R\$ 2.859.831,00
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses <i>(equipamento similar)</i>	un	13	R\$ 219.987,00	R\$ 2.859.831,00

## Propostas Comerciais

- Proposta Claro (06/07/2023);

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
1	NGFW Tipo 1 - Suporte 24/7 por 60 meses	un	2	R\$3.758.353,70	R\$7.516.707,41
2	NGFW Tipo 2 - Suporte 24/7 por 60 meses	un	13	R\$ 3.361.961,35	R\$ 6.723.922,70
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses	un	13	R\$ 3.361.961,35	R\$ 6.723.922,70
4	Solução de gerência centralizada (appliance virtual)	un	1	R\$ 281.688,93	R\$ 281.688,93
5	Solução de gerência de logs (appliance virtual)	un	1	R\$ 995.138,33	R\$ 995.138,33
6	Implantação da Solução com migração da Atual no ambiente on-premisses	un	1	R\$ 128.000,00	R\$ 128.000,00
7	Repasse de conhecimento	horas	60	R\$ 1.666,66	R\$ 100.000,00
8	Serviço técnico especializado do fabricante	horas	300	R\$ 5.046,70	R\$ 1.514.010,00

- Proposta Checkpoint (29/05/2023);

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total

1	NGFW Tipo 1 - Suporte 24/7 por 60 meses	un	2	R\$ 3.091.650,00	R\$ 6.183.300,00
2	NGFW Tipo 2 - Suporte 24/7 por 60 meses	un	13	R\$ 801.876,92	R\$ 10.424.400,00
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses	un	13	R\$ 567.069,23	R\$ 7.371.900,00
4	Solução de gerência centralizada (appliance virtual)	un	1	R\$ 1.061.160,00	R\$ 1.061.160,00
5	Solução de gerência de logs (appliance virtual)	un	1	R\$ 704.040,00	R\$ 704.040,00
6	Implantação da Solução com migração da Atual no ambiente on-premisses	un	1	R\$ 440.100,00	R\$ 440.100,00
7	Repasse de conhecimento	horas	60	R\$ 2.170,00	R\$ 130.200,00
8	Serviço técnico especializado do fabricante	horas	300	R\$ 2.000,00	R\$ 600.000,00

- Proposta Inorpel (06/06/2023);

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
1	NGFW Tipo 1 - Suporte 24/7 por 60 meses	un	2	R\$ 3.862.058,11	R\$ 7.724.116,23
2	NGFW Tipo 2 - Suporte 24/7 por 60 meses	un	13	R\$ 562.879,46	R\$ 7.317.433,09
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses	un	13	R\$ 562.879,46	R\$ 7.317.433,09
4	Solução de gerência centralizada (appliance virtual)	un	1	R\$ 306.298,84	R\$ 306.298,84
5	Solução de gerência de logs (appliance virtual)	un	1	R\$ 1.078.910,58	R\$ 1.078.910,58

6	Implantação da Solução com migração da Atual no ambiente on-premisses	un	1	R\$ 195.000,00	R\$ 195.000,00
7	Repasse de conhecimento	horas	60	R\$ 540,00	R\$ 32.400,00
8	Serviço técnico especializado do fabricante	horas	300	R\$ 4.013,06	R\$ 1.203.918,00

- Proposta Ciron (29/05/2023);

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
1	NGFW Tipo 1 - Suporte 24/7 por 60 meses	un	2	R\$ 9.121.553,40	R\$ 18.243.106,80
2	NGFW Tipo 2 - Suporte 24/7 por 60 meses	un	13	R\$ 677.657,40	R\$ 8.809.546,20
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses	un	13	R\$ 677.657,40	R\$ 8.809.546,20
4	Solução de gerência centralizada (appliance virtual)	un	1	R\$ 271.968,00	R\$ 271.968,00
5	Solução de gerência de logs (appliance virtual)	un	1	R\$ 271.968,00	R\$ 271.968,00
6	Implantação da Solução com migração da Atual no ambiente on-premisses	un	1	R\$ 83.125,36	R\$ 83.125,36
7	Repasse de conhecimento	horas	60	R\$ 6.737,50	R\$ 404.250,00
8	Serviço técnico especializado do fabricante	horas	300	R\$ 2.119,79	R\$ 635.937,00

