GOVERNO DO DISTRITO FEDERAL

INSTITUTO DE GESTÃO ESTRATÉGICA DE SAÚDE DO DISTRITO FEDERAL

Gerência de Infraestrutura de Tecnologia da Informação e Comunicação

Núcleo de Rede

Unidade: GGTEC

Solicitante: Sergio Gustavo Evangelista da Mata

Interessado/Responsável: Sergio Gustavo Evangelista da Mata

E-mail: infraestrutura@igesdf.org.br

Contato: (61) 3315-8900 **Ramal:** 9236

1. DO OBJETO

1.1. O presente Elemento Técnico tem por objeto a contratação de empresa especializada na prestação de serviços para provimento de infraestrutura de tecnologia nas modalidades on-premises, em cloud pública, serviços de cloud, SaaS, Segurança da Informação e Serviços Especializados para atendimento às demandas do IGESDF. Todos os itens contidos neste objeto deverão ser fornecidos na modalidade as *a service*, ou seja, como serviços, considerando o custo por hora dos ativos e recursos a serem suportados, conforme volumetria, arquitetura de infraestrutura e necessidades que porventura surgirem de computação em nuvem, disponibilização de solução contra ameaças digitais e serviço de mensageria e colaboração em nuvem distribuídos, necessários para garantir a operação dos serviços de TI do Instituto de Gestão Estratégica de Saúde do Distrito Federal – IGESDF.

1.2. A solução será composta por:

LOTE	ITEM	SUB ITEM	DETALHAMENTO	UNIDADE	QTDE
	1 - IaaS On-premises	1.1	Infraestrutura como Serviço - Hiperconvergência, reservada por 1 ano *	Node/ Ano	5
		1.2	Disponibilização de antivírus para servidores Windows e Linux	Servidor/Mês	150
		1.3	Serviço de proteção de endpoints integrados com EDR *	Estação/Mês	10000
		1.4	Disponibilização de Next Generation Firewall em Alta Disponibilidade - TIPO 1	Unidade/Mês	2
		1.5	Disponibilização de Next Generation Firewall em Alta Disponibilidade - TIPO 2	Unidade/Mês	13
		1.6	Transceiver para Next Generation Firewall - TIPO 1	Unidade/Mês	30
		1.7	Transceiver para Next Generation Firewall - TIPO 2	Unidade/Mês	30
		1.8	Transceiver para Next Generation Firewall - TIPO 3	Unidade/Mês	30

		1.9	Transceiver para Next Generation Firewall - TIPO 4	Unidade/Mês	30
		1.10	Transceiver para Next Generation Firewall - TIPO 5	Unidade/Mês	30
		1.11	Transceiver para Next Generation Firewall - TIPO 6	Unidade/Mês	30
		1.12	Serviço de controle de acesso seguro a rede LAN e WLAN, reserva por 1 ano.	Instância 500 Usuários	5
	ITEM	**SUB ITEM**	**DESCRIÇÃO DO SERVIÇO (POR RESERVA DE RECURSO)**	**UNIDADE**	**QTDE**
1	**2 - IaaS Cloud Pública**	2.1	Máquina virtual padrão - adquirida por meio de vCPU, reservada por 1 ano	Unidade de vCPU/hora	1986000
		2.2	Máquina virtual padrão - adquirida por meio de memória, reservada por 1 ano	Gigabyte de memória/hora	
		2.3	Máquina virtual Windows - adquirida por meio de vCPU, reservada por 1 ano	Unidade de vCPU/hora	
		2.4	Máquina virtual Windows - adquirida por meio de memória, reservada por 1 ano	Gigabyte de memória/hora	
		2.5	Máquina virtual com serviço de hospedagem de container gerenciado - adquirida por meio de vCPU, reservada por 1 ano	Unidade de vCPU/hora	
		2.6	Máquina virtual padrão - adquirida por meio de vCPU (por demanda)	Unidade de vCPU/hora	
		2.7	Máquina virtual padrão - adquirida por meio de memória (por demanda)	Gigabyte de memória/hora	
		2.8	Máquina virtual Windows - adquirida por meio de vCPU (por demanda)	Unidade de vCPU/hora	
		2.9	Máquina virtual Windows - adquirida por meio de memória (por demanda)	Gigabyte de memória/hora	
		2.10	Serviço de armazenamento de blocos (SSD)	Gigabyte/mês	
		2.11	Serviço de armazenamento de blocos (HDD)	Gigabyte/mês	
		2.42	Serviço de armazenamento de objetos	Gigabyte/mês	
		2.13	Tráfego de saída da rede	Gigabyte/mês	
		2.14	Tráfego de rede do balanceador de carga	Gigabyte/mês	
		2.15	Tráfego de rede do CDN	Gigabyte/mês	
		2.16	Serviço de balanceamento de carga (*)	Unidade/hora	
		2.17	Serviço de balanceamento de carga utilizando gerenciador de tráfego (*)	DNS Queries Milhão/Mês	
		2.18	Porta de conexão de fibra 10Gbps	Unidade/hora	
		2.19	Serviço de DNS – Hospedagem de zonas	Zona/mês	
		2.20	Serviço de DNS – Consultas	Milheiro de consulta/mês	
		2.21	Serviço de VPN	Gigabyte/Mês	
		2.22	Serviço de VPN Gateway	Hora de Conexão	
		2.23	Serviço Web Aplication Firewall adquirido por regra de ACL (**)	ACL/hora	
		2.24	Serviço Web Aplication Firewall adquirido por hora (**)	Gateway/hora	

