GOVERNO DO DISTRITO FEDERAL

INSTITUTO DE GESTÃO ESTRATÉGICA DE SAÚDE DO DISTRITO FEDERAL

Gerência de Tecnologia da Informação e Comunicação

Núcleo de Rede

ELEMENTO TÉCNICO

Nº 4/2023 - IGESDF/UCAD/SUCAD/GETIC/NURED

Unidade: IGESDF

Solicitante: DALOG (Despacho - IGESDF/DP/DALOG (83059697)

Interessado/Responsável: DALOG / GGLOG

E-mail: infraestrutura@igesdf.org.br

Contato: (61) 3315-8900 Ramal: xxxx

1. 1. DO OBJETO

1.1. O presente Elemento Técnico tem por objeto a eventual contratação de empresa especializada na prestação de serviços para provimento de Serviços de Nuvem Pública, Serviço de Serviço de Next Generation Firewall e Controle de acesso, Serviço de Conectividade de Rede, Serviço de Segurança para EndPoint e Auditoria, Serviço de Licenciamento Microsoft e Serviços Especializados todos por demanda para atendimento às demandas do IGESDF.

1.2. A solução será composta por 5 lotes dispostos da seguinte forma:

- **Anexo I**: Lote 1- IaaS - Nuvem Pública;
- **Anexo II**: Lote 2 - SaaS - Serviço de Next Generation Firewall ;
- **Anexo III:** Lote 3 – SaaS - Serviço de Conectividade e Controle de acesso;
- **Anexo IV**: Lote 4 – SaaS - Serviço de Proteção de EndPoints e Auditoria ;
- **Anexo V:** Lote 5 - PaaS - Serviço de Licenciamento Microsoft (MS)

LOTE	ITEM	Subitem	Tipo de Instancia	Métrica	USN (Previsto)	Valor Unitário	Valor Mensal previsto	Valor Anual previsto	Valor previsto para 30 meses
			Instancia - 1 (Linux) com 1 vCPU e 2 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 2 (Linux) com 2 vCPU e 4 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 3 (Linux) com 4 vCPU e 8 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 4 (Linux) com 4 vCPU e 16 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 5 (Linux) com 8 vCPU e 32 GB de memória RAM (por			R$	R$	R$	R$

			demanda)						
		1.1	Instancia - 6 (Linux) com 16 vCPU e 64 GB de memória RAM (por demanda)	Instancia/Mês	1.500.000	R$	R$	R$	R$
			Instancia - 7 (Linux) com 32 vCPU e 64 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 8 (Linux) com 32 vCPU e 128 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 9 (Windows) com 1 vCPU e 2 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 10 (Windows) com 2 vCPU e 4 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 11 (Windows) com 2 vCPU e 8 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 12 (Windows) com 4 vCPU e 16 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 13 (Windows) com 8 vCPU e 32 GB de memória RAM (por demanda)			R$	R$	R$	R$
1	IaaS - Nuvem Pública		Instancia - 14 (Windows) com 16 vCPU e 64 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 15 (Windows) com 32 vCPU e 64 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 16(Windows) com 32 vCPU e 128 GB de memória RAM (por demanda)			R$	R$	R$	R$
		Subitem	**Descrição**	**Métrica**	**QNTD. (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
		1.2	Serviço de Storage Block-Level SSD (por demanda)	TB/Mês	100	R$	R$	R$	R$

		1.3	Serviço de Storage Block-Level HDD (por demanda)	TB/Mês	100	R$	R$	R$	R$
		1.4	Serviço de Storage File-Level (por demanda)	TB/Mês	50	R$	R$	R$	R$
		1.5	Serviço de backup e restore (por demanda)	Mensal	200	R$	R$	R$	R$
		1.6	Balanceamento de carga (por demanda)	Unidade/Mês	20	R$	R$	R$	R$
		1.7	Porta de conexão de fibra 1 GBPS (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		1.8	Porta de conexão de fibra 10 gbps (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		1.9	Serviço de Tráfego de Saída de Rede (por demanda)	Mensal	100	R$	R$	R$	R$
		1.10	Serviço de DNS (por demanda)	Mensal	100	R$	R$	R$	R$
		1.11	Serviço de VPN (por demanda)	Unidade/Mês	20	R$	R$	R$	R$
		1.12	Serviço de Web Application Firewall (por demanda)	Unidade/Mês	200	R$	R$	R$	R$
		1.13	Serviço de Autenticação Integrado com AD (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		1.14	Serviço de Monitoramento (por demanda)	Unidade/Mês	1	R$	R$	R$	R$
		1.15	Serviços Especializados de Nuvem Pública (por demanda)	Hora	4.000	R$	R$	R$	R$
LOTE	**ITEM**	**Subitem**	**Descrição**	**Métrica**	**QNTD (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
2	SaaS - Serviço de Next Generation Firewall	2.1	Serviço Next Generation Firewall do TIPO 1 (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		2.2	Serviço Next Generation Firewall do TIPO 2 (por demanda)	Unidade/Mês	20	R$	R$	R$	R$
LOTE	**ITEM**	**Subitem**	**Descrição**	**Métrica**	**QNTD (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
		3.1	Serviço Conectividade de Rede – Tipo 1 (por demanda)	Unidade/Mês	4	R$	R$	R$	R$

3	SaaS - Serviço de Conectividade e Controle de acesso	3.2	Serviço Conectividade de Rede – Tipo 2 (por demanda)	Unidade/Mês	90	R$	R$	R$	R$
		3.3	Serviço Conectividade de Rede – Tipo 3 (por demanda)	Unidade/Mês	60	R$	R$	R$	R$
		3.4	Serviço de Conectividade Sem Fio (por de manda)	Unidade/Mês	300	R$	R$	R$	R$
		3.5	Software de Controle de Acesso à Rede (por de manda)	Unidade/Mês	1	R$	R$	R$	R$
LOTE	**ITEM**	**Subitem**	**Descrição**	**Métrica**	**QNTD (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
4	SaaS - Serviço de Proteção de EndPoints e Auditoria	4.1	Serviço de proteção de EndPoints (por demanda)	Unidade/Mês	4.000	R$	R$	R$	R$
		4.2	Serviço de Auditoria (por demanda)	Unidade/Mês	4.000	R$	R$	R$	R$
LOTE	**ITEM**	**Subitem**	**Descrição**	**Métrica**	**QNTD (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
5	SaaS - Serviço de Licenciamento Microsoft (MS)	5.1	Office 365 E1STANDARDPACK ou equivalente (por demanda)	Unidade/Mês	4.000	R$	R$	R$	R$
		5.2	Microsoft 365 E3SPE_E3 ou equivalente (por demanda)	Unidade/Mês	1.000	R$	R$	R$	R$
		5.3	Power BI ProPOWER_BI_PRO ou equivalente (por demanda)	Unidade/Mês	10	R$	R$	R$	R$
		5.4	Systencenter - SCCM (por demanda)	Unidade/Mês	1	R$	R$	R$	R$
		5.5	TS RDS licença per user (por demanda)	Unidade/Mês	200	R$	R$	R$	R$
		5.6	Azure Active Directory Premium P1 ou equivalente (por demanda)	Unidade/Mês	50	R$	R$	R$	R$
		5.7	Serviços Consultoria Técnica Especializada (por demanda)	Horas	4.000	R$	R$	R$	R$

2. ESPECIFICAÇÃO DETALHADA DO OBJETO A SER CONTRATADO

2.1. Especificação detalhada e quantidades, conforme:

- **Anexo I**: Lote 1- IaaS - Nuvem Pública;
- **Anexo II**: Lote 2 - SaaS - Serviço de Next Generation Firewall;
- **Anexo III:** Lote 3 – SaaS - Serviço de Conectividade e Controle de acesso;
- **Anexo IV**: Lote 4 – SaaS - Serviço de Proteção de EndPoints e Auditoria ;
- **Anexo V:** Lote 5 - PaaS - Serviço de Licenciamento Microsoft (MS);
- **Anexo VI:** Proposta;
- **Anexo VII:** Ordem de Serviço
- **Anexo VIII:** Ordem de Fornecimento;
- **Anexo IX:** Unidades do IGESDF;
- **Anexo X:** Fiscal do Contrato e seu respectivo Substituto;

3. JUSTIFICATIVA PARA A AQUISIÇÃO E/OU CONTRATAÇÃO DO SERVIÇO

3.1. Computação em nuvem é um modelo para permitir que o provisionamento de recursos e serviços possam ser realizados de qualquer lugar e a qualquer momento, de maneira conveniente, com acesso através de rede a recursos computacionais configuráveis (ex.: redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente provisionados e devolvidos com o mínimo de esforço em gerenciamento ou interatividade com o provedor de serviços;

3.2. Tal modelo pode conferir grande incremento da racionalidade administrativa e elevada redução de gastos para o IGESDF, pois possibilita eliminar despesas com construção de salas-cofres, suprimento de energia elétrica e refrigeração, compras de no-breaks e de outros equipamentos e softwares, bem como diminuição de dispêndios com equipe qualificada e manutenção das instalações e equipamentos. Também permite que a equipe de TI do órgão fique focada em outras áreas estratégicas da organização, tendo atuação mais finalística.

3.3. Ainda há uma notável flexibilidade do novo modelo em relação à infraestrutura convencional, pois permite que o contratante aumente ou diminua a capacidade ambiente de computação em nuvem de acordo com suas necessidades. Recursos como processamento, armazenamento, memória e rede (utilização de banda) devem estar disponíveis de acordo com a necessidade do negócio, podendo aumentar ou diminuir junto com seu ambiente, de acordo com a demanda necessária.

3.4. A solução contra ameaças digitais deverá englobar alocação de equipamentos, produtos, peças e softwares necessários à perfeita consecução das atividades e atendimento às especificações técnicas durante o prazo de vigência, incluindo manutenção e atualização dos produtos e softwares utilizados e monitoramento de segurança em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, nos trezentos e sessenta e cindo dias do ano).

3.5. O serviço de mensageria e colaboração em nuvem consiste em uma solução de produtividade e colaboração, disponibilizada em ambiente de nuvem, que integra aplicativos e recursos digitais com vistas a proporcionar ferramentas que possibilitem o aumento da eficiência na realização de atividades comuns relacionadas a produção digital de conteúdo e na organização e comunicação dentro das equipes de trabalho

3.6. **São características da computação em nuvem:**

3.6.1. **Computação em nuvem:** É um modelo para permitir que o provisionamento de recursos e serviços possam ser realizados de qualquer lugar e a qualquer momento, de maneira conveniente, com acesso através de rede a recursos computacionais configuráveis (ex.: redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente provisionados e devolvidos com o mínimo de esforço em gerenciamento ou interatividade com o provedor de serviços.

3.6.2. **Infraestrutura como Serviço (Infrastructure as a Service - IaaS):**Encarregada por disponibilizar toda a infraestrutura necessária para os modelos PaaS e o SaaS. O principal objetivo deste modelo é tornar mais fácil e acessível o fornecimento de recursos, tais como servidores, rede, armazenamento e outros recursos de computação essenciais para construir um ambiente sob demanda, podendo incorporar sistemas operacionais e aplicativos.

3.6.3. **Plataforma como Serviço (Platform as a Service - Paas):**Oferece as licenças de software, infraestrutura, manutenção, sistemas de comunicação e tudo o mais necessário para disponibilizar um aplicativo ou site.

3.6.4. **Software como Serviço (Software as a Service - SaaS):**O fornecedor do software se responsabiliza por toda a estrutura necessária para a disponibilização do sistema (servidores, conectividade, cuidados com segurança da informação), e o cliente utiliza o software via internet.

3.6.5. **Autosserviço sob demanda:** A **CONTRATANTE** pode unilateralmente provisionar a capacidade computacional necessária, como servidores e redes de armazenamento, de maneira

automática sem precisar de interação humana com cada provedor de serviços em nuvem.

3.6.6. **Amplo acesso pela rede:** Recursos computacionais estão disponíveis através da rede e acessados através de mecanismos padrões que promovem o uso heterogêneo de plataformas clientes (ex.: smartphones, tablets, laptops, estações de trabalho).

3.6.7. **Rápida Elasticidade:** Capacidades podem ser elasticamente aumentadas ou diminuídas de acordo com a demanda atual e o perfil de uso das aplicações. Estas alterações podem ser realizadas a qualquer momento, possibilitando otimização do uso de recursos e consequente economia de valores.

3.6.8. **Serviço mensurado:** Sistemas em nuvem automaticamente controlam e otimizam o uso de recursos, levando em consideração capacidades de monitoramento em um nível apropriado para o tipo de serviço (ex.: armazenamento, processamento, largura de banda, e usuários ativos por contas.) O uso de recursos pode ser monitorado, controlado, e reportado, provendo transparência tanto para o provedor quanto para o consumidor do serviço utilizado. Buscando promover a melhor gestão de recursos de infraestrutura e na qualidade dos serviços de TI, a referida contratação pretende suprir o IGESDF quanto a necessidade de recursos de TI com solução eficiente, de alta disponibilidade e com baixo custo.

3.7. O IGESDF possui como missão institucional prestar serviços de alta complexidade em saúde aos usuários do SUS aliados à produção e aplicação de conhecimentos, por meio de uma gestão ágil, efetiva e sustentável. Em decorrência disso, necessita de infraestrutura adequada de TI que atenda às necessidades do IGESDF de forma adequada para melhor condução de suas atividades.

3.8. A cada dia, o IGESDF necessita automatizar seus processos operacionais e administrativos, desta forma passa a depender cada vez mais de sua infraestrutura tecnológica para viabilizar suas atividades e implementar novas soluções, otimizando custos e melhoria da qualidade dos serviços prestados aos seus clientes e usuários do IGESDF.

3.9. O IGESDF é responsável por planejar, desenvolver, implantar e manter os sistemas de informação necessários ao funcionamento deste Instituto, seja com recursos internos ou externos. Além disso, é sua responsabilidade propor políticas e planejar, coordenar, supervisionar e orientar normativamente as atividades de gestão dos recursos de tecnologia da informação.

3.10. O Plano Diretor de Tecnologia da Informação – PDTI é o instrumento que permite nortear e acompanhar a atuação da área de Tecnologia da Informação, definindo as estratégias e planos de ações para implantá-las, visando obter melhor gestão dos recursos e maior qualidade na prestação de serviços aos cidadãos de Brasília pelo IGESDF.

3.11. Baseado no Planejamento Estratégico Institucional do IGESDF, foi realizado o alinhamento deste com as necessidades estratégicas do IGESDF, de forma a garantir que as metas e ações de TI sejam organizadas para atender aos objetivos finalísticos do IGESDF.

3.12. A previsão de atendimento ao estabelecido no PDTI em sua Diretriz nº 4 "..Diretriz Nº 04 – Possuir uma infraestrutura de TI de alta disponibilidade, visando garantir a continuidade da operação com o mínimo de interrupção..."

3.13. Alinhamento ao proposto no Objetivo Estratégico 06 do PDTI: "...OE.06 – Prover infraestrutura de Tecnologia da Informação e Comunicação adequada para sustentar às necessidades do IGESDF

- Reestruturação e ampliação da Infraestrutura de TIC..."

3.14. **Reconhecimento das necessidades identificadas pelas áreas estratégicas no PDTI:**

- N27- Readequação de infraestrutura em nuvem
- N29- Implantação Data Center
- N38- Infraestrutura Física de TI projetada para atender as necessidades futuras do IGESDF

3.15. **O projeto visa atingir os seguintes objetivos:**

3.15.1. Redução de custos de manutenção e melhor eficiência pelo uso racional dos recursos, uma vez que estes foram definidos de forma a atender as necessidades do usuário.

3.15.2. Ganho de economia de escala, pois, ao prospectar grandes volumes licitados, a Administração Pública amplia seu poder de compra junto aos fornecedores e reduz consideravelmente os preços, fato que certamente não ocorreria quando do fracionamento de certames.

3.15.3. Atender ao demandado no Processo SEI nº 04016-00004350/2019-45, o Despacho -

IGESDF/DP/DALOG (83059697) "...o qual encaminham os autos a Gerência de Tecnologia da Informação e Comunicação para que instaure imediatamente novo processo regular com vistas à contratação do objeto em tela, com urgência que o caso requer, uma vez que a vigência do contrato se encerrará em 21/09/2022..."

3.15.4. Atender ao demandado no Processo SEI nº 04016-00015863/2023-68, o **Despacho - IGESDF/CONAD/CONT (108108424)**, "...o qual encaminham os autos a Gerência de Tecnologia da Informação e Comunicação a necessidade da Controladoria Interna, e das suas Coordenações, de organizar os dados dos trabalhos realizados, bem como de apresentá-los à alta gestão de forma contínua, encaminhamos a Documentação Inicial de Demanda - DID (106560699) para ciência e as providências pertinentes..."

3.15.5. Atender ao demandado no Processo SEI nº 04016-00067289/2022-42, o **Memorando Nº 119/2022 - IGESDF/DP/DIEP/GGADM** (90742975), "...o qual encaminham os autos a Gerência de Tecnologia da Informação e Comunicação que seja realizado estudo técnico para o levantamento de requisitos para a disponibilização de internet *wireless* nos seguintes setores: Unidades de Pronto Atendimento: sala vermelha, sala amarela e espaço de ensino (sala de aula). Hospital de Base do Distrito Federal: Pronto Socorro, Enfermarias, Unidades de Terapia Intensiva, Ambulatório (consultórios) e Espaços de Ensino (salas de aula, biblioteca e auditório), Hospital Regional de Santa Maria: Pronto Socorro, Enfermarias, Unidades de Terapia Intensiva, Ambulatório (consultórios) e Espaços de Ensino (salas de aula, biblioteca e auditório)..."

3.15.6. Atender ao Processo **SEI nº 04016-00046991/2022-72**, ".... onde é informado sobre a essencialidade do ativos de rede, a obsolescência dos equipamentos que estão em uso a mais de 10 anos e não possuem garantia, os impactos referente a indisponibilidade ou falha."

4. PRAZO DESEJADO PARA ENTREGA DO BEM E/OU INÍCIO DA PRESTAÇÃO SERVIÇOS E A PREVISÃO DE VIGÊNCIA CONTRATUAL

4.1. O contrato terá sua vigência pelo prazo 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.

5. DO PRAZO DE INÍCIO DE FORNECIMENTO:

5.1. Deverá ser realizado reunião entre a **CONTRATADA** e a equipe técnica da **CONTRATANTE** para alinhamento de cronograma de implementação.

5.2. Devido a imprescindibilidade do fornecimento da solução, o inicio da entrega dos itens relacionados em cada lote, deve ser:

a) **Lote 1: IaaS - Serviço de Nuvem Pública:** Mediante a assinatura do CONTRATO, será realizado reunião com a Gerencia de TI e Fiscais do CONTRATO no prazo máximo de 5 (cinco) dias corridos, onde será definido os recursos iniciais necessários para migração de nuvem e hiperconvergencia prestados pelo contrato antigo para o novo contrato. Após a emissão da Ordem de Fornecimento (**Anexo VIII)**, a **CONTRATADA** deve iniciar suas atividades no prazo máximo de 10 (dez) dias corridos e a entrega total deve ser concluída no prazo mínimo de 30 (trinta) dias corridos e prazo máximo de 60(sessenta) dias corridos após a emissão de Ordem de Fornecimento (**Anexo VIII)**.

b) **Lote 2: SaaS - Serviço de Serviço de Next Generation Firewall:** Mediante a assinatura do CONTRATO, sera emitida a Ordem de Fornecimento (**Anexo VIII)** com quantitativo inicial, o prazo de entrega dos serviços deve iniciar no prazo máximo de 30 (trinta) dias corridos e a entrega total deve ser concluída no prazo máximo de 60 (sessenta) dias corridos após a emissão de Ordem de Fornecimento **(Anexo VIII)**.

c) **Lote 3: SaaS - Serviço de Conectividade de Rede e Controle de acesso:** Mediante a assinatura do CONTRATO, sera emitida a Ordem de Fornecimento (**Anexo VIII)** com quantitativo inicial, o prazo de entrega dos serviços deve iniciar no prazo máximo de 30 (trinta) dias e a entrega total deve ser concluída no prazo máximo de 60 (trinta) dias após a emissão de Ordem de Fornecimento **(Anexo VIII).**

d) **Lote 4: SaaS - Serviço de Segurança para EndPoint e Auditoria:** Mediante a assinatura do CONTRATO, sera emitida a Ordem de Fornecimento **(Anexo VIII)** com quantitativo inicial, o prazo de entrega dos serviços deve iniciar no prazo máximo de 30 (trinta) dias e a entrega total deve ser concluída no prazo máximo de 60 (trinta) dias corridos após a emissão de Ordem de Fornecimento (**Anexo VIII)**.

e) **Lote 5: PaaS - Serviço de Licenciamento Microsoft (MS):** Mediante a assinatura do CONTRATO, sera emitida a Ordem de Fornecimento (**Anexo VIII)** com quantitativo inicial, o prazo de entrega dos serviços deve iniciar no prazo máximo de 10 (dez) dias corridos e a entrega total deve ser

concluída no prazo máximo de 30 (trinta) dias corridos após a emissão de Ordem de Fornecimento (**Anexo VIII)**.

5.3. Caso haja alguma impossibilidade no cumprimento do prazo do **item 5.2**, a **CONTRATADA** deverá emitir justificativa formal para obtenção da extensão do prazo, sendo prorrogável por igual período

5.4. A Ordem de Fornecimento (**Anexo VII)** é utilizado para determinar a disponibilidade do Lote e seus Subitens, incluindo todas as configurações necessárias para o uso inicial. Por sua vez a gestão mensal do Lotes e Subitens a ser utilizado durante toda a vigência do CONTRATO, sera realizada mediante a Ordem de Serviço (**Anexo VII**).

6. UNIDADE NA QUAL O BEM DEVERÁ SER ENTREGUE E/OU O SERVIÇO DEVERÁ SER PRESTADO

6.1. Os serviços deverão ser prestados de forma a atender todas as unidades do IGESDF.

6.2. Atualmente as unidades do IGESDF estão no **Anexo IX,** cabe ainda destacar que este anexo, é meramente informativo e que a qualquer momento podem ser adicionado ou removido unidades sem ônus para os contratos.

7. INDICAÇÃO DO FISCAL DO CONTRATO, E SEU RESPECTIVO SUBSTITUTO

7.1. A informação referente ao Fiscal do contrato e seu respectivo substituto esta disponível no **ANEXO X**

8. DOCUMENTOS DE QUALIFICAÇÃO TÉCNICA

8.1. **COMPROVAÇÃO DA QUALIFICAÇÃO TÉCNICA:**

8.1.1. Atestado (s) de capacidade técnica, fornecido (s) por pessoa (s) jurídica (s) de direito público ou privado, para as quais o CONTRATADO tenha executado o fornecimento da solução com a complexidade operacional equivalente aos especificados neste Elemento Técnico.