### Estimativa do Valor da Solução 1 e forma de cálculos

A estimativa de custos da Solução 1 foi estimada por item, utilizando preços do mercado e aplicando redução de 50%, conforme IN SEGES /ME Nº 65, DE 7 DE JULHO DE 2021, artigo 6º, § 2º, nas cotações comerciais recebidas por empresas.

A metodologia de cálculo utilizada para a estimativa segue o cálculo da Média, Mediana e o Desvio Padrão; O Coeficiente de Variação: calculado dividindo-se o

Desvio Padrão pela Média. O Limite Superior: calculado pela soma do Desvio Padrão com a Média. O Limite Inferior: calculado pela subtração do Desvio Padrão da Média.

Se o coeficiente de variação se mostrar inferior a 25%, os valores da amostra mostram-se homogêneos. Assim, a estimativa será a média dos valores encontrados. Caso o coeficiente de variação se mostrar superior a 25%, serão desconsiderados os valores acima do Limite Superior e abaixo do Limite Inferior.

Como o novo conjunto de valores (Coluna Saneado) também apresentou Coeficiente de Variação superior a 25%, os valores do subconjunto da amostra ainda se mostram dispersos, a estimativa será a mediana dos valores saneados. Como o novo conjunto de valores apresentou Coeficiente de Variação inferior a 25%, os valores do subconjunto mostram-se homogêneos. Assim, a estimativa será a média dos valores saneados.

item	Descrição	QTD	Valor Unitário Estimado	Valor Total Estimado
1	NGFW Tipo 1 - Suporte 24/7 por 60 meses	2	R\$1.691.507,73	R\$3.383.015,46
2	NGFW Tipo 2 - Suporte 24/7 por 60 meses	13	R\$299.961,38	R\$3.899.497,94
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses	13	R\$276.480,61	R\$3.594.247,93
4	Solução de gerência centralizada (appliance virtual)	1	R\$143.325,96	R\$143.325,96
5	Solução de gerência de logs (appliance virtual)	1	R\$463.014,82	R\$463.014,82
6	Implantação da Solução com migração da Atual no ambiente on-premisses	1	R\$67.687,56	R\$67.687,56
7	Repasso de conhecimento	60	R\$673,33	R\$40.399,80
8	Serviço técnico especializado do fabricante	300	R\$1.355,48	R\$406.644,00
<b>SOLUÇÃO 1 - VALOR TOTAL ESTIMADO</b>				<b>R\$11.997.833,47</b>

**Solução 3:** Licitação Pública para Contratação de Equipamento de Firewall com SD-WAN Físico, compatível Ambiente de Nuvem com contratação de NGFW Virtual.

## Pregões

- Pregão MP/MS (07/03/2023) – Item 1, 2, 3 e 7;

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
1	NGFW Tipo 1 - Suporte 24/7 por 60 meses <i>(equipamento similar)</i>	un	2	R\$ 1.387.710,00	R\$ 2.775.420,00
2	NGFW Tipo 2 - Suporte 24/7 por 60 meses <i>(equipamento similar)</i>	un	13	R\$ 151.311,00	R\$ 1.967.043,00
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses <i>(equipamento similar)</i>	un	13	R\$ 100.147,00	R\$ 1.301.911,00
7	Repasse de conhecimento	horas	-	R\$ 120.000,00	R\$ 120.000,00

- Pregão TRF 1A/DF (01/06/2023) – Item 1 e 7;

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
1	NGFW Tipo 1 - Suporte 24/7 por 60 meses <i>(equipamento similar)</i>	un	2	R\$ 749.604,66	R\$ 1.499.209,32
7	Repasse de conhecimento	horas	-	R\$ 39.200,00	R\$ 39.200,00