		2.25	Serviço de Backup	Instância/mês	
		2.26	Serviço de armazenamento de Backup	Gigabyte/mês	
		2.27	Serviço de Autenticação (Integração com AD) adquirido por usuário (***)	Por usuário/Mês	
		2.28	Serviço de Autenticação (Integração com AD) adquirido por mês (***)	Gigabyte/Mês	
		2.29	Serviço de Auditoria e Análise de Logs	Gigabyte/Mês	
		2.30	IP Público	Unidade/Mês	
		2.31	Serviços de BI	Unidade/Mês	
		2.32	Serviços de Plataforma de Gerencia para BI	Unidade/Mês	
	ITEM	**SUB ITEM**	**DETALHAMENTO**	**UNIDADE**	**QTDE**
	3 - Serviços de Cloud	3.1	Disponibilização de caixas postais e colaboração TIPO I	Usuário / mês	10000
		3.2	Disponibilização de caixas postais e colaboração TIPO II	Usuário / mês	1500
	ITEM	**SUB ITEM**	**DETALHAMENTO**	**UNIDADE**	**QTDE**
	4 - SaaS - Business Inteligence em Cloud	4.1	Serviço de fornecimento de software de análise de dados , reservado 1 ano	Servidor	1
		4.2	Treinamentos direcionados de BI	Turma	2
		4.3	Serviços Especializados em Business Intelligence (BI).	Horas	1080
	ITEM	**SUB ITEM**	**DETALHAMENTO**	**UNIDADE**	**QTDE**
	5 - Serviços Especializados.	5.1	Serviços de Monitoramento de infraestrutura IaaS, reservado 1 ano	Mensal	12
		5.2	Serviços Especializados em IaaS.	Horas	25000
		5.3	Serviços de Plataforma integrada (Managed Security Services), reservado 1 ano	Mensal	12
		5.4	Serviço de scan de vulnerabilidades em Bases de dados, reservado 1 ano	Mensal	12
		5.5	Serviço de pentest em redes corporativas, reservado 1 ano	Mensal	12
		5.6	Serviço de provas de penetração em Aplicações, reservado 1 ano	Mensal	12
		5.7	Serviço de penetração em Bases de dados (BD), reservado 1 ano	Mensal	12
		5.8	Serviço gerenciado no Proactive Threat Hunting e serviços especializados em Cyberintelligence, reservado 1 ano	Mensal	12

2. DA JUSTIFICATIVA

2.1. 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.

2.2. 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.

2.3. 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 também planejar, coordenar, supervisionar e orientar normativamente as atividades de gestão dos recursos de tecnologia da informação.

2.4. O projeto visa atingir os seguintes objetivos:

a) 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.

b) 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. DA DESCRIÇÃO DA SOLUÇÃO

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. 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).

3.3. 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.

3.4. **São características essenciais**:

a) **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.

b) **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).

c) **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.

d) **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.

3.5. 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.

3.6. **A solução ofertada deve ser composta por:**

a) Serviços de computação em nuvem;

b) Solução contra ameaças digitais;

c) Serviço de Mensageria e colaboração em nuvem;

4. DO PARCELAMENTO DO OBJETO

4.1. A contratação ora pretendida a ser atendida por um único fornecedor, se mostra mais adequada, neste caso, visto que se o serviço fosse dividido em itens ou lotes diferentes, apesar de oferecerem soluções similares em conceito, os fornecedores trabalham com características de execução diferentes, o que poderia acarretar numa incompatibilidade técnica para integração de toda solução.