8.1.2. Serão aceitos somente atestados expedidos após a conclusão do contrato ou decorrido no mínimo um ano do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior.

8.1.3. A empresa participante deve disponibilizar, quando demandada, todas as informações necessárias à comprovação da legitimidade do atestado, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.

8.1.4. Os atestados deverão ser emitidos em papel timbrado e conter:

- Razão Social, CNPJ e Endereço Completo da Empresa Emitente;
- Razão Social da Contratada;
- Número e vigência do contrato se for o caso;
- Objeto do contrato;
- Declaração de que foram atendidas as expectavas quanto ao cumprimento de cronogramas pactuados;
- Local e Data de Emissão;
- Identificação do responsável pela emissão do atestado,
- Cargo, Contato (telefone e correio eletrônico);
- Assinatura do responsável pela emissão do atestado;
- Devem ser originais ou autenticados, se cópias, e legíveis;

8.1.5. No caso de apresentação de atestado de empresas privadas, não serão considerados aqueles apresentados por empresas participantes do mesmo grupo empresarial da **CONTRATADA**. Serão consideradas como de mesmo grupo, empresas controladas pela **CONTRATADA** , ou que tenham pelo menos uma pessoa física ou jurídica que seja sócia da empresa emitente e da **CONTRATADA** .

8.1.6. Será aceito o somatório de atestados para comprovar a capacidade técnica e operacional, desde que reste demonstrada a execução concomitante dos contratos

9. DO CRITERIO DE JUGALMENTO DAS PROPOSTAS:

9.1. Atendidos todos os requisitos estabelecidos neste Elemento Técnico, será **CONTRATADA** a empresa que apresentar o **MENOR PREÇO POR LOTE** e atenda as qualificações

deste instrumento, nos termos do Regulamento de Compras e Contratações do IGESDF.

10.

Brasília/DF, 12 de maio de 2023.

Identificação do Responsável pela elaboração do Elemento Técnico nº 04/2023

THIAGO DE LACERDA CHAVES

Chefe do Núcleo de Rede

00012361

ANDERSON JESUS DE MENEZES

Gerente de Tecnologia da Informação e Comunicação

00014066

GUSTAVO MAGNO DA CRUZ

Gerência Geral de Logística de Serviços

12039

Na atribuição de autoridade imediata superior responsável pela Superintendência de Tecnologia da Informação, APROVO e AUTORIZO o presente Elemento Técnico, conforme preconiza o Regulamento Próprio de Compras e Contratações do IGESDF.

ANTONIO CARLOS GARCIA MARTINS CHAVES

Diretoria de Administração e Logística

00015119

CARLOS FERNANDO DAL SASSO DE OLIVEIRA

Superintendente da Unidade Central de Administração

00012037

11. **ANEXO I - LOTE 1- IAAS - SERVIÇO DE NUVEM PÚBLICA**

11.1. Todos os itens relacionados no **Lote 1: IaaS - Serviço de Nuvem Pública,** somente serão executados sob demanda da **CONTRATANTE**, podendo ser descontinuados a qualquer momento pela **CONTREATANTE**

LOTE	ITEM	Subitem	Tipo de Instancia	Métrica	USN (Previsto)	Valor Unitário	Valor Mensal previsto	Valor Anual previsto	Valor previsto para 30 meses
			Instancia - 1 (Linux) com 1 vCPU e 2 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 2 (Linux) com 2 vCPU e 4 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 3 (Linux)						

			com 4 vCPU e 8 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 4 (Linux) com 4 vCPU e 16 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 5 (Linux) com 8 vCPU e 32 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 6 (Linux) com 16 vCPU e 64 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 7 (Linux) com 32 vCPU e 64 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 8 (Linux) com 32 vCPU e 128 GB de memória RAM (por demanda)			R$	R$	R$	R$
		1.1	Instancia - 9 (Windows) com 1 vCPU e 2 GB de memória RAM (por demanda)	Instancia/Mês	1.500.000	R$	R$	R$	R$
			Instancia - 10 (Windows) com 2 vCPU e 4 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 11 (Windows) com 2 vCPU e 8 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 12 (Windows) com 4 vCPU e 16 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 13 (Windows) com 8 vCPU e 32 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 14 (Windows) com 16 vCPU e 64 GB de memória RAM (por demanda)			R$	R$	R$	R$
1	IaaS - Nuvem Pública		Instancia - 15 (Windows) com 32 vCPU e 64 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 16(Windows) com 32						

			vCPU e 128 GB de memória RAM (por demanda)			R$	R$	R$	R$
		Subitem	**Descrição**	**Métrica**	**QNTD. (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
		1.2	Serviço de Storage Block-Level SSD (por demanda)	TB/Mês	100	R$	R$	R$	R$
		1.3	Serviço de Storage Block-Level HDD (por demanda)	TB/Mês	100	R$	R$	R$	R$
		1.4	Serviço de Storage File-Level (por demanda)	TB/Mês	50	R$	R$	R$	R$
		1.5	Serviço de backup e restore (por demanda)	Mensal	200	R$	R$	R$	R$
		1.6	Balanceamento de carga (por demanda)	Unidade/Mês	20	R$	R$	R$	R$
		1.7	Porta de conexão de fibra 1 GBPS (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		1.8	Porta de conexão de fibra 10 gbps (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		1.9	Serviço de Tráfego de Saída de Rede (por demanda)	Mensal	100	R$	R$	R$	R$
		1.10	Serviço de DNS (por demanda)	Mensal	100	R$	R$	R$	R$
		1.11	Serviço de VPN (por demanda)	Unidade/Mês	20	R$	R$	R$	R$
		1.12	Serviço de Web Application Firewall (por demanda)	Unidade/Mês	200	R$	R$	R$	R$
		1.13	Serviço de Autenticação Integrado com AD (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		1.14	Serviço de Monitoramento (por demanda)	Unidade/Mês	1	R$	R$	R$	R$
		1.15	Serviços Especializados de Nuvem Pública (por demanda)	Hora	4.000	R$	R$	R$	R$

11.2. **Especificação para o Subitem 1.1 - Instancia (por demanda):**

11.2.1. A **CONTRATADA** atuará como representante (integrador) de um provedor de serviços de computação em nuvem (doravante denominado provedor), em conformidade com as características básicas e definições dispostas neste Elemento Técnico, que atenda todos os itens deste Elemento

Técnico, disponibilizando-os à **CONTRATANTE**.

11.2.2. Todos os serviços apresentados neste Elemento Técnico, somente serão aceitos se forem parte da lista de serviços da nuvem do provedor oferecido pela **CONTRATADA**, devendo ser contabilizados por meio de USNs . (unidade de serviço em nuvem). Não serão aceitas provisões de serviços por meio de instalação de software ou máquinas virtuais para a sua prestação, caso esses serviços não integrem o conjunto de soluções oferecidas no catálogo da nuvem ofertada e não possam ser contabilizados diretamente pelo provedor.

11.2.3. A **CONTRATADA** deverá disponibilizar uma conta no provedor em nome da **CONTRATANTE**, por meio da qual serão provisionados os serviços descritos no **Lote 1- Serviço de Nuvem Pública** deste Elemento Técnico.

11.2.4. Esta conta deverá permitir que a **CONTRATANTE** delegue à **CONTRATADA** o acesso aos recursos em nuvem disponíveis para execução dos serviços técnicos especializados descritos na neste Elemento Técnico.

11.2.5. A dinâmica do processo inclui etapas de registro da demanda, análise e definição dos cenários apropriados, aprovação pela **CONTRATANTE**, execução dos procedimentos de configuração, migração/implantação, testes, homologação da **CONTRATANTE**, colocação em produção, acompanhamento, bilhetagem e faturamento dos serviços mensalmente.

11.2.6. Os serviços de computação em nuvem oferecidos serão adquiridos por meio de Unidades de Serviço em Nuvem (USN), que servirá como base para aquisição de serviços do provedor.

11.2.7. A USN visa estabelecer-se como método previsível, linear e flexível para obtenção de uma quantidade objetivamente definida a ser cobrada pelos serviços de computação em nuvem. A métrica de USN consiste no estabelecimento de valor de referência específico para cada tipo de serviço de nuvem, conforme métrica individual associada ao consumo dos recursos.

11.2.8. O valor de referência de USN será dimensionado utilizando-se como referência valores apresentados pelo mercado na fase de cotação de preços.

11.2.9. A **CONTRATANTE** fará uso e efetuará o pagamento apenas das USNs relativas aos serviços solicitados à **CONTRATADA**, até o limite máximo das USNs estimadas.

11.2.10. O provedor disponibilizado pela **CONTRATADA** deverá fornecer todos os serviços listados na Tabela de Quantidades, de acordo com as descrições e níveis mínimos de serviço respectivos.

11.2.11. Os serviços descritos na Tabela de Quantidades deverão ser executados em território nacional, o que inclui armazenar os dados e informações da **CONTRATANTE** em datacenters instalados fisicamente no Brasil, incluindo replicação e cópias de segurança (backups), conforme disposto na Norma Complementar nº 14/IN01/DSIC/SCS/GSIPR, de modo que a **CONTRATANTE** disponha de todas as garantias da legislação brasileira enquanto tomadora do serviço e responsável pela guarda das informações armazenadas em nuvem.

11.2.12. Deverá ser disponibilizado pela **CONTRATADA** um portal contendo informações sobre:

a) Planilha de preços: valores praticados pela **CONTRATADA** com os preços de todos os serviços (em USN); informar também quais serviços do provedor são gratuitos;

b) Relatório de Faturamento: relatórios com consumo de serviços do provedor;

c) Informações sobre o contrato: detalhamento do contrato, tipos de serviços;

d) Relatórios de avaliação de otimização e performance, contendo sugestões de melhorias, ajustes em diversos aspectos da infraestrutura;

11.2.13. Os relatórios deverão ser disponibilizados pelo portal, com periodicidade diária, semanal ou mensal, a depender das características do serviço ou recurso avaliado, abrangendo aqueles listados na Tabela 1 deste Elemento Técnico. O serviço estará dentro das responsabilidades da CONTRATADA, não sendo cobrado como serviço adicional.

11.2.14. O provedor de nuvem deve disponibilizar, no mínimo, os seguintes sistemas operacionais e bancos de dados, nas suas versões estáveis; os quais deverão suportar ser instalados nas máquinas virtuais:

a) Windows 10 ou superior

b) Windows Server 2019 ou superior;

c) RHEL, CENTOS, Alma Linux e Rocky Linux, Debian, Ubuntu e SuSe;

d) MySQL Server, SQL Server e PostgreSQL (versões atuais);

11.2.15. O provedor deve prover serviços de autoscaling, permitindo que soluções tenham acesso automático a maior quantidade de recursos computacionais, em função da demanda.

11.2.16. Níveis mínimos de serviços (NMS) são critérios objetivos e mensuráveis estabelecidos com a finalidade de aferir e avaliar fatores como qualidade, desempenho e disponibilidade dos serviços. O NMS de **disponibilidade das instâncias deve ser igual ou superior a 99,80%** para cada período de 1 mês.

11.2.17. A **CONTRATADA** deve oferecer calculadora ou simulador público de preços para cada **item 1.1** deste Elemento Técnico para o provedor que integra a solução.

11.2.18. A **CONTRATANTE** poderá solicitar ativação de serviços de computação em nuvem contratados, quando couber e for tecnicamente viável, para aplicações publicadas na internet que estejam sob a sua gestão e que estejam em ambiente diverso dos ambientes do provedor.

11.2.19. Todos os dados decorrentes de serviços solicitados pela **CONTRATANTE** à **CONTRATADA** e operacionalizados no provedor serão de propriedade apenas da **CONTRATANTE**, a quem deverá ser assegurado acesso irrestrito a qualquer momento do contrato. Durante todo o contrato, e particularmente ao final desse, independente da razão que tenha motivado o seu término, a **CONTRATADA** repassará à **CONTRATANTE** todas as informações necessárias à continuidade da operação dos serviços em nuvem.

11.2.20. A **CONTRATADA** deverá fornecer, mediante solicitação da **CONTRATANTE**, backup das aplicações, dados e scripts de configuração que estiverem disponíveis em nuvem, o que inclui as imagens das máquinas virtuais de aplicação, cópias dos dados armazenados em dispositivos de armazenamento em nuvem, cópias dos bancos de dados que fazem parte das topologias das aplicações da **CONTRATANTE** provisionadas em nuvem ou que fazem parte de topologias híbridas de aplicações.

11.2.21. Disponibilizar infraestrutura em nuvem para alocação de servidores virtuais executando sistemas operacionais Windows 10 ou superior, Windows Server 2019 ou superior e/ou Linux e espaço de armazenamento em nuvem.

11.2.22. O **CONTRATANTE** poderá a qualquer momento provisionar novos servidores virtuais no ambiente em nuvem da **CONTRATADA**, bem como desligar servidores virtuais existentes, sendo tarifado apenas quando os servidores estiverem ligados;

11.2.23. Para cada servidor provisionado deverá estar disponível uma área de no mínimo 200 GB de disco para carregar o sistema operacional da Instância Virtual (disco de boot) sem ônus para a **CONTRATANTE**;

11.2.24. Cada Instância Virtual poderá ter os seguintes sistemas operacionais:

a) Windows 10 ou superior

b) Windows Server 2019 ou superior;

c) RHEL, CENTOS, Alma Linux e Rocky Linux, Debian, Ubuntu e SuSe;

d) MySQL Server, SQL Server e PostgreSQL (versões atuais);

11.3. **Especificação do subitem 1.2 – Serviço de Storage Block-Level SSD** (por demanda)**:**

11.3.1. Serviço para utilização de volume de armazenamento block-level.

11.3.2. Deverá possibilitar que o volume criado seja anexado às máquinas virtuais e reconhecido pelo SO como um dispositivo físico e local.

11.3.3. Deverá ser baseado em discos de estado sólido (SSD).

11.3.4. Deverá possuir função de criptografia do volume com mudança de chave gerenciada pelo próprio provedor ou pela **CONTRATANTE**.

11.3.5. A CONTRATADA deve informar o desempenho mínimo, em IOPS e MiB/s, para o volume provisionado.

11.3.6. O desempenho informado pela **CONTRATADA** para o volume provisionado deve se manter ao longo do contrato, podendo ser comprovado por meio de benchmark definido a critério da **CONTRATANTE**.

11.3.7. Serviço para utilização de volume de armazenamento de objetos.

11.3.8. Deverá ser durável, escalável e seguro.

11.3.9. Deverá possuir recurso de versionamento.

11.3.10. Deverá possuir interface web para inclusão e consultas de informações.

11.3.11. Deverá possuir API para upload de arquivos via aplicações desenvolvidas por terceiros.

11.4. **Especificação do subitem 1.3 – Serviço de Storage Block-Level HDD** (por demanda)**:**

11.4.1. Serviço para utilização de volume de armazenamento block-level.

11.4.2. Deverá possibilitar que o volume criado seja anexado às máquinas virtuais e reconhecido pelo SO como um dispositivo físico e local.

11.4.3. Deverá ser baseado em discos de estado sólido (HDD).

11.4.4. Deverá possuir função de criptografia do volume com mudança de chave gerenciada pelo próprio provedor ou pela **CONTRATANTE**.

11.4.5. A CONTRATADA deve informar o desempenho mínimo, em IOPS e MiB/s, para o volume provisionado.

11.4.6. O desempenho informado pela **CONTRATADA** para o volume provisionado deve se manter ao longo do contrato, podendo ser comprovado por meio de benchmark definido a critério da **CONTRATANTE**.

11.4.7. Serviço para utilização de volume de armazenamento de objetos.

11.4.8. Deverá ser durável, escalável e seguro.

11.4.9. Deverá possuir recurso de versionamento.

11.4.10. Deverá possuir interface web para inclusão e consultas de informações.

11.4.11. Deverá possuir API para upload de arquivos via aplicações desenvolvidas por terceiros.

11.5. **Especificação do subitem 1.4 – Serviço de Storage File-Level HDD** (por demanda)**:**

11.5.1. Serviço para utilização de volume de armazenamento file-level.

11.5.2. Deverá possibilitar que o volume criado seja anexado às máquinas virtuais como área de rede.

11.5.3. Deverá ser baseado em discos de estado sólido (HDD).

11.5.4. Deverá possuir função de criptografia do volume com mudança de chave gerenciada pelo próprio provedor ou pela **CONTRATANTE**.

11.5.5. Deverá possuir função de desduplicação e compressão de dados.

11.5.6. Deverá suportar NFS e SMB;

11.5.7. Deverá suportar snapshot e clones point-in-time;

11.5.8. O desempenho informado pela **CONTRATADA** para o volume provisionado deve se manter ao longo do contrato, podendo ser comprovado por meio de benchmark definido a critério da **CONTRATANTE**.

11.5.9. Serviço para utilização de volume de armazenamento de objetos.

11.5.10. Deverá ser durável, escalável e seguro.

11.5.11. Deverá possuir recurso de versionamento.

11.5.12. Deverá possuir interface web para inclusão e consultas de informações.

11.5.13. Deverá possuir API para upload de arquivos via aplicações desenvolvidas por terceiros

11.6. **Especificação Subitem 1.5 - Serviço de Backup e Restore** (por demanda):

11.6.1. Serviço para fornecer backup (ou proteção) e restauração de dados na nuvem;

11.6.2. Deverá alocar e gerenciar automaticamente o armazenamento de backup;

11.6.3. Deverá permitir a transmissão segura e o armazenamento dos dados criptografados;

11.6.4. Deverá fornecer backups consistentes, garantindo que correções adicionais não sejam necessárias para restaurar os dados;

11.6.5. Deverá suportar backup full, incremental e diferencial durante vigência do contrato;

11.6.6. Deverá permitir transferência de dados ilimitada, tanto para backup quanto para restore;

11.6.7. Deverá fornecer sistema de alertas para falhas no processo de backup, ou consistência dos arquivos;

11.6.8. Serviço com possibilidade de armazenamento heterogêneo, local ou em nuvem, de cópias de segurança;

11.6.9. O serviço de armazenamento de Backup em nuvem, deve prover escalabilidade e

proporcionar alta disponibilidade, sem necessidade de manutenção ou sobrecarga de monitoramento;

11.6.10. Os dados devem ser persistidos com redundância, de no mínimo 1 cópias dos dados em equipamentos de hardware diferentes, de forma a prevenir perda de dados com falhas de hardware;

11.6.11. Deverá permitir retenção de dados por período indeterminado;

11.6.12. Deverá permitir a criptografia dos dados.

11.6.13. O serviço deve possuir um software de gerenciamento no qual podem ser configurados diversos perfis de backup, incluindo pastas, data e hora que devem ser realizados os backups. Deve possibilitar a instalação em mais de um computador (sem limites) e ter suporte aos sistemas operacionais (Linux e Windows).

11.6.14. O sistema deve permitir o backup de arquivos com nomes longos (maiores que 255 caracteres) incluindo caracteres especiais. Além disso, deve permitir o backup de arquivos em uso através do recurso de cópias de sombras do Windows

11.6.15. Deve possuir gerência única para realizar de ambiente em nuvem híbrida, local e nuvem.

11.6.16. Deve suportar para MongoDB.

11.6.17. Deve suportar point-in-time backup para: Oracle, SQLServer e Postgree.

11.6.18. Deve suportar Docker

11.6.19. A **CONTRATADA**tem obrigação de monitorar os serviços de backup, verificando e corrigindo qualquer erro que possa surgir durante o backup, pelo menos uma vez ao dia. O sistema deve enviar e-mail para o cliente com o resultado detalhado de cada backup realizado

11.6.20. A empresa deverá ter um suporte disponível 24x7x365

11.7. **Especificação Subitem 1.6 - Balanceamento de Carga** (por demanda**):**

11.7.1. Serviço de transmissão de dados do Balanceador de Carga;

11.7.2. Serviço para utilização de balanceador de carga, que distribuirá o tráfego de entrada para as máquinas virtuais.

11.7.3. Deverá permitir que a carga seja balanceada entre máquinas virtuais que estejam em locais físicos distintos

11.7.4. Deverá ser escalável, de maneira a crescer ou diminuir seu poder de processamento, em função do fluxo de dados que por ele trafegar.

11.7.5. Deverá possibilitar a utilização de HTTP, HTTPS e TCP para efetuar o balanceamento de carga, bem como a realização de health check nas máquinas virtuais por meio dos mesmos protocolos.

11.7.6. Serviço para controlar a distribuição do tráfego do usuário para pontos de extremidade da aplicação;

11.7.7. Deverá fornecer failover automático quando um ponto de extremidade ficar inativo;

11.7.8. Deverá permitir a melhora da capacidade de resposta do aplicativo direcionando o tráfego para o ponto de extremidade com a menor latência de rede para o cliente;

11.7.9. Deverá permitir operações de manutenção planejada nas aplicações sem tempo de inatividade;

11.7.10. Deverá suportar o tráfego para pontos de extremidade externos de outras nuvens, habilitando seu uso com implantações locais, inclusive de nuvem híbrida.

11.8. **Especificações Subitem 1.7 – Porta de Conexão de Fibra 1 GBPS** (por demanda):

11.8.1. Serviço de conexão de fibra dedicada entre a infraestrutura de rede local da **CONTRATANTE** e uma porta de interface do provedor, visando à interconexão segura e rápida entre os dois, sem tráfego pela internet.

11.8.2. A porta do provedor deverá estar localizada em território nacional.

11.8.3. Velocidade de no mínimo 1 GBits/s;

11.8.4. Todos os custos de conexão da **CONTRATANTE** até a porta de conexão do provedor serão de responsabilidade da **CONTRATANTE**.

11.9. **Especificações Subitem 1.8 – Porta de Conexão de Fibra 10 GBPS** (por demanda):

11.9.1. Serviço de conexão de fibra dedicada entre a infraestrutura de rede local da **CONTRATANTE** e uma porta de interface do provedor, visando à interconexão segura e rápida entre os dois, sem tráfego pela internet.

11.9.2. A porta do provedor deverá estar localizada em território nacional.

11.9.3. Velocidade de no mínimo 10 GBits/s;

11.9.4. Todos os custos de conexão da **CONTRATANTE** até a porta de conexão do provedor serão de responsabilidade da **CONTRATANTE**.