- Pregão DPU (13/12/2022) – Item 1, 4 e 7;

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
1	NGFW Tipo 1 - Suporte 24/7 por 60 meses <i>(equipamento similar)</i>	un	2	R\$ 966.000,00	R\$ 1.932.000,00
4	Solução de gerência centralizada (appliance virtual)	un	1	R\$ 179.500,00	R\$ 179.500,00

7	Repasse de conhecimento	horas	-	R\$ 72.000,00	R\$ 72.000,00
---	-------------------------	-------	---	---------------	---------------

- Pregão CFEF (23/05/2023) – Item 3;

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses <i>(equipamento similar)</i>	un	13	R\$ 86.833,33	R\$ 1.128.833,29

- Pregão COREN (27/04/2023) – Item 3;

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses <i>(equipamento similar)</i>	un	13	R\$ 146.457,2	R\$ 1.903.943,60

- Pregão MP/MS (07/03/2023) – Item 3;

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses <i>(equipamento similar)</i>	un	13	R\$ 100.147,00	R\$ 1.301.911,00

### Sites de Revendas na internet

- <https://www.timix.com.br/> - Itens 2 e 3

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
2	NGFW Tipo 2 - Suporte 24/7 por 60 meses <i>(equipamento similar)</i>	un	13	R\$ 172.941,96	R\$ 2.248.245,48

3	NGFW Tipo 3 - Suporte 24/7 por 60 meses  (equipamento similar)	un	13	R\$ 172.941,96	R\$ 2.248.245,48
---	--	----	----	----------------	------------------

- <https://www.firewall1.com.br/> - Itens 2 e 3

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
2	NGFW Tipo 2 - Suporte 24/7 por 60 meses  (equipamento similar)	un	13	R\$ 195.957,60	R\$ 2.547.448,8
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses  (equipamento similar)	un	13	R\$ 195.957,60	R\$ 2.547.448,8

## Propostas Comerciais

- Proposta Checkpoint (29/05/2023);

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
1	NGFW Tipo 1 - Suporte 24/7 por 60 meses	2	un	R\$ 2.274.384,59	R\$ 4.548.769,17
2	NGFW Tipo 2 - Suporte 24/7 por 60 meses	13	un	R\$ 473.229,00	R\$ 6.151.977,00
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses	13	un	R\$ 265.979,11	R\$ 3.457.728,44
4	Solução de gerência centralizada (appliance virtual)	1	un	R\$ 293.577,00	R\$ 293.577,00
5	Solução de gerência de logs (appliance virtual)	1	un	R\$ 279.148,99	R\$ 279.148,99

6	Implantação da Solução com migração da Atual no ambiente on-premisses	1	un	R\$ 305.650,00	R\$ 305.650,00
7	Repasse de conhecimento	60	horas	R\$ 1.833,33	R\$ 110.000,00
8	Serviço técnico especializado do fabricante	300	Horas	R\$ 384,17	R\$ 115.251,00

- Proposta Inorpel (06/06/2023);

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
1	NGFW Tipo 1 - Suporte 24/7 por 60 meses	2	un	R\$ 2.352.309,31	R\$ 4.704.618,62
2	NGFW Tipo 2 - Suporte 24/7 por 60 meses	13	un	R\$ 342.839,64	R\$ 4.456.915,32
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses	13	un	R\$ 342.839,64	R\$ 4.456.915,32
4	Solução de gerência centralizada (appliance virtual)	1	un	R\$ 186.561,05	R\$ 186.561,05
5	Solução de gerência de logs (appliance virtual)	1	un	R\$ 657.144,80	R\$ 657.144,80
6	Implantação da Solução com migração da Atual no ambiente on-premisses	1	un	R\$ 195.000,00	R\$ 195.000,00
7	Repasse de conhecimento	60	horas	R\$ 540,00	R\$ 32.400,00
8	Serviço técnico especializado do fabricante	300	Horas	R\$ 384,17	R\$ 115.251,00