4.2. Conforme Acórdão 861/2013-Plenário - É lícito os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si. Além disso, a solução de TI, objeto da contratação, possui uma natural indivisibilidade, o que também inviabiliza a contratação de seus serviços por item de forma separada.

4.3. Segundo o acórdão 5260/2011 – TCU – 1ª câmara, de 06/07/2011, "Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si". A adjudicação global proposta nesse documento agrupa solução e serviços de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia, bem como de aplicabilidade em busca de uma única solução, sem causar qualquer prejuízo à ampla competitividade.

4.4. Ademais, a opção pela contratação conjunta, e não fracionada, dos serviços, não constitui qualquer afronta aos termos da Súmula 247 do TCU. Veja- se o que diz a Sumula:

> "É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade."

4.5. Tanto a disciplina legal, quanto a Súmula do TCU, indicam que a viabilidade técnica do fracionamento deve ser analisada para fins de determinar a possibilidade de licitações distintas (ou lotes distintos na mesma licitação) do objeto que se pretende adquirir. No caso em comento, o objeto licitado envolve tratamento técnico, que demanda que o fornecedor dos serviços tenha conhecimento sobre toda a solução existente. Partir as contratações, deixando a possibilidade de empresas diferentes prestarem os serviços, é assumir um grande risco para este Instituto, pois deixará aberta a

oportunidade para problemas de integração e de administração da solução CONTRATADA.

4.6. Nesse sendo, em respeito à legislação vigente e na busca pela economicidade, se optou por garantir a padronização dos serviços a partir da contratação de um único prestador para realizar os serviços em questão.

4.7. Este Instituto entende que para manter a padronização dos serviços contratados, devido ao tratamento técnico que demanda que o fornecedor dos serviços tenha conhecimento sobre toda a solução, a forma de contratação mais indicada é aquela que não necessita do parcelamento do objeto.

5. DOS REQUISITOS DA SOLUÇÃO

5.1. Item 01 - INFRAESTRUTURA COMO SERVIÇO – IAAS – ON PREMISES:

5.1.1. Sub-Item 1.1 - INFRAESTRUTURA COMO SERVIÇO - HIPERCONVERGÊNCIA:

5.1.1.1. Disponibilizar infraestrutura para nuvem privada e híbrida e serviços especializados, monitoramento e suporte técnico.

5.1.1.2. A CONTRATADA deverá disponibilizar, instalar e configurar equipamentos de hardware em arquitetura hiperconvergente;

5.1.1.3. A CONTRATADA deverá fornecer hypervisor para toda a solução de Hiperconvergência;

5.1.1.4. A CONTRATADA deverá configurar a solução de hardware de forma a entregar serviços de nuvem privada e híbrida com conexão a nuvem contratada no item 1 deste Elemento Técnico.

5.1.1.5. **ESPECIFICAÇÕES DO HARDWARE**

a) O cluster hiperconvergente para implantação da nuvem privada e híbrida será instalado nas dependências da CONTRATANTE;

b) O cluster deve ser composto por um mínimo de 5 (cinco) nós (servidores de rede);

c) Cada nó que compõe o cluster hiperconvergente deve ter, no mínimo, as especificações descritas abaixo:

Processadores Intel® Xeon® Scalable Processors	**Quantidade de memória RAM bruta (GB)**	**Armazenamento bruto em disco de estado sólido (GB)**	**Quantidade de interfaces 10GbE**
12 cores 2.6 GHz	192	7680	4

d) Cache de no mínimo 800GB;

e) Permitir expansão de memória RAM até 1536 GB com a simples substituição dos módulos existentes;

f) Possuir fontes de alimentação elétrica hot-pluggable com redundância mínima 1+1, com potência suficiente para suportar a configuração ofertada;

g) Acompanhar todas as licenças de software necessárias para o pleno funcionamento da solução com todos os recursos especificados neste Elemento Técnico.