11.9.5. **Especificações Subitem 1.9 – Tráfego de Saída de Rede (por demanda):**

11.9.5.1. Serviço de transmissão de dados de saída da rede.

11.9.5.2. Nenhum tráfego de entrada para a rede será cobrado.

11.9.5.3. Serviço de atribuição de endereço IP público (estático ou dinâmico), dedicado, até que seja liberado pela **CONTRATADA** a pedido da **CONTRATANTE**, ou no caso de ser dinâmico, até que o recurso seja desligado.

11.10. **Especificação Subitem 1.10 – Serviço de DNS** (por demanda):

11.10.1. O Serviço consiste em um espaço de gerenciamento no qual é possível criar, editar, alterar e excluir entradas no DNS. Cada zona DNS representa um limite de autoridade sujeito à gestão por determinadas entidades.

11.10.2. O Serviço consiste em realizar consultas DNS que representa a ação de um host buscar um registro específico que está exposto na zona DNS. Para realizar essa consulta o host percorre toda a árvore hierárquica até achar o registro específico.

11.10.3. Deverá ser possível realizar buscas nos registros disponíveis, quais sejam do tipo A, AAAA, CNAME, MX, PTR, NS, SOA, SRV e TXT, sendo cada um específico para cada finalidade.

11.11. **Especificação Subitem 1.11 - Serviço de VPN** (por demanda):

11.11.1. Serviço para uso de Rede Privada Virtual (Virtual Private Network – VPN);

11.11.2. O serviço será contratado usando a métrica de GB trafegado por mês;

11.11.3. Deve permitir a criação de conexões site-to-site e client-to-site para a mesma VPN e fornecer scripts e/ou software para a criação dessas conexões;

11.11.4. Somente o tráfego de saída será contabilizado para cobrança do serviço;

11.11.5. O tráfego de saída para o serviço de VPN não se confunde nem poderá ser cobrado em duplicidade com o tráfego de saída de rede descrito no **item 11.9**

11.11.6. O tráfego de dados através da conexão deve ser por túnel VPN utilizando o protocolo IPSec;

11.11.7. A taxa de transferência mínima na conexão VPN deve ser de 1000 Gbps, podendo, entretanto, ser inferior quando limitada pela capacidade da conexão (link de dados) da **CONTRATANTE**.

11.11.8. A **CONTRATADA** deverá prover um gateway de VPN para a rede da **CONTRATANTE**;

11.11.9. Possibilitar o envio do tráfego criptografado em uma conexão pública;

11.11.10. Permitir a criação de VPN conforme descrito no Serviço de VPN;

11.12. **Especificação Subitem 1.12 - Web Aplication Firewall (WAF)** (por demanda)

11.12.1. A implantação, configuração, gerenciamento, monitoramento dos serviços ofertados e manutenção e suporte da solução deverão ser realizados pela **CONTRATADA**.

11.12.2. É de responsabilidade da **CONTRATADA** todas as despesas com materiais, mão-de-obra, transportes, hospedagem, equipamentos, máquinas, impostos, seguros, taxas, tributos, incidências fiscais, trabalhistas, previdenciárias, salários, custos diretos e indiretos, encargos sociais e contribuições de qualquer natureza ou espécie, necessários à perfeita execução do objeto.

11.12.3. Quaisquer atualizações dos softwares das soluções deverão ser realizadas sem interrupções dos serviços WAF.

11.12.4. É de responsabilidade da **CONTRATADA** o fornecimento dos serviços de suporte técnico

especializado de primeiro, segundo e terceiro nível para o ambiente contratado, inclusive de forma presencial quando este for necessário para o atendimento dos chamados e/ou normalização do ambiente.

11.12.5. Entende-se por suporte técnico, mas não se limitando a, toda ação necessária da **CONTRATADA** para a normalização dos serviços WAF, solicitações da **CONTRATANTE** para a realização de configurações no ambiente WAF, criação e exclusão de regras e políticas de segurança entre outras que se fizerem necessárias na solução.

11.12.6. Em situações que forem identificadas como origem do incidente falhas nos links de comunicação e estes serem causados por contratos da **CONTRATANTE** com outras empresas, a **CONTRATANTE** deverá realizar o acionamento e acompanhamento do suporte técnico da referida empresa fornecedora do link afetado, para que esta realize a normalização dos seus serviços.

11.12.7. Todos os chamados, sejam abertos pela **CONTRATANTE** ou pela **CONTRATADA** de forma proativa e/ou reativa, deverão ser registrados em ferramenta para este fim, a qual deverá possibilitar a extração das informações de acordo com os relatórios exigidos mensalmente.

11.12.8. Os chamados abertos pelo **CONTRATANTE** serão referentes às atividades sob responsabilidade da **CONTRATADA**, englobando: instalação, configuração, recuperação, alteração e remoção de equipamentos, configurações na solução WAF, endereçamento IP, SNMP, organização e atualização da gerência e considerando-se todos os serviços contratados de maneira a assegurar a integridade, a qualidade e desempenho dos serviços dentro dos limites estabelecidos.

11.12.9. A **CONTRATADA** deverá manter atualizados no seu sistema de chamados as informações e status de andamento no atendimento dos incidentes/requisições.

11.12.10. Eventuais paradas na solução WAF, em qualquer nível, ou qualquer outra parada de responsabilidade da **CONTRATADA**, deverá ser comunicada tempestivamente a **CONTRATANTE** através de e-mail ou telefone(s) que possam garantir contato imediato a ser(em) informado(s) pela **CONTRATANTE**.

11.12.11. Todas as interrupções programadas deverão ser comunicadas ao **CONTRATANTE** com antecedência mínima de 5 (cinco) dias úteis, e deverão ser realizadas preferencialmente aos domingos e feriados, ou em data e horário pré-definidos pelo **CONTRATANTE**, de acordo com o fuso horário da localidade onde ocorrerá a interrupção. As paradas programadas deverão ser autorizadas pelo **CONTRATANTE** antes de sua execução.

11.12.12. O **CONTRATANTE** poderá solicitar de acordo com suas necessidades, a qualquer tempo, alteração nas configurações da solução WAF.

11.12.13. O **CONTRATANTE** poderá solicitar, a qualquer tempo, os dados, logs e demais informações armazenadas pela **CONTRATADA** em seu ambiente de gerência, rela vos ao projeto do **CONTRATANTE**.

11.12.14. Os dados e informações armazenados poderão ser solicitados pelo **CONTRATANTE**, a qualquer tempo à **CONTRATADA** que deverá disponibilizá-los no prazo máximo de 5 (cinco) dias úteis, em meio a ser definido pela **CONTRATANTE** e/ou na base de dados da solução de gerência (carga dos dados extraídos e removidos).

11.12.15. Serviço para fornecer proteção centralizada dos aplica vos Web, contra vulnerabilidades e eventuais ataques;

11.12.16. Deverá fornecer proteção sem modificar o código de back-end;

11.12.17. Deverá proteger vários aplica vos Web ao mesmo tempo por trás de um gateway de aplicativo;

11.12.18. Deverá fornecer monitoramento das aplicações Web contra-ataques usando um log em tempo real;

11.12.19. Deverá permitir personalização de regras e grupos de regras, a fim de atender as necessidades das aplicações e eliminar falsos positivos.

11.13. **Especificação Subitem 1.13 - Autenticação integração com AD** (por demanda):

11.13.1. Serviço para fornecer uma identidade comum para acesso aos recursos na nuvem;

11.13.2. Deverá sincronizar o serviço de diretório local com o serviço de diretório da nuvem.

11.13.3. Deverá garantir que as informações de identidade dos usuários e grupos locais correspondam às da nuvem;

11.13.4. Deverá permitir aos usuários alterar e redefinir suas senhas na nuvem e ter sua política de senha local aplicada;

11.13.5. Deverá permitir a escolha de quais objetos serão sincronizados.

11.14. **Especificação Subitem 1.14 – Serviço de Monitoramento** (por demanda):

11.14.1. A **CONTRATADA** deverá monitorar toda a infraestrutura disponibilizada em nuvem em regime de 24x7x365;

11.14.2. Deve ser disponibilizado a **CONTRATANTE** acesso WEB a plataforma de monitoramento utilizada pela **CONTRATADA**. Nesta plataforma, deve ser possível gerar relatórios de tráfego de dado, utilização de recursos, nível de serviço entre outros relatórios que podem ser solicitados sem ônus a **CONTRATANTE**

11.14.3. A **CONTRATADA** deverá disponibilizar Plataforma WEB para registro e acompanhamentos dos chamados e SLA.

11.14.4. A **CONTRATADA** deverá disponibilizar Central de Serviços para registro e acompanhamento dos chamados técnicos da **CONTRATANTE;**

11.14.5. A **CONTRATADA** deverá tratar todos os eventos da infraestrutura e identificar quais eventos são incidentes;

11.14.6. A equipe de monitoramento deverá abrir chamados para todos os incidentes e indicar a resolução adotada em cada chamado;

11.14.7. A equipe de monitoramento deverá escalonar os chamados de incidentes que não tiverem procedimento padrão ou que não forem solucionados após a execução do procedimento padrão;

11.14.8. A **CONTRATANTE** irá indicar quais são os caminhos para escalonamento dos chamados.

11.15. **Especificações Subitem 1.15 – Serviços Especializados em Nuvem Pública** (por demanda):

11.15.1. Os serviços de especializados em Nuvem Pública serão demandados para a realização de todas as atividades referentes a disponibilização de serviços na nuvem contratada;

11.15.2. Serão incluídos nesse serviço as seguintes atividades:

a) Planejamento de migração de servidores e/ou serviços e/ou dados para a nuvem pública;

b) Preparação do ambiente da nuvem pública para receber servidores e/ou serviços e/ou dados da **CONTRATANTE**;

c) Instalação, configuração e suporte técnico de ferramenta(s) para orquestração dos serviços entre as nuvens privada e pública;

d) Serviços sobre o uso dos recursos da nuvem privada;

e) Serviços de tunning, ajustes, correção de falhas, detecção de problemas na infraestrutura de nuvem pública;

11.16. **Níveis de Serviço para Serviços Especializados em Nuvem Pública:**

11.16.1. A **CONTRATADA** deve prestar um serviço de qualidade. Para tanto, são estabelecidas nesse Elemento Técnico metas para os serviços prestados. Os serviços serão medidos com base em indicadores de níveis de serviço específicos.

11.16.2. A apuração dos indicadores relativos ao tempo de atendimento dos Chamados será calculada sempre com base na data e hora de registro inicial e final dos Chamados. No cálculo serão desconsiderados os períodos em que os Chamados estiveram suspensos mediante a aprovação da **CONTRATANTE** ou não estiveram sob a responsabilidade da **CONTRATADA**.

11.16.3. A **CONTRATADA**, deve manter atualizado os Chamados abertos e que forem de responsabilidade de terceiros com as seguintes informações: nome de quem está atuando na tratativa e prazo de solução.

11.16.4. Quando não forem atingidos os níveis de serviços exigidos em contrato, a **CONTRATANTE** aplicará um redutor na fatura dos serviços (glosa), de forma a retratar que a qualidade dos serviços recebidos não foi de acordo com a qualidade exigida em contrato.

11.16.5. As glosas serão calculadas e aplicadas sobre o valor total da Ordem de Serviço que não atingiu a meta exigida.

11.16.6. A **CONTRATADA** só poderá faturar os serviços executados após o fechamento dos relatórios de serviços do mês e a correta aplicação das glosas devidas. A nota fiscal deve ser emitida já com o valor de glosa aplicado.

11.16.7. Tabela de níveis de serviço:

Indicadores de nível de serviço/mês	Unidade de medida	Meta exigida	Glosa aplicável
Revisão da Ordem de Serviço	Horas	24 horas após a solicitação formal	0,1% + (0,1% para cada 24horas acima negociado)
Resolução da Ordem de Serviço	Prazo negociado	Prazo negociado (1)	0,5% + (0,1% para cada dia acima do negociado)
(1)Para cada Ordem de Serviço em que o prazo de 24 horas não seja atendido, será negociado o prazo de entrega de acordo com a complexidade da solicitação			

11.17. **Migração Obrigatório dos Serviços Atuais**

11.17.1. Os serviços de migração de infraestrutura On-Premises / Hyperconvergência / Cloud atuais serão obrigatórios a nova **CONTRATADA** sem custo para a **CONTRATANTE**.

11.17.2. Devem cumprir minimamente as seguintes etapas:

- Mapeamento do ambiente atual;
- Criação de um inventário de aplicações;
- Planejamento de migração;
- Teste da nova infraestrutura fornecida;
- Execução Migração e testes funcionais;

11.17.3. Os ativos e aplicações estarão disponíveis em tempo de vistoria ao ambiente do IGESDF anterior ao pregão.

11.18. **Manutenção e suporte Tecnico**:

11.18.1. A Manutenção E Suporte Técnico referente a prestação de serviços de Nuvem Pública devem estar de acordo com o especificado neste item.

11.18.1.1. O suporte e a manutenção deverão ser providos durante toda vigência do contrato.

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

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

11.18.1.4. A **CONTRATADA** deve ser emitido relatório mensal referente a atualização 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.

11.18.1.5. 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.

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

11.18.1.7. A **CONTRATADA**, deverá utilizar a ferramenta de ITSM própria, para registro de chamados e relatórios.

11.18.1.8. Todo chamado registrado, deve ser enviado notificação de forma automática aos fiscais do contrato.

11.18.1.9. Para finalizar os chamados registrados devem ser inseridos os registros das tratativas

adotadas.

11.18.1.10. Todo e qualquer problema detectado nos itens/serviços descritos neste Elemento Técnico, deverão ser, de forma imediata, ser relatados à equipe de Fiscais do **CONTRATANTE**.

11.18.1.11. Todas as mudanças adotadas por iniciativa da **CONTRATADA** nas configurações

11.18.1.12. deverão ser efetuadas mediante aprovação do **CONTRATANTE**.

11.18.1.13. A CONTRATADA deverá emitir uma declaração prévia, com antecedência mínima de 15 (quinze) dias, 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.

11.18.1.14. O suporte deverá incluir resposta a chamados críticos em tempo inferior a sessenta minutos e permitir a comunicação por meio de e-mail, chat e 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.

11.18.1.15. Os serviços de Suporte Técnico compreendem todos os chamados rela vos aos itens referenciados neste 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**.

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

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

11.18.1.18. 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, com SLA de 20 minutos 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.

11.18.1.19. 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%

11.19. **Obrigações da Contratada:**

11.19.1. A **CONTRATADA** de prestar os serviços com pessoal adequadamente qualificado e capacitado para suas atividades.

11.19.2. Cumprir rigorosamente todas as programações e atividades do objeto do contrato.

11.19.3. Prestar os serviços de acordo com o especificado neste instrumento.

11.19.4. 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.

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

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

11.19.7. 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.

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

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

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

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

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

11.19.13. 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.

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

11.19.15. 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.

11.19.16. 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.

11.19.17. 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.

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

12. ANEXO II: LOTE 2 - SAAS - SERVIÇO DE NEXT GENERATION FIREWALL

12.20. Todos os itens relacionados no **Lote 2: SaaS - Serviço de Next Generation Firewall ,** somente serão executados sob demanda da **CONTRATANTE**, podendo ser descontinuados a qualquer momento pela **CONTREATANTE**

LOTE	ITEM	Subitem	Descrição	Métrica	QNTD (Previsto)	Valor Unitário	Valor Mensal previsto	Valor Anual previsto	Valor previsto para 30 meses
2	SaaS - Serviço de Next Generation Firewall	2.1	Serviço Next Generation Firewall do TIPO 1 (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		2.2	Serviço Next Generation Firewall do TIPO 2 (por demanda)	Unidade/Mês	20	R$	R$	R$	R$

12.21. **Especificações Subitem 2.1 – Serviço Next Generation Firewall do TIPO 1 (por demanda):**

12.21.1. 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.

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

12.21.3. 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.

12.21.4. 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.

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

12.21.6. Deve possuir firewall com capacidade mínima de processamento de 100 (cem) Gbps.

12.21.7. Deve possuir IPS com capacidade mínima de processamento de 14 (quatorze) Gbps.

12.21.8. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 10 (dez) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.

12.21.9. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 8 (oito) Gbps.

12.21.10. Deve possuir VPN com capacidade mínima de, pelo menos, 55 (cinquenta) Gbps de tráfego IPSec.

12.21.11. Deve suportar no mínimo 8.000.000 (oito milhões) conexões simultâneas.

12.21.12. Deverão ser licenciados para suportar, pelo menos, 10.000 (dez mil) usuários de VPN SSL.

12.21.13. Deve suportar, pelo menos, 450.000 (quatrocentos e cinquenta mil) novas conexões por segundo.

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

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

12.21.16. Deve possuir, pelo menos, 8 (oito) interfaces RJ 45.

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

12.21.18. Deve possuir, pelo menos, 4 (quatro) interfaces 10 Gigabit SFP+.

12.21.19. Deve incluir licença para a funcionalidade de VPN SSL.

12.21.20. Deve estar licenciado para 10 instâncias de firewalls virtuais.

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

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

12.22. **Especificações Subitem 2.2 – Serviço Next Generation Firewall do TIPO 2 (por demanda):**

12.22.1. 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.

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

12.22.3. 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.

12.22.4. 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.

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

12.22.6. Deve possuir firewall com capacidade mínima de processamento de 3 (tres) Gbps.

12.22.7. Deve possuir IPS com capacidade mínima de processamento de 1 (hum) Gbps.

12.22.8. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 370 (trezentos e setenta) Mbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.

12.22.9. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 620 (seiscentos e vinte) Mbps.

12.22.10. Deve possuir VPN com capacidade mínima de, pelo menos, 4 (quatro) Gbps de tráfego IPSec.

12.22.11. Deve suportar 700.000 (setecentos mil) conexões simultâneas.

12.22.12. Deverão ser licenciados para suportar, pelo menos, 150 (cento e cinquenta) usuários de VPN SSL.

12.22.13. Deve suportar, pelo menos, 30.000 (trinta mil) novas conexões por segundo.

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

12.22.15. Deve suportar, pelo menos, 450 (quatrocentos e cinquenta) túneis de VPN Client-Site.

12.22.16. Deve possuir, pelo menos, 10 (oito) interfaces RJ 45.

12.22.17. Deve incluir licença para a funcionalidade de VPN SSL.

12.22.18. Deve estar licenciado para 10 instâncias de firewalls virtuais.

12.22.19. Deve possuir armazenamento interno de no mínimo 64 (sessenta e quatro) GB

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

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

12.23. **REQUISITOS GERAIS DE FUNCIONALIDADES E LICENCIAMENTOS COMUNS para NGFW do TIPO 1 e TIPO 2:**

12.23.1. **Funcionalidades de Firewall:**

12.23.1.1. Deve possuir controle de acesso à internet por endereço IP de origem e destino;

12.23.1.2. Deve possuir controle de acesso à internet por sub rede;

12.23.1.3. Deve suportar tags de VLAN (802.1q);

12.23.1.4. Deve possuir ferramenta de diagnóstico do tipo tcpdump;

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

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

12.23.1.7. Deve suportar single-sign-on para Active Directory, RADIUS;

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

12.23.1.9. 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;

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

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

12.23.1.12. Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

12.23.1.13. Deve suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

12.23.1.14. Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;

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

12.23.1.16. Deve possuir tecnologia de firewall do tipo Statefull;

12.23.1.17. 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;

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

12.23.1.19. Deve suportar PBR – Policy Based Routing;

12.23.1.20. Deve permitir a criação de VLANS no padrão IEEE 802.1q;

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

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

12.23.1.23. Deve permitir forwarding de camada 2 para protocolos não IP;

12.23.1.24. Deve suportar forwarding multicast;

12.23.1.25. Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;

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

12.23.1.27. Deve permitir o agrupamento de serviços;

12.23.1.28. Deve permitir o filtro de pacotes sem a utilização de NAT;

12.23.1.29. Deve permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

12.23.1.30. Deve possuir mecanismo de anti-spoofing;

12.23.1.31. Deve permitir criação de regras definidas pelo usuário;

12.23.1.32. Deve permitir o serviço de autenticação para tráfego HTTP e FTP;

12.23.1.33. 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;

12.23.1.34. Deve possuir a funcionalidade de balanceamento e contingência de links;

12.23.1.35. Deve suportar sFlow;

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

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

Linux e Windows;

12.23.1.38. 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;

12.23.1.39. Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

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

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

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

12.23.1.43. 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;

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

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

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

12.23.2. **FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO**

12.23.2.1. 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;

12.23.2.2. Deve permitir modificação de valores DSCP para o DiffServ;

12.23.2.3. Deve permitir priorização de tráfego e suportar ToS;

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

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

12.23.2.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

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

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

12.23.2.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;

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

12.23.2.11. Deve ter a capacidade de permitir a criação de perfis de controle de banda específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows.

12.23.3. **FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY**

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

12.23.3.2. Deve possuir filtragem de e-mail por palavras chaves;

12.23.3.3. Deve permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;

12.23.3.4. Deve possuir, para a funcionalidade de anti-spam, o recurso de RBL;

12.23.3.5. Deve permitir a checagem de reputação da URL no corpo mensagem de correio

eletrônico;

12.23.3.6. Deve ter a capacidade de permitir a criação de perfis de anti-spam específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows.

12.23.4. **FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB**

12.23.4.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança;

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

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

12.23.4.4. Deve possuir a funcionalidade de cota de tempo de utilização por categoria;

12.23.4.5. 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;

12.23.4.6. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

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

12.23.4.8. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;

12.23.4.9. 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;

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

12.23.4.11. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

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

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

12.23.4.14. 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;

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

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

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

12.23.4.18. Deve filtrar o conteúdo baseado em categorias em tempo real;

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

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

12.23.4.21. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

12.23.4.22. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem;

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

12.23.4.24. Deve permitir o bloqueio de redirecionamento HTTP;

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

12.23.4.26. Deve possuir Proxy Explícito e Transparente;

12.23.4.27. Deve implementar roteamento WCCP e ICAP;

12.23.4.28. Deve ter a capacidade de permitir a criação de perfis de filtragem Web específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android,

Apple, Linux e Windows.