- Proposta SigmaTelecom (08/08/2023);

Item	Descrição	Unidade	Qtde	Valor Unitário	Valor Total
1	NGFW Tipo 1 - Suporte 24/7 por 60 meses	2	un	R\$ 1.550.487,00	R\$ 3.100.974,00
2	NGFW Tipo 2 - Suporte 24/7 por 60 meses	13	un	R\$ 265.124,00	R\$ 3.446.612,00
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses	13	un	R\$ 298.458,00	R\$ 3.879.954,00
4	Solução de gerência centralizada (appliance virtual)	1	un	R\$ 455.000,00	R\$ 455.000,00
5	Solução de gerência de logs (appliance virtual)	1	un	R\$ 310.000,00	R\$ 310.000,00
6	Implantação da Solução com migração da Atual no ambiente on-premisses	1	un	R\$ 145.870,00	R\$ 145.870,00
7	Repasso de conhecimento	60	horas	R\$ 4.152,00	R\$ 249.120,00
8	Serviço técnico especializado do fabricante	300	Horas	-	-

### Estimativa do Valor da Solução 3 e forma de cálculos

A estimativa de custos da Solução 1 foi estimada por item, utilizando preços do mercado e aplicando redução de 40%, conforme IN SEGES /ME Nº 65, DE 7 DE JULHO DE 2021, artigo 6º, § 2º, nas cotações comerciais recebidas por empresas.

A metodologia de cálculo utilizada para a estimativa calculará a Média, Mediana e o Coeficiente de Variação. O Coeficiente de Variação será calculado dividindo-se o Desvio Padrão pela Média, o Limite Superior será calculado pela soma do Desvio Padrão com a Média e o Limite Inferior será calculado pela subtração do Desvio Padrão da Média.

Se o coeficiente de variação se mostrar inferior a 25%, os valores da amostra mostram-se homogêneos. Assim, a estimativa será a média dos valores encontrados. Caso o coeficiente de variação se mostrar superior a 25%, serão desconsiderados os valores acima do Limite Superior e abaixo do Limite Inferior.

Como o novo conjunto de valores também apresentou Coeficiente de Variação superior a 25%, os valores do subconjunto da amostra ainda se mostram dispersos, a estimativa será a mediana dos valores saneados. Como o novo conjunto de valores apresentou Coeficiente de Variação inferior a 25%, os valores do subconjunto mostram-se homogêneos. Assim, a estimativa será a média dos valores saneados.

<b>item</b>	<b>Descrição</b>	<b>QTD</b>	<b>Valor Unitário Estimado</b>	<b>Valor Total Estimado</b>
1	NGFW Tipo 1 - Suporte 24/7 por 60 meses	2	R\$1.134.937,20	R\$2.269.874,40
2	NGFW Tipo 2 - Suporte 24/7 por 60 meses	13	R\$194.821,02	R\$2.532.673,26
3	NGFW Tipo 3 - Suporte 24/7 por 60 meses	13	R\$164.515,36	R\$2.138.699,68
4	Solução de gerência centralizada (appliance virtual)	1	R\$177.823,10	R\$177.823,10
5	Solução de gerência de logs (appliance virtual)	1	R\$176.744,70	R\$176.744,70
6	Implantação da Solução com migração da Atual no ambiente on-premises	1	R\$102.261,00	R\$102.261,00
7	Repasse de conhecimento	60	R\$1.592,80	R\$95.568,00
8	Serviço técnico especializado do fabricante	300	R\$1.319,17	R\$395.751,00
<b>SOLUÇÃO 3 - VALOR TOTAL ESTIMADO</b>				<b>R\$7.889.395,14</b>

Solução	TCO
Solução 1	R\$11.997.833,47
Solução 3	R\$7.889.395,14

Tabela Comparativa dos Custos Totais de Propriedade (TCO) entre as soluções.