12.23.5. **FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO**

12.23.5.1. 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;

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

12.23.5.3. Deve estar orientado à proteção de redes;

12.23.5.4. Deve permitir funcionar em modo transparente, sniffer e router;

12.23.5.5. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

12.23.5.6. Deve permitir a criação de padrões de ataque manualmente;

12.23.5.7. Deve possuir integração à plataforma de segurança;

12.23.5.8. Deve possuir capacidade de remontagem de pacotes para identificação de ataques;

12.23.5.9. 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;

12.23.5.10. 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;

12.23.5.11. Deve ter a capacidade de permitir a criação de perfis de inspeção específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows;

12.23.5.12. Deve possuir mecanismos de detecção/proteção de ataques;

12.23.5.13. Deve possuir reconhecimento de padrões;

12.23.5.14. Deve possuir análise de protocolos;

12.23.5.15. Deve possuir detecção de anomalias;

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

12.23.5.17. Deve possuir proteção contra-ataques de Windows ou NetBios;

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

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

12.23.5.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;

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

12.23.5.22. Deve possuir métodos de notificação de detecção de ataques;

12.23.5.23. Deve possuir alarmes na console de administração;

12.23.5.24. Deve possuir alertas via correio eletrônico;

12.23.5.25. 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;

12.23.5.26. Deve ter a capacidade de resposta/logs ativa a ataques;

12.23.5.27. Deve prover a terminação de sessões via TCP resets;

12.23.5.28. Deve armazenar os logs de sessões;

12.23.5.29. Deve atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

12.23.5.30. Deve mitigar os efeitos dos ataques de negação de serviços;

12.23.5.31. Deve permitir a criação de assinaturas personalizadas;

12.23.5.32. Deve possuir filtros de ataques por anomalias;

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

12.23.5.34. Deve permitir filtros de anomalias de protocolos;

12.23.5.35. Deve suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

12.23.5.36. Deve suportar verificação de ataque na camada de aplicação;

12.23.5.37. Deve suportar verificação de tráfego em tempo real, via aceleração de hardware;

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

12.23.6. **FUNCIONALIDADE DE VPN**

12.23.6.1. Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

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

12.23.6.3. Deve possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;

12.23.6.4. Deve possuir suporte a VPN SSL;

12.23.6.5. Deve possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

12.23.6.6. 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;

12.23.6.7. Deve possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;

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

12.23.6.9. Deve permitir a arquitetura de VPN hub and spoke;

12.23.6.10. 3Deve possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

12.23.6.11. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

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

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

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

12.23.6.15. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

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

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

12.23.6.18. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

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

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

12.23.6.21. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

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

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

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

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

12.23.6.26. Deve permitir criação de padrões de aplicação manualmente;

12.23.6.27. Deve ter a capacidade de permitir a criação de perfis de controle de aplicações específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows.

12.23.7. **FUNCIONALIDADE DE DLP (DATA LEAK PREVENTION)**

12.23.7.1. 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;

12.23.7.2. Deve inspecionar, no mínimo, os tráfegos de e-mail, HTTP;

12.23.7.3. Sobre o tráfego de e-mail, Deve inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;

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

12.23.7.5. Deve fazer a varredura no conteúdo de um cookie HTTP buscando por determinado texto;

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

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

12.23.7.8. Deve utilizar expressões regulares para composição das regras de verificação dos tráfegos;

12.23.7.9. 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;

12.23.7.10. 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;

12.23.7.11. 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.

12.23.8. **FUNCIONALIDADE DE BALANCEAMENTO DE CARGA**

12.23.8.1. Deve permitir a criação de endereços IPs virtuais;

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

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

12.23.8.4. 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;

12.23.8.5. Deve permitir persistência de sessão por cookie HTTP ou SSL session ID;

12.23.8.6. Deve permitir que seja mantido o IP de origem;

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

12.23.8.8. 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;

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

12.23.9. **FUNCIONALIDADE DE VIRTUALIZAÇÃO**

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

12.23.9.2. Deve permitir a criação de administradores independentes para cada uma das instâncias virtuais;

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

12.23.10. **FUNCIONALIDADE DE SD-WAN**

12.23.10.1. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

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

12.23.10.3. A solução SD-WAN deve suportar segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

12.23.10.4. 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.

12.23.10.5. Solução deve ser capaz de prover Zero Touch provisioning.

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

12.23.10.7. 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.

12.23.10.8. 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.

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

12.23.10.10. Reconhecimento em camada 7 totalmente segregado da camada 4.

12.23.10.11. 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.

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

12.23.10.13. 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)

12.23.10.14. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6

12.23.10.15. 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.

12.23.10.16. 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.

12.23.10.17. 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.

12.23.10.18. 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.

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

12.24. **Manutenção e suporte Tecnico para o Lote 2**:

12.24.1. A Manutenção E Suporte Técnico referente a prestação de serviços de Nuvem Pública devem estar de acordo com o especificado neste item.

12.24.2. O suporte e a manutenção deverão ser providos durante toda vigência do contrato.

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

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

12.24.5. A CONTRATADA deve ser emitido relatório mensal referente a atualização 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.

12.24.6. 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.

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

12.24.8. A CONTRATADA, deverá utilizar a ferramenta de ITSM própria, para registro de chamados e relatórios.

12.24.9. Todo chamado registrado, deve ser enviado notificação de forma automática aos fiscais do contrato.

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

12.24.11. Todo e qualquer problema detectado nos itens/serviços descritos neste Elemento Técnico, deverão ser, de forma imediata, ser relatados à equipe de Fiscais do **CONTRATANTE**.

12.24.12. Todas as mudanças adotadas por iniciativa da **CONTRATADA** nas configurações

12.24.13. deverão ser efetuadas mediante aprovação do **CONTRATANTE**.

12.24.14. A **CONTRATADA** deverá emitir uma declaração prévia, com antecedência mínima de 15 (quinze) dias, contendo:

12.24.14.1. Descrição do procedimento que será executado;

12.24.14.2. Cronograma de Atividades;

12.24.14.3. Impacto e eventuais procedimentos de contingência;

12.24.14.4. Bem como relatório posterior sobre os resultados obtido.

12.24.15. O suporte deverá incluir resposta a chamados críticos em tempo inferior a sessenta minutos e permitir a comunicação por meio de e-mail, chat e 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.

12.24.16. Os serviços de Suporte Técnico compreendem todos os chamados rela vos aos itens referenciados neste 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**.

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

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

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

12.24.19.1. **Criticidade Alta** - Deveremos entender como criticidade ALTA um serviço totalmente fora de operação, com SLA de 20 minutos para captura de chamado e início de atendimento, e até 04 horas para resolução do problema.

12.24.19.2. **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;

12.24.19.3. **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.

12.24.20. 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
	Deveremos entender como criticidade ALTA um	20 minutos	Até 04 horas para resolução	

Alta	entidade ALTA um serviço totalmente fora de operação	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 providencias equipamento reserva de falhas e este equipamento deverá estar disponível em ate 3 (três) dias corridos	2,0% por dia em atraso

12.25. **Obrigações da Contratada:**

12.25.1. A **CONTRATADA**de prestar os serviços com pessoal adequadamente qualificado e capacitado para suas atividades.

12.25.2. Cumprir rigorosamente todas as programações e atividades do objeto do contrato.

12.25.3. Prestar os serviços de acordo com o especificado neste instrumento.

12.25.4. 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.

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

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

12.25.7. 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.

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

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

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

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

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

12.25.13. 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.

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

12.25.15. 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.

12.25.16. **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.

12.25.17. 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.

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

13. ANEXO IIILOTE 3 – SAAS - SERVIÇO DE CONECTIVIDADE DE REDE E CONTROLE DE ACESSO

13.1. Todos os itens relacionados no **Lote 3: SaaS - Serviço de Conectividade e Controle de acesso,** somente serão executados sob demanda da **CONTRATANTE**, podendo ser descontinuados a qualquer momento pela **CONTREATANTE**

LOTE	ITEM	Subitem	Descrição	Métrica	QNTD (Previsto)	Valor Unitário	Valor Mensal previsto	Valor Anual previsto	Valor previsto para 30 meses
3	SaaS - Serviço de Conectividade e Controle de acesso	3.1	Serviço Conectividade de Rede – Tipo 1 (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		3.2	Serviço Conectividade de Rede – Tipo 2 (por demanda)	Unidade/Mês	90	R$	R$	R$	R$
		3.3	Serviço Conectividade de Rede – Tipo 3 (por demanda)	Unidade/Mês	60	R$	R$	R$	R$
		3.4	Serviço de Conectividade Sem Fio (por de manda)	Unidade/Mês	300	R$	R$	R$	R$
		3.5	Software de Controle de Acesso à Rede (por de manda)	Unidade/Mês	1	R$	R$	R$	R$

13.2. **Especificação para o Subitem 3.1 - Serviço Conectividade do Tipo 1 (por demanda):**

13.2.1. Disponibilização de um equipamento do tipo switch, devendo o mesmo ser instalado e configurado em rack existente nas dependências de cada unidade para a qual o serviço foi contratado, sem ônus adicionais para a **CONTRATANTE**.

13.2.2. Deverão estar inclusas quaisquer atividades secundárias como atualizações de versão, atualizações de segurança, manutenção e suporte técnico. A contratada deverá realizar a instalação e configuração da solução ofertada sem ônus adicionais para a **CONTRATANTE**.

13.2.3. O equipamento deve ser novo e estar em linha de produção, ou seja, sendo produzido pelo fabricante e com o firmware na última versão estável instalado;

13.2.4. Equipamento do tipo comutador de rede ethernet suportando operação em camada 3 do modelo OSI;

13.2.5. Deve possuir 48 (quarenta e oito) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE;

13.2.6. Adicionalmente, deve possuir 4 (quatro) slots QSFP28 para conexão de fibras ópticas operando com velocidades de 40 e 100 Gigabit Ethernet;

13.2.7. Deve permitir a configuração das interfaces QSFP28 para que operem com conexões do tipo "breakout" ou "split", modo em que uma determinada porta 40GbE pode operar com 4 conexões em 10GbE. Deve permitir ainda que as portas 100GbE sejam divididas em 4 conexões de 25GbE;

13.2.8. Deverá vir acompanhado de transceivers 10 Gb SFP+;

13.2.9. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

13.2.10. Deve possuir interface dedicada para gerenciamento local do tipo "out-of-band". Esta interface de gerenciamento deverá possuir porta 1000Base-T com conector RJ-45;

13.2.11. Deve possuir 1 (uma) interface USB;

13.2.12. Deve possuir capacidade de comutação de pelo menos 1.75 Tbps (terabits por segundo) e ser capaz de encaminhar até 1.5 Bpps (bilhões de pacotes por segundo);

13.2.13. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

13.2.14. Deve suportar Q-in-Q, recurso também conhecido como Stacked VLAN ou VLAN sobre VLAN em que é possível configurar duas TAGs de VLAN no mesmo frame;

13.2.15. Deve possuir tabela MAC com suporte a 144.000 endereços;

13.2.16. Deve operar com latência igual ou inferior à 1us (microsegundo);

13.2.17. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

13.2.18. Em conjunto com o Flow Control (IEEE 802.3x) o switch deverá, ao invés de enviar pause frames, definir um limite de banda que poderá ser recebida na interface quando o buffer estiver cheio. O switch deverá medir o volume de utilização do buffer para que o recebimento seja restaurado à capacidade máxima automaticamente;

13.2.19. Deve suportar o padrão IEEE 802.1Qbb (Priority-based Flow Control);

13.2.20. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

13.2.21. Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica;

13.2.22. Deve suportar a comutação de Jumbo Frames;

13.2.23. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

13.2.24. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

13.2.25. Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIP, BGP, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação dos protocolos;

13.2.26. Deve possuir hardware capaz de suportar roteamento multicast através do protocolo PIM-SSM (Protocol Independent Multicast - Source-Specific Multicast). É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação dos protocolos;

13.2.27. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação do protocolo;

13.2.28. Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação do protocolo;

13.2.29. Deve ser capaz de criar múltiplas tabelas de roteamento através de VRF (Virtual Routing and Forwarding). É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação deste recurso;

13.2.30. Deve implementar serviço de DHCP Server e DHCP Relay;

13.2.31. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos;

13.2.32. Deve suportar MLD (Multicast Listener Discovery) Snooping para otimizar a transmissão de tráfego multicast em IPv6;

13.2.33. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN);

13.2.34. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN;

13.2.35. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 30 (trinta) instâncias de Multiple Spanning Tree;

13.2.36. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

13.2.37. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

13.2.38. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

13.2.39. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

13.2.40. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

13.2.41. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

13.2.42. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

13.2.43. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

13.2.44. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

13.2.45. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;

13.2.46. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ);

13.2.47. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

13.2.48. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;

13.2.49. Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement;

13.2.50. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

13.2.51. Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

13.2.52. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

13.2.53. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

13.2.54. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

13.2.55. Deve suportar MAC Authentication Bypass (MAB);

13.2.56. Deve implementar RADIUS CoA (Change of Authorization);

13.2.57. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

13.2.58. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

13.2.59. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

13.2.60. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

13.2.61. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

13.2.62. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

13.2.63. Deve suportar o protocolo PTP (Precision Time Protocol);

13.2.64. Deve implementar Netflow, sFlow ou similar;

13.2.65. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

13.2.66. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

13.2.67. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

13.2.68. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

13.2.69. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

13.2.70. Deve permitir ser gerenciado através de IPv6;

13.2.71. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

13.2.72. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

13.2.73. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

13.2.74. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

13.2.75. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;

13.2.76. Deverá suportar ser configurado e monitorado através de REST API;

13.2.77. Deve possuir ferramenta para captura de pacotes que auxíliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark;

13.2.78. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash;

13.2.79. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

13.2.80. Deve suportar temperatura de operação de até 40º Celsius;

13.2.81. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

13.2.82. Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V;

13.2.83. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

13.2.84. 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;

13.3. **Especificação para o Subitem 3.2 - Serviço Conectividade do Tipo 2 (por demanda)**

13.3.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

13.3.2. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex

destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

13.3.3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

13.3.4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 740W a serem alocados em qualquer uma das portas 1000Base-T;

13.3.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

13.3.6. Deve possuir 1 (uma) interface USB;

13.3.7. Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo);

13.3.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

13.3.9. Deve possuir tabela MAC com suporte a 32.000 endereços;

13.3.10. Deve operar com latência igual ou inferior à 1us (microsegundo);

13.3.11. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

13.3.12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

13.3.13. Deve suportar a comutação de Jumbo Frames;

13.3.14. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

13.3.15. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

13.3.16. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

13.3.17. Deve implementar serviço de DHCP Relay;

13.3.18. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

13.3.19. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

13.3.20. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

13.3.21. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

13.3.22. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

13.3.23. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

13.3.24. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

13.3.25. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

13.3.26. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

13.3.27. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

13.3.28. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

13.3.29. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

13.3.30. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;

13.3.31. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

13.3.32. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

13.3.33. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

13.3.34. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

13.3.35. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

13.3.36. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

13.3.37. Deve suportar MAC Authentication Bypass (MAB);

13.3.38. Deve implementar RADIUS CoA (Change of Authorization);

13.3.39. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

13.3.40. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

13.3.41. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

13.3.42. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

13.3.43. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

13.3.44. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

13.3.45. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

13.3.46. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

13.3.47. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

13.3.48. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

13.3.49. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

13.3.50. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

13.3.51. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

13.3.52. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

13.3.53. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

13.3.54. Deve permitir ser gerenciado através de IPv6;

13.3.55. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

13.3.56. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

13.3.57. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

13.3.58. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

13.3.59. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos

nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;

13.3.60. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;

13.3.61. Deverá suportar ser configurado e monitorado através de REST API;

13.3.62. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);

13.3.63. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

13.3.64. Deve suportar temperatura de operação de até 45º Celsius;

13.3.65. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

13.3.66. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

13.3.67. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

13.3.68. 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;

13.4. **Especificação para o Subitem 3.3 - Serviço Conectividade do Tipo 3 (por demanda):**

13.4.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

13.4.2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

13.4.3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

13.4.4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W a serem alocados em qualquer uma das portas 1000Base-T;

13.4.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

13.4.6. Deve possuir 1 (uma) interface USB;

13.4.7. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo);

13.4.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

13.4.9. Deve possuir tabela MAC com suporte a 32.000 endereços;

13.4.10. Deve operar com latência igual ou inferior à 1us (microsegundo);

13.4.11. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

13.4.12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

13.4.13. Deve suportar a comutação de Jumbo Frames;

13.4.14. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

13.4.15. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

13.4.16. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

13.4.17. Deve implementar serviço de DHCP Relay;

13.4.18. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

13.4.19. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

13.4.20. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning

Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

13.4.21. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

13.4.22. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

13.4.23. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

13.4.24. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

13.4.25. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

13.4.26. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

13.4.27. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

13.4.28. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

13.4.29. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

13.4.30. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;

13.4.31. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

13.4.32. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

13.4.33. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

13.4.34. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

13.4.35. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

13.4.36. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

13.4.37. Deve suportar MAC Authentication Bypass (MAB);

13.4.38. Deve implementar RADIUS CoA (Change of Authorization);

13.4.39. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

13.4.40. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

13.4.41. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

13.4.42. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

13.4.43. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

13.4.44. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

13.4.45. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

13.4.46. Deve permitir a customização do tempo em segundos em que um determinado MAC

Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

13.4.47. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

13.4.48. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

13.4.49. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

13.4.50. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

13.4.51. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

13.4.52. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

13.4.53. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

13.4.54. Deve permitir ser gerenciado através de IPv6;

13.4.55. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

13.4.56. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

13.4.57. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

13.4.58. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

13.4.59. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;

13.4.60. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;

13.4.61. Deverá suportar ser configurado e monitorado através de REST API;

13.4.62. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);

13.4.63. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

13.4.64. Deve suportar temperatura de operação de até 45º Celsius;

13.4.65. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

13.4.66. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

13.4.67. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

13.4.68. 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;

13.5. **Especificação para o Subitem 3.4 - Serviço Conectividade Sem Fio (por demanda):**

13.5.1. Ponto de acesso (AP) que permita acesso dos dispositivos à rede através da wireless e que possua todas as suas configurações centralizadas em controlador wireless;

13.5.2. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

13.5.3. Deve identificar automaticamente o controlador wireless ao qual se conectará;

13.5.4. Deve permitir ser gerenciado remotamente através de links WAN;

13.5.5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

13.5.6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando

simultaneamente, além de permitir configurações independentes para cada rádio;

13.5.7. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;

13.5.8. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

13.5.9. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;

13.5.10. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

13.5.11. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

13.5.12. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

13.5.13. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC;

13.5.14. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;

13.5.15. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

13.5.16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

13.5.17. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

13.5.18. Deve permitir operação em modo Mesh;

13.5.19. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;

13.5.20. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;

13.5.21. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);

13.5.22. Deve suportar OFDMA;

13.5.23. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;

13.5.24. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;

13.5.25. Deve suportar BSS Coloring;

13.5.26. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;

13.5.27. Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);

13.5.28. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz;

13.5.29. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;

13.5.30. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

13.5.31. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;

13.5.32. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;

13.5.33. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);

13.5.34. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;

13.5.35. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

13.5.36. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;

13.5.37. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

13.5.38. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

13.5.39. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

13.5.40. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

13.5.41. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

13.5.42. Deve implementar o padrão IEEE 802.11e; IEEE 802.11h; IEEE 802.3az;

13.5.43. Deve suportar ser gerenciado via SNMP;

13.5.44. Deve suportar consultas via REST API;

13.5.45. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;

13.5.46. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;

13.5.47. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;

13.5.48. Deve possuir indicadores luminosos (LED) para indicação de status;

13.5.49. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;

13.5.50. Deve ser realizado site survey de forma que seja fornecido a melhor cobertura Wifi, melhor taxa de transferência de dados, maior capacidade de rede, roaming e capacidade de serviço (QoS).

13.5.51. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;

13.5.52. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto;

13.5.53. Deve ser certificado pela WIFI Alliance na subcategoria Enterprise/Service Provider Access Point, Switch/Controller or Router;

13.5.54. Deve possuir o certificado de Conectividade Wi-Fi CERTIFIED 6 ™ da WIFI Alliance;

13.5.55. Deverá ser do mesmo fabricante da solução de Gerenciamento;

13.5.56. Deverá estar licenciado para a gerência e controle do item Solução de gerenciamento e controle;

13.5.57. Deve acompanhar todas as licenças necessárias para habilitação dos recursos solicitados e gerenciamento do dispositivo;

13.5.58. 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;

13.6. **Especificação para o Subitem 3.5 - Software de Controle de Acesso à Rede (por de manda)**

13.6.1. Solução de controle de acesso à rede, a ser ofertado em formato de appliance físico ou virtual, este que deverá estar disponível para as plataformas Vmware ESXi, AWS e Microsoft Azure;

13.6.2. Deve ser uma solução multi-vendor capaz de suportar os switches e concentrador VPN do orgão;

13.6.3. Deve suportar variadas soluções de Wi-Fi do mercado, tais como: Aruba, Ruckus, Cisco, Fortinet, Aerohive e Enterasys, pelo menos;

13.6.4. A solução deve estar licenciada para operação com, pelo menos 10.000 (dez mil) endpoints conectados simultaneamente;

13.6.5. A solução deve ser capaz de inspecionar tanto IoT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);

13.6.6. Para estações de trabalho, deve suportar verificação de compliance em VPN IPsec e SSL;

13.6.7. A licença contemplada deverá suportar todas as características exigidas neste termo de referência;

13.6.8. A solução deve permitir diferentes perfis de administração, com a capacidade de limitar e controlar a quantidade de acesso permitido às funcionalidades disponíveis, dependendo do grupo administrativo da organização ao qual o usuário pertence;

13.6.9. Deve detectar e classificar automaticamente o tipo dos dispositivos conectados na rede sem a necessidade de softwares instalados nos dispositivos;

13.6.10. Deve permitir determinar o perfil dos dispositivos descobertos por meio de métodos que não exigem a instalação de agentes, incluindo pelo menos os seguintes:

a) Consultas em DHCP Fingerprint;

b) Consultas via protocolos HTTP/HTTPS;

c) Consultas via protocolo SNMP;

d) Consultas via protocolo SSH;

e) Consultas via protocolo Telnet;

f) Consultas de portas TCP;

g) Consultas de portas UDP;

h) MAC OUI;

i) Consultas via protocolo WMI;

j) Protocolo ONVIF;

k) Protocolo NetFlow;

l) Base assinaturas pré-definidas;

13.6.11. A solução deve ser capaz de reconhecer as seguintes informações sobre os dispositivos conectados à rede:

a) Endereço MAC;

b) Endereço IP;

c) Sistema operacional;

d) Nome do host;

e) Horário de conexão;

f) Usuário conectado;

g) Localização.

13.6.12. A solução deve ser capaz de reconhecer os seguintes sistemas operacionais em execução nos dispositivos conectados à rede:

a) Android;

b) Apple iOS para iPhone,

c) iPod e iPad;

d) Chrome OS;

e) Linux;

f) MacOS X;

g) Windows 7, 8 e 10 ou superior;

13.6.13. Deve lembrar o perfil atribuído a cada dispositivo e verificar sua validade a cada conexão;

13.6.14. Deve permitir a designação de um sponsor para autorizar a categorização dos dispositivo;

13.6.15. Deve permitir a recategorização periódica de dispositivos;

13.6.16. Deve permitir a importação de um arquivo CSV contendo informações sobre os dispositivos a serem registrados;

13.6.17. A solução deve incluir a detecção de dispositivos desconhecidos conectados à rede e adotar medidas de controle para limitar o acesso;

13.6.18. A solução deve suportar autenticação através de EAP-PEAP e EAP-TLS;

13.6.19. A solução deve suportar RADIUS Change of Authorization;

13.6.20. A solução deve suportar MAC Address Bypass;

13.6.21. A solução deve consultar bases LDAP e Active Directory para a identificação de usuários e grupos de usuários;

13.6.22. A solução deve permitir a criação de políticas de controle que combinem informações sobre a identidade do usuário e tipo de dispositivo com objetivo de autorizar dinâmicamente o acesso à rede;

13.6.23. Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede;

13.6.24. Deve garantir a segmentação dinâmica da rede e aplicação de políticas de segurança, tendo como base variadas combinações, como login do AD e atributos (departamento, cidade, email, telefone), características da máquina (asset tag, hostname), localidade e horário;

13.6.25. A solução deve incluir recursos de gerenciamento de visitantes, permitindo a criação de diferentes perfis de utilização e autorização a serem associados aos usuários, distinguindo por exemplo prestadores de serviços dos visitantes;

13.6.26. A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja necessário realizar consultas em bases externas;

13.6.27. A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas;

13.6.28. A solução deve possuir ferramenta que permita a criação de credenciais para eventos;

13.6.29. Deve permitir a definição de complexidade da senha dos usuários visitantes;

13.6.30. Deve ser possível definir um período de validade para as contas de usuários visitantes;

13.6.31. Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes;

13.6.32. A autenticação e autorização dos usuários visitantes deve ocorrer através de portal captivo acessível via browser web;

13.6.33. Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado;

13.6.34. A solução deve vincular o login do visitante à máquina utilizada no acesso;

13.6.35. Deve suportar a validação de credenciais:

a) Em base local interna à ferramenta;

b) Em servidores RADIUS;

c) Em servidores LDAP.

13.6.36. A solução deve autenticar usuários visitantes através das seguintes redes sociais: Facebook, LinkedIn e Twitter;

13.6.37. A ferramenta deve permitir que os usuários visitantes possam realizar auto-registro através do preenchimento de cadastro disponível em portal web;

13.6.38. Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto-registro;

13.6.39. A solução deve suportar o envio da senha de acesso aos visitantes através de SMS e e-mail;

13.6.40. Deve ser possível definir um período para que os usuários visitantes sejam obrigados a se reautenticar;

13.6.41. Deve permitir a designação de grupos de usuários com função de sponsor que ficarão responsáveis por autorizar o acesso dos usuários visitantes e prestadores de serviços;

13.6.42. Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permtir gerência administrativa dos demais recursos da solução;

13.6.43. A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens;

13.6.44. Os usuários do tipo sponsor podem ser cadastrados na base local da ferramenta ou fazer parte de grupo de usuários em base LDAP/Active Directory;

13.6.45. A solução deve incluir recursos de conformidade de endpoint. Antes de permitir que os dispositivos acessem a rede, a solução deve garantir que estes cumpram requisitos de segurança, integridade e conformidade;

13.6.46. Deve permitir o uso de software agente instalado no dispositivo e agentes evanescentes que não precisam ser instalados;

13.6.47. Tanto para IoTs quanto para estações de trabalho, se configurado, não devem ter qualquer acesso à rede de produção enquanto não forem inspecionados e identificados;

13.6.48. Se um dispositivo não passar os testes de conformidade, deve ser possível:

a) Não forçar a remediação;

b) Forçar a remediação imediatamente enviando o dispositivo à rede de quarentena;

c) Permitir a remediação retardada, ou seja, dando um período de tolerância para que o usuário corrija o problema. Caso os problemas persistam, o dispositivo deve ser colocado em quarentena;

13.6.49. A solução deve permitir verificações de conformidade em endpoints que façam uso do sistema operacional:

a) Windows XP, Windows 7, Windows 8, Windows 10 ou superior, MacOS e Linux.

13.6.50. Para garantir a conformidade com as políticas de segurança, a solução deve permitir que sejam verificados os seguintes itens antes de autorizar o acesso de um endpoint na rede:

a) Presença de software de anti-vírus instalado e em execução;

b) Versão do sistema operacional;

c) Nome de domínio do Active Directory ao qual a estação Windows pertença;

d) Serviços em execução para estações Windows;

e) Informações sobre um determinado certificado digital em estações Windows;

f) Registros ou chaves de registro para estações Windows;

g) Processos em execução para estações Windows, Linux e MacOS;

h) Arquivo armazenado em um determinado diretório para estações Windows, Linux e MacOS;

i) Pacotes instalados em estações Linux e MacOS.

j) A solução deve ser capaz de monitorar quando um serviço requirido for desabilitado ou interrompido em computadores. Além disso deve enviar a estação para quarentena de forma a garantir a conformidade com a política de segurança;

k) Deve possuir serviço RADIUS interno, além de permitir o uso de RADIUS externos;

13.6.51. Deve permitir a distribuição de agentes através de, pelo menos, os seguintes métodos:

a) Programas de gerenciamento e distribuição de software;

b) GPO do Active Directory;

c) Captive Portal;

13.6.52. Deve permitir a atualização automática ou programada dos agentes instalados nas máquinas;

13.6.53. O agente instalado nos computadores devem notificar os usuários com mensagens informativas em casos de eventos;

13.6.54. Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais estes foram movidos para o isolamento;

13.6.55. A solução deve compartilhar a identificação dos usuários e/ou dispositivos autenticados para a plataforma de segurança da rede via SSO, de forma que sejam vinculadas aos acessos de Internet, provendo rastreabilidade futura;

13.6.56. No que tange compliance, quando houver sucesso, falha ou alerta, a solução deve permitir as seguintes ações: alerta, envio de email e SMS, desabilitar o host, envio de mensagem direta para o host envolvido e executar políticas adicionais de compliance;

13.6.57. A solução deve integrar com plataformas de MDM, suportando pelo menos: FortiClient, In Tune, Mobile Iron e Air Watch;

13.6.58. Deve suportar integração com soluções de patching;

13.6.59. Deve suportar integração com soluções de análise de vulnerabilidades;

13.6.60. A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida;

13.6.61. A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante;

13.6.62. A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API;

13.6.63. A solução deve armazenar os eventos internamente e permitir que sejam exportados;

13.6.64. A solução deve permitir a exportação dos eventos através de syslog;

13.6.65. Deve suportar alta disponibilidade, suportanto todos os registros e autenticações caso um nó da solução esteja indisponível;

13.6.66. A solução deve ser capaz de isolar hosts na quarentena mesmo quando estes estão conectados em redes de localidades remotas, tais como filiais. Não deve ser necessário estender a VLAN para isso;

13.6.67. Deve possuir registro dos eventos ocorridos na solução, bem como auditoria das configurações efetuadas;

13.6.68. Suportar integração com soluções de segurança de fabricantes como: Fortinet, Palo Alto, FireEye, etc, para correlacionar alertas de segurança e restringir, isolar ou bloquear dispositivos comprometidos que estejam conectados na rede, reduzindo assim o tempo de contenção de ameaças;

13.6.69. Suportar método genérico para integração de dispositivos, usando o recebimento, envio, análise e interpretação de mensagens do tipo syslog;

13.6.70. Deve possibilitar o rastreio de dispositivos, notificando a localização dos mesmos quando se conectarem à rede;

13.6.71. Caso o **CONTRATANTE** não tenha solução de logs compatível com o NAC ofertado, cabe ao fornecedor inclui-la na proposta, sem ônus, considerando licenciamento e/ou hardware adequado para retenção dos logs;

13.6.72. Dentre os relatórios disponiblizados pela solução dedicada de logs, deve suportar relatórios listando os endpoints por localidade e fabricante, usuários associados, além de relatórios de inventário, devices registrados e rogues;

13.7. **Manutenção e suporte Tecnico para o Lote 3**:

13.7.1. A Manutenção E Suporte Técnico referente a prestação de serviços de Nuvem Pública devem estar de acordo com o especificado neste item.

13.7.2. O suporte e a manutenção deverão ser providos durante toda vigência do contrato.

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

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

13.7.5. A CONTRATADA deve ser emitido relatório mensal referente a atualização 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.

13.7.6. 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.

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

13.7.8. A CONTRATADA, deverá utilizar a ferramenta de ITSM própria, para registro de chamados e relatórios.

13.7.9. Todo chamado registrado, deve ser enviado notificação de forma automática aos fiscais do contrato.

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

13.7.11. Todo e qualquer problema detectado nos itens/serviços descritos neste Elemento Técnico, deverão ser, de forma imediata, ser relatados à equipe de Fiscais do **CONTRATANTE**.

13.7.12. Todas as mudanças adotadas por iniciativa da **CONTRATADA** nas configurações

13.7.13. deverão ser efetuadas mediante aprovação do **CONTRATANTE**.

13.7.14. A **CONTRATADA** deverá emitir uma declaração prévia, com antecedência mínima de 15 (quinze) dias, contendo:

13.7.14.1. Descrição do procedimento que será executado;

13.7.14.2. Cronograma de Atividades;

13.7.14.3. Impacto e eventuais procedimentos de contingência;

13.7.14.4. Bem como relatório posterior sobre os resultados obtido.

13.7.15. O suporte deverá incluir resposta a chamados críticos em tempo inferior a sessenta minutos e permitir a comunicação por meio de e-mail, chat e 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.

13.7.16. Os serviços de Suporte Técnico compreendem todos os chamados rela vos aos itens referenciados neste 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**.

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

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

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

13.7.19.1. **Criticidade Alta** - Deveremos entender como criticidade ALTA um serviço totalmente fora de operação, com SLA de 20 minutos para captura de chamado e início de atendimento, e até 04 horas para resolução do problema.

13.7.19.2. **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;

13.7.19.3. **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.

13.7.20. 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 providencias equipamento reserva de falhas e este equipamento deverá estar disponível em ate 3 (três) dias corridos	2,0% por dia em atraso

13.8. **Obrigações da Contratada:**

13.8.1. A **CONTRATADA**de prestar os serviços com pessoal adequadamente qualificado e capacitado para suas atividades.

13.8.2. Cumprir rigorosamente todas as programações e atividades do objeto do contrato.

13.8.3. Prestar os serviços de acordo com o especificado neste instrumento.

13.8.4. 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.

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

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

13.8.7. 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.

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

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

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

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

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

13.8.13. 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.

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

13.8.15. 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.

13.8.16. **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.

13.8.17. 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.

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

14. ANEXO IV: LOTE 4 – SAAS - SERVIÇO DE SEGURANÇA DE ENDIPOINT E AUDITORIA

14.1. Todos os itens relacionados no **Lote 4: SaaS - Serviço de Auditoria,**somente serão executados sob demanda da **CONTRATANTE**, podendo ser descontinuados a qualquer momento pela **CONTREATANTE**

LOTE	ITEM	Subitem	Descrição	Métrica	QNTD (Previsto)	Valor Unitário	Valor Mensal previsto	Valor Anual previsto	Valor previsto para 30 meses
4	SaaS - Serviço de Proteção de EndPoints e Auditoria	4.1	Serviço de proteção de EndPoints (por demanda)	Unidade/Mês	4.000	R$	R$	R$	R$
		4.2	Serviço de Auditoria (por demanda)	Unidade/Mês	4.000	R$	R$	R$	R$

14.2. **Especificações Subitem 4.1 - Serviço de Proteção de EndPoints (por demanda):**

14.2.1. Os softwares (solução) necessários à prestação dos serviços deverão ser instalados, de modo a avaliar e proteger contra códigos maliciosos as estações de trabalho do ambiente da **CONTRATANTE**.

14.2.2. A infraestrutura para implantação da solução, baseando-se nas especificações a abaixo:

a) Os seguintes hipervisores devem ser suportados: VMware ESXi 7.0 ou superior, Microsoft Hyper-V Server 2019 ou superior.

b) Requisitos máximos de VM Servidor para solução:8 CPUs virtuais, 200 GB de espaço em disco 24 GB de RAM e 2 portas virtual switched ports

14.2.3. **Funcionalidades e Requisitos Específicos:**

14.2.3.1. Realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

Windows 7(x86/x64); Windows 8 e 8.1 (x86/x64) e Windows 10 (x86/x64) e superior (todas as versões);

14.2.3.2. Possuir tecnologia de Machine Learning sendo capaz de detectar variantes de malwares desconhecidos por similaridade de código;

14.2.3.3. Possuir módulo de monitoração de comportamento malicioso de aplicações de forma a bloqueá-las mesmo quando a assinatura não for reconhecida;

14.2.3.4. Possuir regras específicas para detecção de ransonware e alertar, reportar e bloquear atividade anômala de arquivos e usuários durante a interação com bases de senhas no formato hash, como por exemplo, SAM local e LSASS;

14.2.3.5. Detectar , analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

14.2.4. **Detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:**

14.2.4.1. Possuir regras específicas para detecção de ransonware e alertar, reportar e bloquear atividade anômala de arquivos e usuários durante a interação com bases de senhas no formato hash, como por exemplo, SAM local e LSASS;

14.2.4.2. Processos em execução em memória principal (RAM);

14.2.4.3. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

14.2.4.4. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;

14.2.4.5. Arquivos recebidos por meio de programas de comunicação instantânea (msn messenger, yahoo messenger, google talk, icq, dentre outros).

14.2.4.6. Permitir configurar o consumo de cpu que será utilizada para uma varredura manual ou agendada;

14.2.4.7. Possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

14.2.4.8. Permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

14.2.4.9. Possuir a capacidade de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

14.2.4.10. Permitir proteção dedicada contra URL's maliciosas voltadas a tecnologia Microsoft Skype for Business e Microsoft Lync Server.

14.2.4.11. Permitir a programação de atualizações automáticas e/ou incremental das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

14.2.4.12. Permitir o rollback das atualizações das listas de definições de vírus e engines;

14.2.4.13. Permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações;

14.2.4.14. Permitir proteção dedicada contra códigos maliciosos voltadas a tecnologia Microsoft Skype for Business e Microsoft Lync Server.

14.2.4.15. Permitir proteção para Office 365 em nuvem, Box, Dropbox, OneDrive for Business, Google Drive utilizando estruturas em nuvem para o gerenciamento do mesmo contra ameaças maliciosas.

14.2.5. **Funcionalidades de Controle de Dispositivos:**

14.2.5.1. Possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

14.2.5.2. Possuir o controle de acesso a drives de mídias de armazenamento como CD-ROM e DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

14.2.5.3. Possuir a capacidade de identificar smartphones e tablets como destinos de cópias de

arquivos e tomar ações de controle da transmissão;

14.2.5.4. Possuir a capacidade de controlar drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

14.2.5.5. Permitir esc aneamento dos dispositivos removíveis e periféricos (USB, disquete, CD-ROM) mesmo com a política de bloqueio total ativa

14.2.6. **Funcionalidades de Host IPS e Host Firewall:**

14.2.6.1. Possuir a capacidade de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

- Windows XP, Windows 7 (x86/x64), Windows 8 e 8.1 (x86/x64) e Windows 10 (x86/x64) e superiores;

14.2.6.2. Permitir que todas as regras das funcionalidades de firewall e IPS de host atuem apenas em modo detecção ou prevenção;

14.2.6.3. Efetuar varredura de segurança automática ou sob demanda que aponte vulnerabilidades de sistemas operacionais e aplicações e atribua automaticamente as regras de Host IPS para proteger a estação de trabalho ou notebook contra a possível exploração da vulnerabilidade;

14.2.6.4. A varredura de segurança deve ser capaz de identificar as regras de Host IPS que não são mais necessárias e desativá-las automaticamente;

14.2.6.5. e) Prover proteção contra as vulnerabilidades de aplicações terceiras, por meio de regras de host ips, tais como oracle java, abobe pdf reader, adobe flash player, realnetworks real player, Microsoft office, apple itunes, apple quick time, apple safari, google chrome, mozilla firefox, opera browser, ms internet explorer, entre outras;

14.2.6.6. Permitir a emissão de alertas via SMTP e SNMP;

14.2.6.7. Permitir criação de regras de firewall utilizando os seguintes protocolos: Icmp, icmpv6, igmp, ggp, tcp, pup, udp, idp, nd, raw, tcp+udp.

14.2.6.8. Permitir criação de regras de firewall por origem de ip ou mac ou porta e destino de ip ou mac ou porta;

14.2.6.9. Permitir a criação de contextos para a aplicação para criação de regras de firewall;

14.2.6.10. Permitir o isolamento de interfaces de rede, possibilitando o funcionamento de uma interface por vez.

14.2.7. **Funcionalidades de Controle de Aplicação:**

14.2.7.1. Possuir a capacidade de realizar o controle de aplicações nos seguintes sistemas operacionais:

- Windows 7 (x86/x64), Windows 8 e 8.1 (x86/x64), Windows 10 (x86/x64) e superiores;

14.2.7.2. Permitir a criação de políticas de segurança personalizadas;

14.2.7.3. Permitir o controle do intervalo de envio dos logs e para envio de atualização de cada política;

14.2.7.4. Permitir a definição de qual servidor de gerenciamento o agente de segurança deverá comunicar-se;

14.2.7.5. Permitir as seguintes ações: Permissão de execução; Bloqueio de execução e Bloqueio de novas instalações;

14.2.7.6. Permitir os seguintes métodos para identificação das aplicações: Assinatura sha-1 do executável;

14.2.7.7. Atributos do certificado utilizado para assinatura digital do executável; Caminho lógico do executável e Base de assinaturas de certificados digitais válidos e seguros;

14.2.7.8. Possuir categorias de aplicações e permitir a utilização de múltiplas regras de controle de aplicações;

14.2.7.9. Possuir atu alização das categorias de maneira automatizada

14.2.8. **Funcionalidades de Proteção contra Vazamento de Informações:**

14.2.8.1. Possuir a capacidade de realizar a proteção contra vazamento de informação nos seguintes sistemas operacionais:

- Windows 7 (x86/x64); Windows 8 e 8.1 (x86/x64), Windows 10 (x86/x64) e superior;

14.2.8.2. Possuir a capacidade de detectar informações, em documentos nos formatos:

- Microsoft office (doc, docx, xls, xlsx, ppt, pptx) openoffice, rft, wordpad, text; xml, html; postscript, pdf, tiff, zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2, unix/linux zip, lzh;

14.2.8.3. Possuir a capacidade de detectar informações, com base em:

- Dados estruturados, Palavras ou frases configuráveis, Expressões regulares e Extensão dos arquivos;

14.2.8.4. Permitir a configuração de quantas camadas de compressão serão verificadas;

14.2.8.5. Permitir a criação de modelos personalizados para identificação de informações;

14.2.8.6. Possuir a capacidade de identificar e bloquear informações no mínimo para os seguintes meios de transmissão:

a) Cliente de e-mail;

b) Protocolos http, https, ftp;

c) Mídias removíveis e discos óticos cd/dvd;

d) Aplicações de mensagens instantâneas;

e) Tecla de printscreen;

f) Aplicações p2p;

g) Área de transferência do Windows;

h) Webmail;

i) Armazenamento na nuvem (cloud);

j) Impressoras;

k) Scanners

l) Compartilhamentos de arquivos; Activesync; Portas COM e LPT; Modems.

m) Permitir proteção dedicada contra vazamento de informações voltadas a solução Microsoft Skype for Business e Microsoft Lync Server.

n) Permitir proteção contra vazamento de informação em Office 365 em nuvem, Box, Dropbox, OneDrive for Business, Google Drive utilizando estruturas em nuvem para o gerenciamento do mesmo.

14.2.9. **Funcionalidades de Criptografia:**

14.2.9.1. Possuir a capacidade de realizar a criptografia nos seguintes sistemas operacionais:

- Windows 7 (x86/x64); Windows 8 e 8.1 (x86/x64), Windows 10 (x86/x64) e superiror;

14.2.9.2. Possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), permitindo criptografia para:

a) Disco completo (FDE – full disk encryption);

b) Pastas e arquivos; Mídias removíveis;

c) Anexos de e-mails e Automática de disco;

d) Possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

e) Possuir a capacidade de exceções para criptografia automática;

f) Possuir compatibilidade de autenticação por múltiplos fatores;

g) Permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

h) Possuir autoajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;

i) Possuir mecanismos para wipe (limpeza) remoto;

j) Possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);

k) Possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook;

l) O ambiente de autenticação pré-inicialização deve permitir a conexão a redes sem fio (wireless);

m) Permitir, em nível de política, a indicação de pastas a serem criptografadas;

n) Possibilitar que cada política tenha uma chave de criptografia única;

o) Permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;

p) Possibilitar a desativação de dispositivos de gravação de mídias óticas e de dispositivos de armazenamento USB;

q) Possibilitar apagar todos os dados do dispositivo na ocorrência de um número personalizável de tentativas inválidas de autenticação

14.2.10. **Deve permitir o provisionamento de configurações de:**

a) Wi-fi, Exchange Activesync, vpn, proxy http global e certificados;

b) Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão sd e após atualização de vacinas;

c) Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número bloqueados para recebimento de chamadas;

d) Deve possuir funcionalidade de firewall para bloqueio de tráfego de entrada e saída, com possibilidades de enumeração de regras de exceção;

e) Deve permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL's acessadas;

f) Deve permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;

g) Deve permitir o bloqueio de aplicativos de acordo com sua faixa etária indicativa;

14.2.11. **Controle da política de segurança de senhas, com critérios mínimos de:**

a) Tempo de expiração;

b) Bloqueio automático da tela;

c) Bloqueio por tentativas inválidas;

d) Deve proteger as senhas de credenciais administrativas locais dos desktops Windows e Mac em repositório central seguro, que permita a aplicação de políticas granulares de rotações e trocas automáticas das senhas, mitigando situações de roubo, perda e exploração de credenciais.

e) Quando os desktops Windows e Mac não puderem estar conectados de forma permanente ao repositório central seguro de credenciais, deve aplicar, de forma autônoma, políticas de rotação de credenciais locais até a sincronização das mesmas definidas no repositório central da solução.

f) O repositório central seguro de credenciais deve incorporar medidas de segurança como Certificação Common Criteria (CC) - ISO/IEC 15408, banco de dados das credenciais hardenizado, com criptografia, AES-256, FIPS1402, PKCS#11 ou superior e protegida por Web Application Firewall.

g) Controle de acesso à seguinte lista funções e status de ativação de funções dos dispositivos móveis:

- Bluetooth, Câmera, Cartões de memória, Wlan/wifi, GPS, Microsoft Activesync, MMS/SMS, Alto-falante, Armazenamento USB, 3g, 4g e 5g, Modo de desenvolvedor, Ancoragem (tethering)

14.2.12. **Serviços gerenciados de detecção e respostas a ameaças nos terminais/ Endpoints:**

14.2.12.1. Solução avançada para proteção de endpoint e servidores permitindo a categorização flexível, agrupamento de computadores e mecanismo de limitação de acesso autorizado ao endpoint por meio de autenticação de múltiplo fator na tela de login, suportando, no mínimo, entrega de código via SMS e chamada de voz como fator adicional, questões de segurança como segundo fator e notificações por e-mail, notificações push e tokens OTP, FIDO2/U2F e OATH, invalidando sessões e tokens após um período de inatividade.