## 12. Descrição da solução de TIC a ser contratada

### a. Descrição da Solução Tecnológica

A solução tecnológica consiste na contratação de serviço para uso de 28 NGFWs físicos (2 para Sede e 26 para regionais) com funcionalidade de SD-WAN de mesmo fornecedor compatível com NGFW Virtual para o ambiente da AWS e Azure, um serviço de implantação e migração da solução atual com repasse de conhecimento, garantia e suporte 24/7 com direito de atualização do produto durante a vigência do contrato, 300 horas de serviço de consultoria especializada do fabricante, solução de gerência centralizada e solução de gerenciamento e armazenamento de logs.

### b. Parcelamento da Solução

Não há parcelamento da solução. Justifica-se o agrupamento dos itens pois se trata de uma solução unificada de TIC, cujos itens integrantes são interdependentes. A divisão em lotes acarretaria a não uniformidade da prestação do serviço, dificuldade na gestão dos contratos e fiscalização dos serviços além da perda de economia de escala.

### c. Utilização de SRP

#### c.1. Justificativa SRP

Para contratação em comento, não se aplica.

#### c.2. Participação na IRP

Para contratação em comento, não se aplica.

#### c.3 Utilização por órgão não participante

Para contratação em comento, não se aplica.

## 13. Estimativa de custo total da contratação

Valor (R\$): 7.889.395,14

A Solução 3 apresenta o Valor Total de **R\$7.889.395,14**.

#### **14. Justificativa técnica da escolha da solução**

A solução 3 atende todas as necessidades de negócio e critérios definidos neste estudo.

#### **15. Justificativa econômica da escolha da solução**

A solução 3 foi escolhida por apresentar melhor custo-benefício diante dos critérios previamente definidos, conforme tabela apresentada na Análise comparativa de soluções (item 9). A Solução 3, com pagamento integral, é a solução de menor custo.

#### **16. Benefícios a serem alcançados com a contratação**

Esta contratação tem por finalidade substituir as atuais soluções de segurança e interconectividade de redes descritas na seção anterior (firewall e SD-WAN), promovendo a continuidade de serviço essencial para segurança de perímetro a toda infraestrutura de TI que sustenta todos os sistemas e dados desta Organização, como os sistemas críticos Super, E-aud etc.

Além de preservar a continuidade do serviço essencial, este projeto também tem por finalidade contratar solução on-premises que seja compatível com tecnologias de nuvem AWS e Microsoft Azure, de forma a nivelar e centralizar os mecanismos de detecção e prevenção de ameaças de segurança cibernética em toda a nova infraestrutura híbrida, “on-premises” e “multicloud”, além de garantir a modernização da infraestrutura tecnológica da CGU e adequação às constantes evoluções da área de tecnologia da informação.

#### **17. Providências a serem Adotadas**

Não há necessidade de providências para adequação do órgão, pois a infraestrutura necessária para implantação já existe.

#### **18. Declaração de Viabilidade**

Esta equipe de planejamento declara **viável** esta contratação.

##### **18.1. Justificativa da Viabilidade**

Considerando as disposições constantes neste estudo, sobretudo, acerca das justificativas da necessidade de aquisição e do quantitativo estimado, bem como da análise dos riscos que envolvem a fase inicial deste

procedimento, esta equipe se posiciona pela VIABILIDADE da contratação de **soluções de segurança e interconectividade de redes on-premises** especificada neste documento, por entender que foram razoáveis os fundamentos que motivaram a demanda.

## 19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

### **THIAGO GUEDES PAYSAN**

Integrante requisitante



*Assinou eletronicamente em 09/11/2023 às 14:47:21.*

### **PIERRY ANGELO PEREIRA**

Integrante Técnico



*Assinou eletronicamente em 09/11/2023 às 17:23:21.*

Despacho: Declaro que o conteúdo do presente documento está adequado às disposições da Instrução Normativa nº 94/2022 – SGD/ME.

### **HENRIQUE APARECIDO DA ROCHA**

Autoridade Máxima de TIC



*Assinou eletronicamente em 09/11/2023 às 14:50:05.*