14.2.12.2. Deve ter recursos avançados de análise de comportamento e modo de coleta somente para avaliação e validação das políticas criadas.

14.2.12.3. A proponente deverá ter seu próprio processo de inteligência contra ameaças em tempo real (VirusTotal, NSRL e base própria de conhecimento) com monitoramento de endpoint deverá ser comprovado por documentação e ou contratos ativos nacionais ou globais.

14.2.12.4. A proponente deve incluir um processo como fonte de inteligência de informações, suportado por uma equipe avançada do provedor, com capacidade global para coletar, investigar e descobrir os ataques, campanhas e malware avançado que são gerados todos os dias como uma ameaça de dia zero.

14.2.12.5. Deverá ter a capacidade de monitorar, detectar e responder em um esquema 24x7x365 que permita o acionamento de ações de alerta, procedimentos de investigação remota com acesso aos ativos possivelmente afetados, bem como um possível escopo em resposta e correção.

14.2.12.6. A equipe de proteção avançados que executará todo o ciclo de monitoramento, detecção, caça e identificação de ameaças e deve ter um nível avançado de qualificações e experiência nas camadas mais avançadas de detecção e caça de ameaças.

14.2.12.7. A equipe avançada da proponente precisará fazer uma revisão manual para identificar e capturar ameaças através da infraestrutura **IGESDF,**à medida que novas tendências e ameaças de ataques são lançadas globalmente.

14.2.12.8. O provedor d eve fornecer uma solução/ plataforma que disponibilize um console ou portal para acesso e integração de dispositivos que atendam às seguintes especificações:

a) Implementação, configuração e operação da plataforma de proteção e monitoramento de terminais/ endpoints.

b) O provedor deve fornecer uma solução que suporte à proteção em plataformas com sistema operacional Windows e Linux.

c) A solução dev e ter a capacidade de monitorar a atividade do terminal no nível de identificação de objetos, memória e violações de políticas (Hardening)

14.2.12.9. Análise de atividades a partir de um conjunto de indicadores de compromisso previamente definidos e estabelecidos entre a proponente e o IGESDF.

14.2.12.10. Processos em execução, visando detectar e bloquear tentativas de roubo de credenciais armazenadas em browsers e no Windows;

14.2.12.11. Intervenção em dispositivos que foram afetados por alguma vulnerabilidade ou ataque.

14.2.12.12. Coleta de Evidência e analisar eventos sobre artefatos perigosos na memória e discos rígidos.

14.2.12.13. Possibilitar o monitoramento e a criação de evidência em vídeo de certas execuções de arquivo e de execuções sob certas condições definidas em política

14.2.12.14. Remover direitos de administrador local, gerenciando a elevação de privilégios temporária sob demanda e granular (comandos e tarefas) baseada em políticas, com controle em nível de processos-pai e processos-filhos, prevenindo movimentação lateral

14.2.13. **A ativação do serviço de proteção de terminal deve considerar as seguintes fases:**

14.2.13.1. **Provisionamento do serviço**: a proponente deve coordenar com **IGESDF** a integração e a autorização das fontes na solução de monitoramento e detecção, conforme previamente analisado e projetado pelo **IGESDF** e pelo fornecedor.

14.2.13.2. Gerenciamento da solução: a proponente deve executar a operação e manutenção da plataforma de monitoramento e detecção de terminais, incluindo a configuração e políticas da solução, manutenção, verificação de integridade, atualizações e suporte.

14.2.13.3. Intervenção & correção: A proponente deve executar ações de intervenção nos

dispositivos afetados, bem como ações de correção.

14.2.13.4. A **CONTRATADA**deve permitir o acesso ao pessoal que IGESDF determinar sob as seguintes considerações:

a) A proponente deverá habilitar uma plataforma centralizada de acesso à Web para a equipe do **IGESDF,**onde deve ser possível consultar o monitoramento e o gerenciamento de atividades relacionadas aos dispositivos/ endpoints do **IGESDF.**

b) Os controles de acesso devem ser definidos, limitados ao pessoal do provedor e ou **IGESDF** que executa ações de administração da plataforma.

14.2.13.5. O serviço deve fornecer uma visão e acesso à plataforma de gerenciamento, considerando os seguintes aspectos obrigatórios:

a) Visão atualizada e histórica dos dados e apresentação da posição no ambiente do **CONTRATANTE** integrado ao serviço.

b) Canal de comunicação seguro com o provedor e a equipe do IGESDF.

c) Interface para o gerenciamento de tickets relacionados ao serviço e relatórios associados aos resultados do monitoramento e detecção de eventos nos terminais do IGESDF.

d) Painel com as informações de contato da equipe do IGESDF.

e) Painel com a documentação das políticas de serviço e segurança associadas.

f) Painel para criação de relatórios de segurança pelo time de SI do IGESDF.

g) Painel que mostra o progresso nos processos de integração de fontes à solução.

14.2.13.6. O fornecedor deve gerenciar a solução/ plataforma através de sua própria equipe técnica, que inclui os seguintes escopos:

a) Executar gerenciamento da plataforma, monitoramento e status, configurações e desempenho.

b) O ge renciamento e a manutenção da solução devem ser cobertos por um esquema de serviço 24x7x365.

14.2.13.7. As solicitações e o gerenciamento das configurações de política devem obedecer aos seguintes requisitos:

a) Processo de controle de alterações de fornecedores para terminais integrados a plataforma web.

14.2.13.8. Coordenar e avaliar em conjunto entre o provedor e o IGESDF as mudanças que podem afetar a operação dos terminais.

14.2.13.9. Gerenciar s olicitações de controle de alterações através de:

a) A plataforma de gerenciamento centralizado do serviço de monitoramento e detecção de ameaças.

b) Contato telefônico: acesso ao número de telefone para que o IGESDF, possa solicitar alterações nas políticas ou dispositivos integrados no serviço.

c) E-mai l de contato: acesso a um e-mail para que o IGESDF possa solicitar alterações nas políticas ou dispositivos integrados no serviço

14.2.13.10. O gerenciamento de disponibilidade da solução deve considerar o seguinte:

a) O provedor monitorará a disponibilidade e o nível de serviço da solução

b) Se ne cessário, o contato técnico deve ser coordenado para ações mais avançadas

14.2.13.11. O fornecedor deve executar ações de investigação, análise e resposta que considere:

a) Monitoramento e investigação que permitem ao IGESDF identificar o nível de risco associado a uma ameaça / vulnerabilidade e isso permite estabelecer ações primárias de correção / contenção.

b) Ca pacidade de estender/ escalar ações de investigação por meio de serviços adicionais de provedores, como em conjunto com a equipe de contenção e de RI ou investigação digital forense.

14.2.14. Fornecer um modelo de proteção contínua contra ameaças avançadas, considerando:

a) **Detecção em tempo real** - A partir de uma análise em tempo real, é realizado um cruzamento de informações com um banco de dados e base de conhecimento ou fontes de inteligência para determinar e identificar comportamentos suspeitos nos endpoints do IGESDF.

b) **Resposta** - a partir de possíveis evidências de um ataque realizado ou de uma vulnerabilidade explorada, isole os dispositivos afetados e realize ações de mitigação em coordenação com o **IGESDF**.

c) **Determine o impacto** - De acordo com as informações coletadas e analisadas, o escopo do incidente deve ser identificado.

d) **Remediação** - Com as informações sobre o escopo do impacto, o fornecedor deve desenvolver e aplicar um plano de remediação eficaz.

e) **Aplicar contramedidas** - A fornecedor deve atualizar as medidas de monitoramento e proteção assim que o incidente for mitigado e remediado por meio de um plano de proteção contra futuras ameaças desconhecidas.

14.2.15. O fornecedor deve realizar a identificação preventiva contra ameaça.

14.2.16. Essas atividades devem se concentrar na detecção de ameaças latentes sob um modelo holístico de identificação de ataques

14.2.17. A identificação desses padrões avançados de ameaças deve ser correlacionada com os eventos das fontes encontradas nos serviços gerenciados de monitoramento e detecção de ameaças.

14.2.18. Se ações de correção forem geradas com base na análise e identificação preventiva de ameaças latentes, o procedimento de RI definido por IGESDF deverá ser seguido em conjunto com o provedor.

14.2.19. Nesse caso, um protocolo de notificação de incidentes deve ser definido entre o provedor e o IGESDF.

14.2.20. Além disso, para a correção de incidentes, um protocolo de notificação de incidentes deve ser definido entre o provedor e o IGESDF, incluindo os seguintes critérios:

Opções de Resposta a Incidentes	**Descrição**
Blacklisting o bloqueio do hash deste processo	Ativar bloqueio de arquivo hash ou atualizar processo de blacklist
Quarentena do endpoint	Restrição de acesso à rede, apenas o ambiente da equipe RI terá acesso.
Sessão interativa com o terminal afetado	Análise por meio de shell
Download de arquivos deste endpoint	Começando com o processo de investigação de RI, pode ser necessário fazer o download de informações para contenção da vulnerabilidade ou análise.
Excluir arquivos deste terminal	Remover arquivos danificados no endpoint
Acesso a arquivos ou memória dos hosts	Coletando Arquivos ou Memória do Host

14.3. **Especificação Subitem 4.1 – Serviços de Auditoria** (por demanda):

14.3.1. O serviço a ser prestado deve ser comporto por Sistema de Gerenciamento Centralizado

(gerenciador da solução) e atender ao parque de ativos do IGESDF, com licenças ou agentes compatíveis para a detecção de incidentes de segurança e vulnerabilidades em endpoints (estações de trabalho e servidores em ambientes Windows, tanto físicos quanto virtuais).

14.3.2. Com o objetivo de adequar os processos de governança, todos os módulos que compõem a solução deverão se integrar visando constituir um ambiente homogêneo de análise, investigação, inteligência, defesa cibernética, possibilitando pronta resposta a eventos diversos. É fundamental que a solução seja única, permitindo relacionar serviços, processos e metodologias de TIC e de Negócio do IGESDF

14.3.3. A solução deve prover detecção automatizada dos incidentes de segurança fornecendo informações detalhadas sobre o incidente ou vulnerabilidade para pronta ação de contenção e resposta, disponibilizando a informação em seus níveis de criticidade tanto no dashboard, em tempo real, quanto em seu histórico por meio de relatórios.

14.3.4. Todas as funcionalidades referentes à detecção de incidentes, visando a contenção de tais ameaças, devem ser passíveis de automatização;

14.3.5. A solução deve permitir a evidenciação de vazamentos de dados via dispositivos de armazenamento removíveis, inclusive telefones celulares, armazenadores em nuvem, e-mail, mensageria instantânea, web, impressão, área de transferência, captura de tela e compartilhadores de arquivos.

14.3.6. Análise comportamental de softwares instalados nos endpoints;

14.3.7. Monitoramento on-line de todas as atividades de usuários, processos, arquivos e acessos à rede, incluindo equipamentos sem agente da solução instalado.

14.3.8. A solução deve ser capaz de prover informações detalhadas que auxiliem nos trâmites jurídicos em caso de reclamações inerentes ao uso ou vazamento de dados.

14.3.9. A implementação e configuração necessárias para o perfeito funcionamento da solução é de responsabilidade da **CONTRATADA**

14.3.10. A solução deverá monitorar e auditar os principais recursos de segurança dos endpoints no dashboard e relatórios como: dados sobre existência e atualizações do antivírus, firewall, antispyware e sistema operacional.

14.3.11. **Da interface de gerenciamento, visualização e relatórios:**

14.3.11.1. A solução deve ser capaz de integrar em uma única console de visualização, dados e metadados de logs e fluxos de rede de modo que permita identificar rapidamente a causa raiz dos incidentes detectados no ambiente em console única;

14.3.11.2. A solução deve suportar o gerenciamento dos componentes através de uma interface de gerência central;

14.3.11.3. A solução deve permitir buscas utilizando expressões regulares e palavras-chave em todo o conteúdo dos dados capturados;

14.3.11.4. A solução deve possuir a capacidade de navegação continua sobre os dados em formato “drill down”, podendo realizar pesquisas avançadas para melhor correlação de eventos;

14.3.11.5. A solução deve permitir a criação e customização de regras, alertas, gráficos e relatórios na própria interface;

14.3.11.6. Deve permitir a geração de relatórios gerenciais relativo aos logs de todas as fontes de dados usadas para alimentar a solução.

14.3.11.7. Deverá permitir a criação de dashboards customizados de tal modo que cada caso de uso implementado possa ter seu dashboard.

14.3.11.8. As funções de manutenção e operação da solução podem estar integradas no mesmo console de administração.

14.3.11.9. Possuir acesso seguro e criptografado de forma a garantir a autenticidade, confidencialidade e integridade dos dados.

14.3.11.10. Possuir interface web;

14.3.11.11. Possuir a capacidade de efetuar a segregação de funções dos usuários da solução;

14.3.11.12. A solução deve possuir controle de acesso baseado em papéis e perfis de usuários;

14.3.11.13. A solução deve possuir mecanismo de auditoria através da geração de logs das atividades realizadas no console de gerência e investigação;

14.3.11.14. Fornecer visualização e ações diferenciadas por perfis de acesso;

14.3.11.15. Deve permitir a visualização de eventos, alertas e incidentes;

14.3.11.16. Possuir a funcionalidade de visualização de eventos e alertas de segurança em tempo real;

14.3.11.17. Deverá permitir a livre customização da interface, definindo página inicial por usuário e dashboards customizados;

14.3.11.18. Permitir a criação de dashboards customizados, contendo apenas gráficos e tabelas escolhidas pelo usuário.

14.3.11.19. Deverá ser fornecido com dashboards pré-configurados e permitir a criação de novos dashboards;

14.3.12. **Deverá permitir a fácil criação de uma vasta gama de efeitos visuais**:

14.3.12.1. Tabelas, Gráfico com agrupamento em período, Gráficos de linhas, Gráficos de barras, Gráficos de pizza;

14.3.12.2. Deverá implementar dashboards de monitoramento de resultados históricos e em tempo real;

14.3.12.3. Deverá permitir a criação de dashboards diretamente dos resultados da pesquisa, sem necessidade de configuração manual;

14.3.12.4. Deverá suportar pesquisas no histórico de eventos, fornecendo capacidade de drill-down, ou seja, visualizar os detalhes dos eventos, quando aplicável, para análise forense e investigação de incidentes.

14.3.12.5. Deverá suportar a procura por texto, campos pré-definidos, palavras chaves, operações boleanas e expressões regulares;

14.3.12.6. Deverá implementar visualização em tempo real de eventos que atendam ao critério de seleção definido pelo usuário;

14.3.12.7. Permitir a criação de novos relatórios;

14.3.12.8. Deverá possuir relatórios pré-configurados separados em categorias;

14.3.12.9. A solução deve permitir que os relatórios sejam executados periodicamente (diário, semanal, quinzenal e mensal) ou de forma tempestiva.

14.3.12.10. Apresentar relatórios de eventos, alertas e incidentes em nível técnico e gerencial, os quais devem ter a possibilidade de serem gerados em pdf ou csv;

14.3.12.11. Deverá permitir o agendamento de geração de relatórios periódicos, notificar ou enviar automaticamente os relatórios gerados para os destinatários;

14.3.13. **Agentes para endpoints**

14.3.13.1. Deverão funcionar por meio de software (agente) instalado, independente do ambiente que esteja sendo executado (máquina física ou virtual);

14.3.13.2. Os agentes serem instalados nos endpoints deverão ser compatíveis, no mínimo, com os seguintes sistemas Operacionais:

14.3.13.3. Windows XP, Windows 7 32bits e 64 bits, Windows 10 32bits e 64 bits, Windows 11 32bits e 64 bits ou superior

14.3.13.4. Windows Server em suas versões 2012 R2, 2016 e 2019, 32 bits e 64 bits ou superior.

14.3.13.5. Deverá identificar os endpoints com agentes desatualizados.

14.3.14. **Distribuição e instalação**

14.3.14.1. Descoberta automática dos endpoints que não possuem o agente instalado;

14.3.14.2. Descoberta automática e evidenciação dos agentes que eventualmente tenham sido paralisados propositadamente;

14.3.14.3. A instalação do agente deve possuir um pacote único a todas as versões do sistema operacional Windows.

14.3.14.4. A instalação do agente em endpoints Windows deve ser realizada e gerenciada pela própria solução, por ferramenta do IGESDF, ou manualmente, por usuário autorizado, de forma remota e autônoma, oculta, sem interferência do usuário final e sem a necessidade de reiniciar a máquina;

14.3.14.5. Poder ser instalado em qualquer departamento da organização, sem a dependência de gerenciamento de rede (Por exemplo: Active Directory), e sem necessidade de configuração de usuários e arquivos.

14.3.14.6. Poder ser instalado em DMZ para comunicações/atualizações de agentes instalados em endpoints que poderão estar sendo utilizados fora do ambiente do IGESDF

14.3.15. **Consumo de recursos**

14.3.15.1. Os agentes não poderão consumir recursos substanciais do endpoint ou interferir em seus itens de configuração (memória, processamento e espaço em disco local e tráfego de rede), não podendo ultrapassar 2% (dois por cento) de consumo, em média, de cada item, aferidos individualmente.

14.3.16. **Segurança**

14.3.16.1. As atualizações ou comunicações que eles necessitarem deverão ser feitas pelo gerenciador da solução. Caso o endpoint esteja sendo utilizado fora do ambiente corporativo, este poderá acessar o gerenciador da solução via internet apenas para coleta de atualizações e para envio de incidentes registrados. Esses acessos devem ser definidos através de políticas internas do IGESDF e os dados devem trafegar por meio do protocolo TLS 1.1 ou superior;

14.3.16.2. Deve possuir proteção contra desinstalação ou interrupção do agente;

14.3.17. **Inteligência Artificial**

14.3.17.1. Deve detectar e analisar, automaticamente e em tempo real, por aprendizado de máquina (“Machine Learning” ou “Deep Learnig”) e análise comportamental de usuários e máquinas monitoradas;

14.3.17.2. Capacidade de aprendizado de comportamento de usuários para aprimoramento das detecções de comportamentos suspeitos.

14.3.17.3. Deve possuir tecnologia de análise de arquivos binários para identificação de comportamento malicioso.

14.3.17.4. Deve permitir a utilização de Centro de Inteligência de reputação para análise granular de arquivos ou URL’s , de modo a prover rápida detecção de novas ameaças.

14.3.17.5. Deve ser capaz de correlacionar eventos e alertas de forma automática para maior acertividade na identificação de ameaças e comportamento anormal no endpoint.

14.3.17.6. Deve possuir tecnologia de investigação forense preditiva.

14.3.18. **Monitoramento e auditoria em endpoints**

14.3.18.1. Emissão de alertas no Console Centralizado indicando uma nova classe de dispositivo encontrada, ao identificar um novo dispositivo conectado no endpoint, cujo hardware seja desconhecido (alerta de alteração de hardware);

14.3.18.2. Monitoramento e coleta de eventos de logon e logoff de usuários, bloqueio e desbloqueio de sessão e acessos a compartilhamentos;

14.3.18.3. Monitoramento de páginas web acessadas e download de arquivos a partir de páginas web;

14.3.18.4. Monitoramento, registro e emissão de alertas sobre:

14.3.18.5. Tentativas de evitar a coleta de dados da solução;

14.3.18.6. Tentativas de desinstalar a solução; e

14.3.18.7. Alterações nas chaves de registro e em arquivos de configuração do sistema operacional.

14.3.18.8. Monitoramento de acesso remoto aos endpoints, de forma centralizada, via gerenciador da solução;

14.3.18.9. Monitoramento, emissão de alertas e bloqueio automático ou manual de processos de softwares não autorizados;

14.3.18.10. Identificação de patches não aplicados em sistemas operacionais e softwares instalados em endpoints;

14.3.18.11. Todos os registros de eventos classificados como incidentes deverão ser passiveis de

envio ao gerenciador da solução;

14.3.19. **Monitoramento e detecção dos seguintes atributos de hardware e software**:

14.3.19.1. Versões, Número de série, Fabricante, Datas, Identificação de novas instalações de software; e Localização imediata da primeira instalação do software na rede.

14.3.20. **Monitoramento e detecção da performance dos endpoints, contemplando dos seguintes atributos**:

14.3.20.1. CPU, I/O, Memória física e Unidade de armazenamento.

14.3.21. **Monitoramento e detecção de processos, drivers e serviços:**

14.3.21.1. Identificação de novo processo e localização da primeira ocorrência;

14.3.21.2. Identificar processos suspeitos através de análise comportamental;

14.3.21.3. Identificação de alteração de comportamento de processo, através de mudança de registro de versão, hash, assinatura, nome original e soma de verificação (checksum).

14.3.21.4. Análise comportamental de softwares: monitoração de softwares, tendo por finalidade identificar e subsidiar ação de contenção de contaminações diversas em endpoints;

14.3.21.5. Identificação de execução de softwares ou versões de softwares que possuam vulnerabilidades.;

14.3.21.6. Verificação de unicidade dos arquivos por meio da análise de hash, evitando que o mesmo binário seja analisado diversas vezes;

14.3.21.7. Identificação de tráfegos de entrada e saída, com base em endereços de hardware, protocolos, endereçamento IP e portas (serviços);

14.3.21.8. Capacidade parametrizada de coletar, registrar e armazenar todas as conexões (TCP) ou transmissões (UDP) de rede, incluindo informações sobre endereços IP, portas de origem e destino e domínios DNS;

14.3.21.9. Informar programas e processos em execução em tempo real;

14.3.21.10. Registro de softwares (instalados, executados e em execução), com possibilidade de mitigação de softwares vulneráveis em execução bem como a data de instalação de cada item.

14.3.21.11. Monitorar e alertar sobre arquivos e programas suspeitos na rede, bem como a utilização de recursos elevados do endpoint ou sistema operacional;

14.3.21.12. Possuir mitigação automatizada ou manual capaz de encerrar processos em execução.

14.3.21.13. Detecção e alerta de contaminações diversas, backdoors e qualquer outra forma de código mal-intencionado;

14.3.21.14. Detecção de contaminações por comportamento, utilizando assinaturas;

14.3.21.15. Detecção de código malicioso por análise comportamental;

14.3.21.16. Identificação de propagação de contaminações diversas e atividades suspeitas de criptografia de arquivos;

14.3.21.17. Motor de análise e detecção de dados acessados pelo usuário, em trânsito, para fora ou dentro da rede e armazenados localmente ou em um compartilhamento de rede;

14.3.21.18. Identificar, por meio de varreduras automatizadas, a superfície de ataque (vulnerabilidades, falhas, configurações inseguras e portas abertas).

14.3.21.19. Permitir administração de endpoints off-site (conexão VPN, nuvem);

14.3.21.20. Deve ser capaz de identificar processos sendo executados a partir de um dispositivo USB;

14.3.21.21. Deve ser capaz de identificar acessos a aplicações em nuvem no endpoint;

14.3.22. **Monitoramento de tráfego, manipulação e processamento de dados**

14.3.22.1. Monitorar arquivos criados, acessados, modificados ou renomeados na unidade local;

14.3.22.2. Monitorar arquivos criados, acessados, modificados ou renomeados em discos removíveis, incluindo dispositivos móveis conectados, dispositivos USB e outras mídias removíveis;

14.3.22.3. Monitorar arquivos criados, acessados, modificados ou renomeados em drives de CD/DVD;

14.3.22.4. Monitorar arquivos acessados ou excluídos em compartilhamentos de rede;

14.3.22.5. Monitorar o uso de captura de tela, independente do tipo;

14.3.22.6. Monitorar uso de dados por Peer-to-peer (P2P);

14.3.23. **Monitorar qualquer comando digitado pelo usuário, script automático ou serviço no Powershell e Prompt de Comando, capaz de manipular arquivos, com no mínimo monitoramento dos seguintes comandos:**

14.3.23.1. Net Share;

14.3.23.2. Dir, rmdir,mkdir;

14.3.23.3. Del;

14.3.23.4. Net use;

14.3.23.5. Monitorar o uso de aplicativos que executam comandos remotamente;

14.3.23.6. Monitorar a utilização da função Executar do Windows pelo usuário, capaz de manipular e acessar arquivos;

14.3.23.7. Permitir a monitoração de dados transmitidos via HTTP;

14.3.23.8. Permitir a monitoração para transmissões HTTPS pelo Internet Explorer, Mozilla Firefox e Google Chrome com ou sem a utilização do Proxy da infraestrutura;

14.3.23.9. Permitir a monitoração para Transmissões via FTP;

14.3.23.10. Permitir a monitoração para arquivos enviados a qualquer tipo de impressora local e de rede;

14.3.23.11. Possuir capacidade para executar verificações de filtro com base no tipo e local do arquivo;

14.3.23.12. Monitoramento de acesso remoto aos endpoints, de forma centralizada, via gerenciador da solução;

14.3.23.13. Permitir a monitoração de compartilhamento de dados em rede ou em nuvem, a partir do endpoint;

14.3.23.14. Monitoramento de páginas web acessadas, inclusive anônimas, com tempo de uso por janela;

14.3.23.15. Monitoramento de downloads de arquivos a partir de páginas web;

14.3.23.16. Monitoramento de transferência de arquivos por Bluetooth;

14.3.23.17. Monitoramento e coleta de eventos de logon e logoff de usuários, bloqueio e desbloqueio de sessão e acessos a compartilhamentos;

14.3.23.18. Monitoramento de alterações da configuração de segurança do navegador, possibilitando a abertura de brechas para vazamento ou acesso a dados sensíveis via WEB;

14.3.23.19. Monitoramento do uso de aplicativos capazes de realizar alterações e acessos a banco de dados Microsoft SQL Server;

14.3.24. **Coletas para investigação**

14.3.24.1. Permitir a coleta de, no mínimo, as seguintes informações para investigação, sendo remoto ou não:

14.3.24.2. Falhas de logon e logoff;

14.3.24.3. Logins paralelos;

14.3.24.4. Acessos a URL;

14.3.24.5. Logs do Windows com eventos de aplicação, segurança e sistema;

14.3.24.6. Deverá monitorar todos os acessos e conexões à área de trabalho remoto, identificando qual o processo utizado, tempo de sessão e IP remoto;

14.3.24.7. Histórico de usuários que realizaram logon no equipamento;

14.3.24.8. Portas de rede ativas;

14.3.24.9. Hash MD5, SHA1, SHA2 e SHA3;

14.3.24.10. Processos usando a API do Sistema Operacional;

14.3.24.11. Listagem de volumes;

14.3.25. **Deve ser capaz de identificar automaticamente e em tempo real a primeira detecção de eventos no endpoint:**

14.3.25.1. Conexões de rede;

14.3.25.2. Novas instalações de: Software; Serviço; Driver; Hardware;

14.3.25.3. Alterações/Modificações: Configuração de Autorun do Windows;Comportamento de Processos; Hardware; Tarefa agendada do Windows;

14.3.25.4. Capacidade de realizar uma verificação em tempo real se o evento no endpoint também é único em toda a rede, para identificação da origem do problema;

14.3.26. **Serviço de Gerenciamento da Solução**

14.3.26.1. O Serviço baseia-se em auditoria e governança do ambiente de TI, trazendo governança, conformidade, segurança e controle do ambiente.

14.3.26.2. O controle adequado do ambiente o fará aderente as boas práticas reduzindo abruptamente sua exposição e brechas para incidentes de segurança.

14.3.27. **Serviço de Diagnóstico:**

14.3.27.1. Consiste na avaliação contínua do ambiente, feita de forma cíclica e automatizada, sendo consolidada em relatórios periódicos padronizados.

14.3.27.2. Tem como propósito a identificação de inconformidades do ambiente que possam ser caracterizadas como vulnerabilidades. Serão gerados relatórios para cada estrutura de TI auditada pela solução (endpoint).

14.3.27.3. Os relatórios apresentam a lista de vulnerabilidades identificadas, criticidade, quantidade e localização. Com base no conteúdo extraído serão fornecidas recomendações gerais para remediação dos pontos identificados. Estas ações devem ser executadas pela equipe da **CONTRATANTE** a fim de mitigar o risco identificado.

14.3.27.4. Os relatórios são apresentados de forma periódica e são sempre comparados com os relatórios do último período apresentando adicionalmente uma visão de evolução/involução do ambiente para acompanhamento da alta gestão.

14.3.27.5. Será de responsabilidade da **CONTRATADA**a personalização e acompanhamento de painéis e alertas que são gerados em tempo real, identificando eventuais comportamentos anormais ou ocorrências que possam caracterizar possíveis falhas de segurança.

14.3.27.6. Os painéis refletem, em tempo real, os itens dos relatórios de diagnóstico e contém os indicadores que demonstram as possíveis vulnerabilidades ou comportamentos anormais, possibilitando a avaliação ações de reação ou mitigação a tentativas de ataques.

14.3.27.7. Os painéis fornecem visualizações do funcionamento dos elementos e serviços mais críticos de cada tópico (segurança, inventário, atividade de usuários e processos suspeitos) de modo que o monitorador possa visualizar qualquer anomalia, identificar sua origem e executar alguma ação de mitigação.

14.3.27.8. Os serviços serão executados para os seguintes componentes monitorados:

14.3.27.9. Atividade dos usuários, Compartilhamento de arquivos e Atividades das Estações de Trabalho;

14.3.27.10. Fornecer relatórios de métricas, indicadores de riscos ou de comprometimento, atualizados trimestralmente, acompanhando a mudança do cenário monitorado e surgimento de novos indiciadores.

14.3.27.11. Prover, sempre que demandado, informações de inventário de Hardware atualizados, exibindo todos os dispositivos conectados à rede, com informações detalhadas sobre seus componentes físicos (CPU, Memória, Disco e espaço utilizado, etc.) assim como todos os objetos em base de usuários e softwares e suas versões instalados nas máquinas.

14.3.27.12. Garantir que dispositivos e/ou softwares não autorizados sejam encontrados na rede ou máquinas monitoradas.

14.3.27.13. Apresentar quinzenalmente todas as estações de trabalho monitoradas que se

encontram em situação de vulnerabilidade, como por exemplo sistema operacional desatualizado ou antivírus desligado, assim como o nível de criticidade quando possível.

14.3.27.14. Apresentar quinzenalmente, usuários que realizem o uso de ferramentas de script, quando isso fugir de suas tarefas padrões de acordo com a política definida pelo órgão.

14.3.27.15. Averiguar quinzenalmente que todos os navegadores web das estações de trabalho estão em sua versão mais eficiente de trabalho, garantindo que apenas as ferramentas permitidas estão sendo usadas para execução dos trabalhos.

14.3.27.16. Revisão quinzenal de navegação web dos usuários em suas estações de trabalho, garantindo o acesso apenas a serviços de e-mail autorizados e sites que não apresentem alguma ameaça a disponibilidade dos serviços do tribunal.

14.3.27.17. Relatório de todas as estações identificadas nos últimos 30 dias como infectadas por artefatos comumente conhecidos como maliciosos ou que contenham em sua estrutura indicadores de motores usados em certos tipos de contaminação. Tal varredura também ocorrerá para dispositivos externos com funcionalidade de armazenamento, evidenciando caso ocorra o vazamento de alguma informação.

14.3.27.18. Monitoramento contínuo de todo escopo proposto através da coleta, tratamento e normalização de logs em formato leve, permitindo consultas ágeis da trilha de auditoria em casos de comportamentos suspeitos e atividades comumente entendidas como maliciosas.

14.3.27.19. Evidenciar sempre que algum artefato ou ação suspeita for identificado pela primeira vez em nas estações de trabalho, facilitando o rastreio de vetores de entrada à rede e, quando possível, alerta sobre ameaças em tempo hábil. Tal evidência deve ser enviada no período de até 2 horas úteis.

14.3.27.20. Parametrização e envio de alertas em tempo real quando alguma ação considerada suspeita ou maliciosa for realizada dentro do escopo monitorados. Será realizado as configurações junto ao tribunal ao fim de garantir a menor incidência de falso positivos possíveis.

14.3.28. **Manutenção e suporte Tecnico**:

14.3.28.1. A Manutenção E Suporte Técnico referente a prestação de serviços de Nuvem Pública devem estar de acordo com o especificado neste item.

14.3.28.2. O suporte e a manutenção deverão ser providos durante toda vigência do contrato.

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

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

14.3.28.5. A **CONTRATADA** deve ser emitido relatório mensal referente a atualização 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.

14.3.28.6. 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.

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

14.3.28.8. A **CONTRATADA**, deverá utilizar a ferramenta de ITSM própria, para registro de chamados e relatórios.

14.3.28.9. Todo chamado registrado, deve ser enviado notificação de forma automática aos fiscais do contrato.

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

14.3.28.11. Todo e qualquer problema detectado nos itens/serviços descritos neste Elemento Técnico, deverão ser, de forma imediata, ser relatados à equipe de Fiscais do **CONTRATANTE**.

14.3.28.12. Todas as mudanças adotadas por iniciativa da **CONTRATADA** nas configurações

14.3.28.13. deverão ser efetuadas mediante aprovação do **CONTRATANTE**.

14.3.28.14. A **CONTRATADA** deverá emitir uma declaração prévia, com antecedência mínima de 15 (quinze) dias, 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.

14.3.28.15. O suporte deverá incluir resposta a chamados críticos em tempo inferior a sessenta minutos e permitir a comunicação por meio de e-mail, chat e 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.

14.3.28.16. Os serviços de Suporte Técnico compreendem todos os chamados rela vos aos itens referenciados neste 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**.

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

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

14.3.28.19. 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, com SLA de 20 minutos 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.

14.3.28.20. 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%
	Deveremos entender como	20 minutos	Até 08 horas	

Baixa	Severidade Baixa os testes funcionais e consultas gerais do equipamento	20 minutos para captura de chamado	para resolução do problema	0,5%

14.3.29. **Obrigações da CONTRATADA:**

14.3.29.1. A **CONTRATADA**de prestar os serviços com pessoal adequadamente qualificado e capacitado para suas atividades.

14.3.29.2. Cumprir rigorosamente todas as programações e atividades do objeto do contrato.

14.3.29.3. Prestar os serviços de acordo com o especificado neste instrumento.

14.3.29.4. 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.

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

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

14.3.29.7. 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.

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

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

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

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

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

14.3.29.13. 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.

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

14.3.29.15. 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.

14.3.29.16. **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.

14.3.29.17. 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.

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

15. ANEXO V: LOTE 5 – PAAS - SERVIÇO DE LICENCIAMENTO MICROSOFT (MS)

15.1. Todos os itens relacionados no **Lote 5: PaaS - Serviço de Licenciamento Microsoft (MS),** somente serão executados sob demanda da **CONTRATANTE**, podendo ser descontinuados a qualquer momento pela **CONTREATANTE**

LOTE	ITEM	Subitem	Descrição	Métrica	QNTD	Valor	Valor Mensal	Valor Anual	Valor previsto

LOTE	ITEM	Subitem	Descrição	Métrica	(Previsto)	Unitário	Mensal previsto	Anual previsto	para 30 meses
5	PaaS - Serviço de Licenciamento Microsoft (MS)	5.1	Office 365 E1STANDARDPACK ou equivalente (por demanda)	Unidade/Mês	4.000	R$	R$	R$	R$
		5.2	Microsoft 365 E3SPE_E3 ou equivalente (por demanda)	Unidade/Mês	1.000	R$	R$	R$	R$
		5.3	Power BI ProPOWER_BI_PRO ou equivalente (por demanda)	Unidade/Mês	10	R$	R$	R$	R$
		5.4	Systencenter - SCCM (por demanda)	Unidade/Mês	1	R$	R$	R$	R$
		5.5	TS RDS licença per user (por demanda)	Unidade/Mês	200	R$	R$	R$	R$
		5.6	Azure Active Directory Premium P1 ou equivalente (por demanda)	Unidade/Mês	50	R$	R$	R$	R$
		5.7	Serviços Consultoria Técnica Especializada (por demanda)	Horas	4.000	R$	R$	R$	R$

15.2. **Especificação do Subitem 5.1 - Office 365 E1STANDARDPACK ou equivale (por demanda)**

a) O plano Office 365 E1 é uma solução integrada de colaboração e produtividade incluindo as seguintes funcionalidades: Office para aplicativos móveis e Office para Web com Word, PowerPoint, OneNote e Excel.

b) E-mail e calendários – Exchange Online com experiência do Outlook, caixa de correio de 50GB, caixa de correio de arquivo morto de 50GB, caixas de correio compartilhadas de 50GB e anexos de até 150MB.

c) Hub para trabalho em equipe – Microsoft Teams que reúne chats, conteúdo, pessoas e ferramentas. Pesquisa e mensagens ilimitadas, acesso para convidado, versão web dos aplicativos Word, PowerPoint, Excel e OneNote no Teams, domínio de e-mail personalizado e hospedagem de e-mails do Exchange, mais de 140 aplicativos e serviços integrados e armazenamento de arquivos.

d) Reuniões online – Microsoft Teams com áudio, vídeo em alta definição, webconferência e streaming. Chamadas de áudio e vídeo online individuais e em grupo, reuniões de canal, compartilhamento de tela, reuniões agendadas, gravação de reunião, audioconferência.

e) Social e intranet – Sharepoint Online e Yammer que reúnem gerenciamento de conteúdo, sites de equipes, compartilhamento de arquivos, dados, notícias e recursos, acesso para convidado, intranet móvel e inteligente, portais, notificações e aprovações, fluxos de trabalho, rede social corporativa, eventos ao vivo incluindo reuniões abertas, reuniões corporativas e treinamentos, comunidades de interesse, portal de ideias e comentários.

f) Arquivos – OneDrive for Business com 1TB de armazenamento. Solução segura de arquivos em nuvem, compartilhamento, controle de acesso e edição colaborativa.

g) Arquivos – OneDrive for Business com 1TB de armazenamento. Solução segura de arquivos em nuvem, compartilhamento, controle de acesso e edição colaborativa.

h) Conteúdo – Microsoft Stream e Sway que reúnem serviço de streaming de vídeo, recursos de conversão de voz em texto, legendas automáticas e detecção de rosto, retenção de conhecimento e

engajamento em treinamentos e cursos, criação e compartilhamento de relatórios interativos, histórias pessoais e apresentações.

i) Gerenciamento de tarefas – Microsoft Planner e Microsoft To Do que reúnem planos e planejamentos pessoais e de equipes com controle de atividades, organização e atribuição de tarefas, compartilhamento de arquivos e chat sobre trabalho.

j) Aplicativos de negócios - Microsoft Power Apps e Microsoft Power Automate que reúnem ferramentas de low-code para criação de aplicativos, fluxos de trabalho, automação de processos e formulários personalizados.

k) Análise de produtividade pessoal – Microsoft MyAnalytics com insights de produtividade pessoal, conectado ao Outlook, que utilizam Inteligência Artificial para sugerir formas de trabalhar com mais inteligência, melhorando foco, bem-estar, contatos e colaboração.

l) Microsoft Graph API – API e gateway do Office 365 para dados e inteligência. As APIs REST ou SDKs permitem acessar pontos de extremidade e desenvolver aplicativos compatíveis com cenários que abrangem produtividade, colaboração, educação, segurança, identidade, acesso, gerenciamento de dispositivo dentre outras funcionalidades.

m) Office Delve – Gerenciamento de perfil individual do Office 365 com ferramentas para descobrir e organizar informações importantes.

n) Sincronização com Active Directory on-premise para single sign-on (SSO).

o) Gerenciamento de Dispositivos Móveis para Office 365 – funcionalidades de gerenciamento para iOS, Android e Windows Phone, inventário de dispositivos móveis que acessam aplicações corporativas, limpeza total ou seletiva do dispositivo, definições de configuração do dispositivo móvel (comprimento do PIN, PIN necessário, tempo de bloqueio, dentre outros), certificação raiz e detecção de jailbreak, controle de acesso a e-mail e documentos corporativos com base em políticas de conformidade e relatórios.

p) Licença cliente de acesso padrão, Client Access License (CAL), aos serviços on-premise do Exchange Server, SharePoint Server e Skype for Business Server.

q) Permite a classificação manual do recurso Data Governance e a aplicação manual de políticas para retenção e detenção de dados.

r) eDiscovery search.

15.3. **Especificação do Subitem 5.2 - Microsoft 365 E3SPE_E3 ou equivalente (por demanda)**

a) O plano Office 365 E3 é uma solução integrada de colaboração e produtividade incluindo as seguintes funcionalidades: a. Aplicativos cliente do Office (Outlook, Word, Excel, PowerPoint, OneNote, Access e Publisher) em até 05 (cinco) PCs/Macs + cinco tablets + cinco smartphones por pessoa com o Office 365 ProPlus.

b) E-mail e calendários – Exchange Online com experiência do Outlook, caixa de correio de 100GB, caixa de correio de arquivo morto ilimitada, caixas de correio compartilhadas de 50GB e anexos de até 150MB

c) Hub para trabalho em equipe – Microsoft Teams que reúne chats, conteúdo, pessoas e ferramentas. Pesquisa e mensagens ilimitadas, acesso para convidado, versão web dos aplicativos Word, PowerPoint, Excel e OneNote no Teams, domínio de e-mail personalizado e hospedagem de e-mails do Exchange, mais de 140 aplicativos e serviços integrados e armazenamento de arquivos.

d) Reuniões online – Microsoft Teams com áudio, vídeo em alta definição, webconferência e streaming. Chamadas de áudio e vídeo online individuais e em grupo, reuniões de canal, compartilhamento de tela, reuniões agendadas, gravação de reunião, audioconferência.

e) Social e intranet – Sharepoint Online e Yammer que reúnem gerenciamento de conteúdo, sites de equipes, compartilhamento de arquivos, dados, notícias e recursos, acesso para convidado, intranet móvel e inteligente, portais, notificações e aprovações, fluxos de trabalho, rede social corporativa, eventos ao vivo incluindo reuniões abertas, reuniões corporativas e treinamentos, comunidades de interesse, portal de ideias e comentários.

f) Arquivos – OneDrive for Business com armazenamento ilimitado. Solução segura de arquivos em nuvem, compartilhamento, controle de acesso e edição colaborativa. h. Conteúdo – Microsoft Stream e Sway que reúnem serviço de streaming de vídeo, recursos de conversão de voz em texto, legendas automáticas e detecção de rosto, retenção de conhecimento e engajamento em treinamentos e cursos, criação e compartilhamento de relatórios interativos, histórias pessoais e apresentações.

g) Gerenciamento de tarefas – Microsoft Planner e Microsoft To Do que reúnem planos e

planejamentos pessoais e de equipes com controle de atividades, organização e atribuição de tarefas, compartilhamento de arquivos e chat sobre trabalho.

h) Aplicativos de negócios - Microsoft Power Apps e Microsoft Power Automate que reúnem ferramentas de low-code para criação de aplicativos, fluxos de trabalho, automação de processos e formulários personalizados.

i) Análise de produtividade pessoal – Microsoft MyAnalytics com insights de produtividade pessoal, conectado ao Outlook, que utilizam Inteligência Artificial para sugerir formas de trabalhar com mais inteligência, melhorando foco, bem-estar, contatos e colaboração.

j) Microsoft Graph API – API e gateway do Office 365 para dados e inteligência. As APIs REST ou SDKs permitem acessar pontos de extremidade e desenvolver aplicativos compatíveis com cenários que abrangem produtividade, colaboração, educação, segurança, identidade, acesso, gerenciamento de dispositivo dentre outras funcionalidades.

k) Office Delve – Gerenciamento de perfil individual do Office 365 com ferramentas para descobrir e organizar informações importantes.

l) Sincronização com Active Directory on-premise para single sign-on (SSO).

m) Gerenciamento de Dispositivos Móveis para Office 365 – funcionalidades de gerenciamento para iOS, Android e Windows Phone, inventário de dispositivos móveis que acessam aplicações corporativas, limpeza total ou seletiva do dispositivo, definições de configuração do dispositivo móvel (comprimento do PIN, PIN necessário, tempo de bloqueio, dentre outros), certificação raiz e detecção de jailbreak, controle de acesso a e-mail e documentos corporativos com base em políticas de conformidade e relatórios.

n) Licença cliente de acesso padrão, Client Access License (CAL), aos serviços on-premise do Exchange Server, SharePoint Server e Skype for Business Server. q. Suporte à diretivas de grupo, telemetria do Office e configurações de Roaming. r. Necessidades legais de conformidade e arquivamento de e-mail – arquivamento, descoberta eletrônica, retenção de caixa de correio. s. Proteção de informações – criptografia de mensagens, gerenciamento de direitos, prevenção de perda de dados para e-mail e arquivos.

15.4. **Especificação do Subitem 5.3 - Power BI ProPOWER_BI_PRO ou equivalente**

a) Conjunto de serviços para comunicar seus dados em qualquer ambiente que eles estejam (local ou na nuvem), permitindo que crie visualizações, aplicar filtros, publicar e compartilhar relatórios e Dashboards

b) Power BI é uma ferramenta usada para analisar e visualizar os dados em modelo self Service, para que usuários tenha independência para criar visualições de Dados. É uma ferramenta para reunir, transformar e criar insights e gráficos a partir de grandes conjuntos de dados e compartilhar com outras pessoas.

15.5. **Especificação do Subitem 5.4 – Systencenter – SCCM (por demanda**)

a) Produto do Windows que permite o gerenciamento, a implantação e a segurança de dispositivos e aplicativos em uma empresa. Entre outros usos potenciais, os administradores geralmente usam o SCCM para proteção de endpoint, gerenciamento de patches e distribuição de software

15.6. **Especificação do Subitem 5.5 – TS RDS (licença per user até 200) (por demanda**)

a) Permitir conexões remotas ao ambiente windows server

15.7. **Especificação do Subitem 5.6 – Azure Active Directory Premium P1 ou equivalente (por demanda**)

a) Fornece gerenciamento de usuários e de grupos, sincronização de diretório local, relatórios básicos, autoatendimento para alteração de senha e logon único no Azure, no Microsoft 365.

b) Suporte à administração avançada, como grupos dinâmicos, gerenciamento de grupos de autoatendimento, Microsoft Identity Manager e recursos de write-back de nuvem, que permitem a redefinição de senha por autoatendimento para os usuários locais

15.8. **Especificação do Subitem 5.7 – Serviços Consultoria Técnica Especializada (sob demanda)**

15.8.1. A **CONTRATADA**deverá apresentar um Contrato de Serviços Técnicos Especializados com o fabricante Microsoft para Suporte Premier especificamente para atender o IGESDF que garanta, quando demandado em atividades e projetos, durante toda a vigência do contrato, acesso à base de conhecimento interna de melhores práticas em projetos realizados, acesso ao código fonte, engenheiros arquitetos e laboratórios de testes dos produtos e aplicações.

15.8.2. Os serviços de Suporte Premier deverão estar disponíveis para acionamento:

a) Para incidentes e problemas: regime de 24 horas x 7 dias na semana x 365 dias no ano, via chamado da Central de Serviços da **CONTRATADA** ;

b) Para a prestação dos Serviços de Arquitetura Tecnológica e Suporte Premier, a **CONTRATADA** deverá disponibilizar recursos técnicos do próprio fabricante.

15.8.3. A **CONTRATADA** deverá designar um profissional adequado do Fabricante para ajudar a gerenciar incidentes críticos ou não, incluindo incidentes de nível inferior focados em promover melhorias proativas no ambiente da solução. Juntamente com o Gerente de Contrato de Serviços, o profissional designado do Fabricante deverá conduzir o gerenciamento de incidentes e escalonamento, incluindo o Gerenciamento 24x7x365 para escalonamento de uma situação crítica de um incidente.

15.8.4. A **CONTRATADA**deverá comprovar ter mecanismos que permitam o IGESDF o uso da Base de Conhecimento exclusiva da Microsoft em prol da melhor realização dos projetos realizados.

15.8.5. Fornecer uma interface de gerenciamento de escalonamento e incidentes com o Fabricante Microsoft, fornecendo suporte a escalonamento e gerenciamento de incidentes.

15.8.5.1. O suporte deverá incluir resposta a chamados críticos em tempo inferior a sessenta minutos e permitir a comunicação por meio de e-mail, chat e 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.

15.8.5.2. Os serviços de Suporte Técnico compreendem todos os chamados rela vos aos itens referenciados neste 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**.

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

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

15.8.5.5. 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, com SLA de 20 minutos 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.

15.8.5.6. 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	Desconto por não atendimento

		atendimento	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%

15.8.6. **Obrigações da CONTRATADA:**

15.8.6.1. A **CONTRATADA**de prestar os serviços com pessoal adequadamente qualificado e capacitado para suas atividades.

15.8.6.2. Cumprir rigorosamente todas as programações e atividades do objeto do contrato.

15.8.6.3. Prestar os serviços de acordo com o especificado neste instrumento.

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

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

15.8.6.6. 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.

15.8.6.7. 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.

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

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

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

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

15.8.6.12. 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.

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

15.8.6.14. 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.

15.8.6.15. **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.

15.8.6.16. 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.

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

16. **ANEXO VI - PROPOSTA**

Ao XXXXXXXXXXX de XXXXXX do XXXXXX

A empresa _____ (razão social), inscrita no CNPJ sob o número_____, inscrição estadual número _____ , sediada no endereço (citar endereço completo), para fins de participação no presente processo Seleção de Fornecedores n.º _____, vem pela presente apresentar - em anexo - sua proposta de preços, de acordo com as exigências do Ato Convocatório supracitado.

LOTE	ITEM	Subitem	Tipo de Instancia	Métrica	USN (Previsto)	Valor Unitário	Valor Mensal previsto	Valor Anual previsto	Valor previsto para 30 meses
		1.1	Instancia - 1 (Linux) com 1 vCPU e 2 GB de memória RAM (por demanda)	Instancia/Mês	1.500.000	R$	R$	R$	R$
			Instancia - 2 (Linux) com 2 vCPU e 4 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 3 (Linux) com 4 vCPU e 8 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 4 (Linux) com 4 vCPU e 16 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 5 (Linux) com 8 vCPU e 32 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 6 (Linux) com 16 vCPU e 64 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 7 (Linux) com 32 vCPU e 64 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 8 (Linux) com 32 vCPU e 128 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 9 (Windows) com 1 vCPU e 2 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 10 (Windows) com 2 vCPU e 4 GB de memória			R$	R$	R$	R$

			RAM (por demanda)						
1	IaaS - Nuvem Pública		Instancia - 11 (Windows) com 2 vCPU e 8 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 12 (Windows) com 4 vCPU e 16 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 13 (Windows) com 8 vCPU e 32 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 14 (Windows) com 16 vCPU e 64 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 15 (Windows) com 32 vCPU e 64 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 16(Windows) com 32 vCPU e 128 GB de memória RAM (por demanda)			R$	R$	R$	R$
		Subitem	**Descrição**	**Métrica**	**QNTD. (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
		1.2	Serviço de Storage Block-Level SSD (por demanda)	TB/Mês	100	R$	R$	R$	R$
		1.3	Serviço de Storage Block-Level HDD (por demanda)	TB/Mês	100	R$	R$	R$	R$
		1.4	Serviço de Storage File-Level (por demanda)	TB/Mês	50	R$	R$	R$	R$
		1.5	Serviço de backup e restore (por demanda)	Mensal	200	R$	R$	R$	R$
		1.6	Balanceamento de carga (por demanda)	Unidade/Mês	20	R$	R$	R$	R$
		1.7	Porta de conexão de fibra 1 GBPS (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		1.8	Porta de conexão de fibra 10 gbps (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		1.9	Serviço de Tráfego de Saída de Rede (por	Mensal	100	R$	R$	R$	R$

			demanda)						
		1.10	Serviço de DNS (por demanda)	Mensal	100	R$	R$	R$	R$
		1.11	Serviço de VPN (por demanda)	Unidade/Mês	20	R$	R$	R$	R$
		1.12	Serviço de Web Application Firewall (por demanda)	Unidade/Mês	200	R$	R$	R$	R$
		1.13	Serviço de Autenticação Integrado com AD (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		1.14	Serviço de Monitoramento (por demanda)	Unidade/Mês	1	R$	R$	R$	R$
		1.15	Serviços Especializados de Nuvem Pública (por demanda)	Hora	4.000	R$	R$	R$	R$
LOTE	**ITEM**	**Subitem**	**Descrição**	**Métrica**	**QNTD (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
2	SaaS - Serviço de Next Generation Firewall	2.1	Serviço Next Generation Firewall do TIPO 1 (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		2.2	Serviço Next Generation Firewall do TIPO 2 (por demanda)	Unidade/Mês	20	R$	R$	R$	R$
LOTE	**ITEM**	**Subitem**	**Descrição**	**Métrica**	**QNTD (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
3	SaaS - Serviço de Conectividade e Controle de acesso	3.1	Serviço Conectividade de Rede – Tipo 1 (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		3.2	Serviço Conectividade de Rede – Tipo 2 (por demanda)	Unidade/Mês	90	R$	R$	R$	R$
		3.3	Serviço Conectividade de Rede – Tipo 3 (por demanda)	Unidade/Mês	60	R$	R$	R$	R$
		3.4	Serviço de Conectividade Sem Fio (por de manda)	Unidade/Mês	300	R$	R$	R$	R$
		3.5	Software de Controle de Acesso à Rede (por de manda)	Unidade/Mês	1	R$	R$	R$	R$
LOTE	**ITEM**	**Subitem**	**Descrição**	**Métrica**	**QNTD (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**

4	SaaS - Serviço de Proteção de EndPoints e Auditoria	4.1	Serviço de proteção de EndPoints (por demanda)	Unidade/Mês	4.000	R$	R$	R$	R$
		4.2	Serviço de Auditoria (por demanda)	Unidade/Mês	4.000	R$	R$	R$	R$
LOTE	**ITEM**	**Subitem**	**Descrição**	**Métrica**	**QNTD (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
5	PaaS - Serviço de Licenciamento Microsoft (MS)	5.1	Office 365 E1STANDARDPACK ou equivalente (por demanda)	Unidade/Mês	4.000	R$	R$	R$	R$
		5.2	Microsoft 365 E3SPE_E3 ou equivalente (por demanda)	Unidade/Mês	1.000	R$	R$	R$	R$
		5.3	Power BI ProPOWER_BI_PRO ou equivalente (por demanda)	Unidade/Mês	10	R$	R$	R$	R$
		5.4	Systencenter - SCCM (por demanda)	Unidade/Mês	1	R$	R$	R$	R$
		5.5	TS RDS licença per user (por demanda)	Unidade/Mês	200	R$	R$	R$	R$
		5.6	Azure Active Directory Premium P1 ou equivalente (por demanda)	Unidade/Mês	50	R$	R$	R$	R$
		5.7	Serviços Consultoria Técnica Especializada (por demanda)	Horas	4.000	R$	R$	R$	R$

1. Prazo de validade da proposta é de 90 (noventa) dias corridos, contados a partir da sua assinatura.

2. Declaramos estar cientes de todas as cláusulas do instrumento convocatório, bem como de seus anexos.

3. Apresentamos, conforme exigido no Ato Convocatório, os dados bancários para pagamento mediante depósito bancário em conta corrente, constando:

a) Nome e número do Banco:

b) Agência:

c) Número da conta concorrente:

4. Declaramos que nos preços cotados estão incluídas todas as despesas, tais como tributos, seguros, transporte, pagamento de mão de obra, treinamento, frete até o destino, seguros, garantia e todos os demais encargos e/ou descontos porventura existentes.

Local/data

_____

(Assinatura do responsável pela empresa)

Nome/Cargo

17. ANEXO VII – ORDEM SERVIÇO

ORDEM DE SERVIÇO

Por intermédio da Ordem de Serviço será solicitado formalmente à **CONTRATADA** a prestação de serviço

IDENTIFICAÇÃO			
OS Nº:	_____/20_____		
Contrato N°:	_____/20_____		
Contratada:	.		
Data da Emissão:	____/____/____	**Área Requisitante do Serviço**:	_____/IGESDF
Usuário Solicitante ou Setor Solicitante:		**Nº do Processo SEI:**	
E-mail:	_____@igesdf.org.br		
Telefone:	(61) 3550-8900 ramal: 9236		
Objeto:	**<Descrição referente ao Lote Contratado>**		

LOTE	ITEM	Subitem	Tipo de Instancia	Métrica	USN (Previsto)	Valor Unitário	Valor Mensal previsto	Valor Anual previsto	Valor previsto para 30 meses
			Instancia - 1 (Linux) com 1 vCPU e 2 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 2 (Linux) com 2 vCPU e 4 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 3 (Linux) com 4 vCPU e 8 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 4 (Linux) com 4 vCPU e 16 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 5 (Linux) com 8 vCPU e 32 GB de memória RAM (por			R$	R$	R$	R$

			demanda)						
1	IaaS - Nuvem Pública	1.1	Instancia - 6 (Linux) com 16 vCPU e 64 GB de memória RAM (por demanda)	Instancia/Mês	1.500.000	R$	R$	R$	R$
			Instancia - 7 (Linux) com 32 vCPU e 64 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 8 (Linux) com 32 vCPU e 128 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 9 (Windows) com 1 vCPU e 2 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 10 (Windows) com 2 vCPU e 4 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 11 (Windows) com 2 vCPU e 8 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 12 (Windows) com 4 vCPU e 16 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 13 (Windows) com 8 vCPU e 32 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 14 (Windows) com 16 vCPU e 64 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 15 (Windows) com 32 vCPU e 64 GB de memória RAM (por demanda)			R$	R$	R$	R$
			Instancia - 16(Windows) com 32 vCPU e 128 GB de memória RAM (por demanda)			R$	R$	R$	R$
		Subitem	**Descrição**	**Métrica**	**QNTD. (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
		1.2	Serviço de Storage Block-Level SSD (por demanda)	TB/Mês	100	R$	R$	R$	R$

		1.3	Serviço de Storage Block-Level HDD (por demanda)	TB/Mês	100	R$	R$	R$	R$
		1.4	Serviço de Storage File-Level (por demanda)	TB/Mês	50	R$	R$	R$	R$
		1.5	Serviço de backup e restore (por demanda)	Mensal	200	R$	R$	R$	R$
		1.6	Balanceamento de carga (por demanda)	Unidade/Mês	20	R$	R$	R$	R$
		1.7	Porta de conexão de fibra 1 GBPS (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		1.8	Porta de conexão de fibra 10 gbps (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		1.9	Serviço de Tráfego de Saída de Rede (por demanda)	Mensal	100	R$	R$	R$	R$
		1.10	Serviço de DNS (por demanda)	Mensal	100	R$	R$	R$	R$
		1.11	Serviço de VPN (por demanda)	Unidade/Mês	20	R$	R$	R$	R$
		1.12	Serviço de Web Application Firewall (por demanda)	Unidade/Mês	200	R$	R$	R$	R$
		1.13	Serviço de Autenticação Integrado com AD (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		1.14	Serviço de Monitoramento (por demanda)	Unidade/Mês	1	R$	R$	R$	R$
		1.15	Serviços Especializados de Nuvem Pública (por demanda)	Hora	4.000	R$	R$	R$	R$
LOTE	**ITEM**	**Subitem**	**Descrição**	**Métrica**	**QNTD (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
2	SaaS - Serviço de Next Generation Firewall	2.1	Serviço Next Generation Firewall do TIPO 1 (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		2.2	Serviço Next Generation Firewall do TIPO 2 (por demanda)	Unidade/Mês	20	R$	R$	R$	R$
LOTE	**ITEM**	**Subitem**	**Descrição**	**Métrica**	**QNTD (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
			Serviço Conectividade						

3	SaaS - Serviço de Conectividade e Controle de acesso	3.1	de Rede – Tipo 1 (por demanda)	Unidade/Mês	4	R$	R$	R$	R$
		3.2	Serviço Conectividade de Rede – Tipo 2 (por demanda)	Unidade/Mês	90	R$	R$	R$	R$
		3.3	Serviço Conectividade de Rede – Tipo 3 (por demanda)	Unidade/Mês	60	R$	R$	R$	R$
		3.4	Serviço de Conectividade Sem Fio (por de manda)	Unidade/Mês	300	R$	R$	R$	R$
		3.5	Software de Controle de Acesso à Rede (por de manda)	Unidade/Mês	1	R$	R$	R$	R$
LOTE	**ITEM**	**Subitem**	**Descrição**	**Métrica**	**QNTD (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
4	SaaS - Serviço de Proteção de EndPoints e Auditoria	4.1	Serviço de proteção de EndPoints (por demanda)	Unidade/Mês	4.000	R$	R$	R$	R$
		4.2	Serviço de Auditoria (por demanda)	Unidade/Mês	4.000	R$	R$	R$	R$
LOTE	**ITEM**	**Subitem**	**Descrição**	**Métrica**	**QNTD (Previsto)**	**Valor Unitário**	**Valor Mensal previsto**	**Valor Anual previsto**	**Valor previsto para 30 meses**
5	PaaS - Serviço de Licenciamento Microsoft (MS)	5.1	Office 365 E1STANDARDPACK ou equivalente (por demanda)	Unidade/Mês	4.000	R$	R$	R$	R$
		5.2	Microsoft 365 E3SPE_E3 ou equivalente (por demanda)	Unidade/Mês	1.000	R$	R$	R$	R$
		5.3	Power BI ProPOWER_BI_PRO ou equivalente (por demanda)	Unidade/Mês	10	R$	R$	R$	R$
		5.4	Systencenter - SCCM (por demanda)	Unidade/Mês	1	R$	R$	R$	R$
		5.5	TS RDS licença per user (por demanda)	Unidade/Mês	200	R$	R$	R$	R$
		5.6	Azure Active Directory Premium P1 ou equivalente (por demanda)	Unidade/Mês	50	R$	R$	R$	R$
		5.7	Serviços Consultoria Técnica Especializada (por demanda)	Horas	4.000	R$	R$	R$	R$

ARTEFATOS / PRODUTOS	
A serem gerados e/ou atualizados	
Lote 1:IaaS - Nuvem Pública	**Todos os relatórios de entrega, devem ser alinhados com a Gerência de TI e Fiscal do Contrato**
Lote 2: SaaS - Serviço de Next Generation Firewall	
Lote 3: SaaS - Serviço de Conectividade e Controle de acesso	
Lote 4: SaaS - Serviço de Proteção de EndPoints e Auditoria	
Lote 5: PaaS - Serviço de Licenciamento Microsoft (MS)	

CIÊNCIA	
CONTRATANTE	
Gestor do Contrato	**Fiscal do Contrato**
Brasília, ____ de _____ de 20___ Nome: Cargo: Matrícula:	Brasília, ____ de _____ de 20___ Nome: Cargo: Matrícula:
CONTRATADA	
Brasília, ____ de _____ de 20___ Responsável da empresa **CONTRATADA**	

18. **ANEXO VIII - ORDEM DE FORNECIMENTO**

ORDEM DE FORNECIMENTO Nº _____

Solicitamos à Empresa _____, fornecer os itens especificados abaixo nos locais especificados, em conformidade com o objeto, Anexo III do Contrato Nº _____, Ato Convocatório Mercado Digital Nº _____ - IGESDF

LOTE	ITEM	Descrição	Qntde.	Local de entrega

Brasília, _____ de _____ de 20__.

_____

NOME:

Cargo:

Matrícula:

19. ANEXO IX – UNIDADES DO IGESDF

Unidades IGESDF	Endereço
Hospital de Base – HBDF	SMHS - Área Especial, Q. 101 - Asa Sul, Brasília - DF,
Hospital Regional de Santa Maria – HRSM	AC 102, Blocos, Conj. A/B/C - Santa Maria, Brasília - DF,
PO700	SRTV 702, Via W5 Norte, Brasília - DF,
SIA	SIA TRECHO 17, RUA 06, LOTE 115 - SETOR DE INDÚSTRIA E ABASTECIMENTO/BRASÍLIA-DF
UPA - Ceilândia	Área Especial D, Via P1 Norte - Ceilândia, Brasília - DF,
UPA - Núcleo Bandeirante	DF-075, Km 180, Área Especial, EPNB, Brasília - DF,
UPA - Recanto das Emas	Quadra 400-600 s/n, Área Especial, Brasília - DF,
UPA - São Sebastiao	QD 102 conj 1 LT 1, Residencial Oeste, São Sebastião
UPA - Samambaia	QS 107 Conjunto 04 Área especial 01
UPA - Sobradinho	DF 420, em frente a AR 13, próximo ao COER Sobradinho II DF
UPA - Brazlândia	Vila São José, Q 37, AE1, Posto de Saúde
UPA – Ceilândia (Setor O)	Expansão do Setor O, QNO 21 AE D
UPA – Gama	Setor de Indústria QI 7, Área Reservada 2
UPA – Paranoá	Paranoá Parque Q 1/2 Comercial 1 AE 4 EPC
UPA – Planaltina	Quadra 22, MD 1, Lote AE1, Setor Habitacional Mestre d'Armas
UPA – Riacho Fundo II	QN 31 Conjunto 3 Lote 1
UPA – Vicente Pires	Rua 10 QD 4D Chácara 135

20. ANEXO X - FISCAL DO CONTRATO E SEU RESPECTIVO SUBSTITUTO

DESIGNAÇÃO DE FISCAL E FISCAL SUBSTITUTO		
	Fiscal Titular / Substituto	**Fiscal Titular / Substituto**

NOME	Thiago de Lacerda Chaves	Israel de Freitas Cavalcante
CPF	70203490134	3383070107
MATRICULA	12361	12360
CARGO	NURED	NUTEL

Documento assinado eletronicamente por **THIAGO DE LACERDA CHAVES - Matr.0001236-1**, **Chefe do Núcleo de Rede**, em 12/05/2023, às 10:25, 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 **ANDERSON JESUS DE MENEZES Matr.0001406-6**, **Gerente de Infraestrutura de Tecnologia da Informação e Comunicação**, em 12/05/2023, às 11:10, 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 **GUSTAVO MAGNO DA CRUZ - Matr. 0001203-9**, **Gerente Geral de Logística de Serviços**, em 12/05/2023, às 12:59, 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 **CARLOS FERNANDO DAL SASSO DE OLIVEIRA - Matr.0001203-7**, **Superintendente da Unidade Central de Administração**, em 16/05/2023, às 16:43, 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= **112468079** código CRC= **D311D15D**.