5.1.1.6. **ESPECIFICAÇÃO FUNCIONAL DA SOLUÇÃO HIPERCONVERGENTE:**

a) A solução deverá prover uma estrutura hiperconvergente de alta disponibilidade em configuração de cluster para ambiente de virtualização composta de 3 (três) servidores físicos (nós), cada qual com sua respectiva capacidade de processamento, armazenamento e comunicação de rede.

b) Permitir escalabilidade horizontal, isso é, a adição de novos chassis e novos servidores (nós) ao cluster através de uma console gráfica, sem a parada do ambiente de produção, aumentando como um todo a capacidade de armazenamento, processamento e memória disponibilizados ao hypervisor, além de crescer de forma linear o desempenho/performance do ambiente;

c) Permitir adição de um nó por vez;

d) Permitir adição de nós que incrementem apenas o armazenamento do cluster de forma independente do processamento e memória;

e) Permitir remover nós do cluster sem parada no ambiente;

f) Criar um cluster lógico, agregando todos os discos físicos dos servidores contidos na solução, apresentando um único sistema de arquivos ao hypervisor;

g) A solução ofertada deve possuir funcionalidade para expor camada de armazenamento para aplicações físicas (bare metal) através do protocolo iSCSI;

h) Suporte a Hypervisor VMware ESX 6.5 ou mais atual;

5.1.1.7. **Deverá ser fornecida com todos os acessórios necessários para sua instalação, incluindo, mas não se limitando a, trilhos para montagem em rack, cabos de alimentação elétrica e cabos para pelo menos quatro conexões de rede 10GbE (Dez Gigabit Ethernet) por servidor físico respeitando as seguintes especificações mínimas:**

a) Para cada servidor deverão ser fornecidos pelo menos 4 (quatro) transceivers SFP+ (smallform-factorpluggable) com respectivos cabos de fibra padrão OM3 ou superior, com conectores LC em ambas as extremidades e pelo menos 5 (cinco) metros de comprimento; Ou pelo menos 2 (dois) cabos de rede de conexão direta (DirectAttach) ou Twinax com conectores SFP+ em ambas as extremidades e pelo menos 1 (um) metro de comprimento para conexão com os módulos de conexão especificados neste projeto;

b) A solução deverá prover redundância de alimentação elétrica com capacidade de substituição em pleno funcionamento (hot-plug ou hot-swap);

c) Cada servidor deverá ser fornecido com seu próprio sistema de armazenamento de dados integrado para armazenamento local, com capacidade de controlar todo o armazenamento somente em unidades SSD (Solid-state drive).

d) A solução deverá garantir replicação síncrona de todos os dados gravados localmente para outros servidores que compõem o cluster, cada qual com seu respectivo sistema de armazenamento local com garantia de que a promoção e a demoção dos dados ocorram simultaneamente nos servidores do cluster;

e) Deverá suportar a troca dos discos sem parada dos servidores;

f) Todos os nós do cluster devem participar das operações de rebuild de disco, deixando-os mais eficientes a medida que o cluster cresce em número de nós;

g) Deve possuir criptografia através de discos específicos ou software;

h) Cada servidor deverá contemplar pelo menos quatro portas ou conexões físicas 10GbE (TenGigabitEthernet) compatível com conectores SFP+ e duas portas ou conexões físicas 1GbE (GigabitEthernet) compatível com conectores RJ-45, todas elas dedicadas para rede de comunicação em seus respectivos padrões, e pelo menos uma porta 1GbE (Fast Ethernet ou FE) dedicada para gerenciamento remoto compatível com IPM;

i) A solução deve manter os dados das VMs espalhados pelos servidores do cluster - caso essa VM se movimente de um servidor a outro, os dados conseguem ser recuperados e lidos de uma forma mais eficiente

j) No que diz respeito à disponibilidade dos dados, a solução deve garantir que os dados estejam sempre gravados em 2 (dois) ou 3 (três) nós ao mesmo tempo, garantido a resiliência do

cluster e que os dados estejam disponíveis em caso de falhas;

k) A ocorrência de 2 (dois) ou mais clusters distintos, uma ferramenta de gerência unificada deve ser disponibilizada, facilitando a tarefa de administração;

l) O sistema operacional em execução em cada um dos nós deve suportar atualizações do tipo um clique, possibilitando a atualização de todos os nós do cluster de formar simples e automatizada, eliminando a intervenção manual do administrador e parada no ambiente;

m) O sistema operacional em execução em cada um dos nós deve suportar atualizações do tipo um clique também para o hypervisor, possibilitando a atualização de todos os nós do cluster de formar simples e automatizada, eliminando a intervenção manual do administrador e parada no ambiente;

n) A solução deve suportar, via software, desduplicação e compressão de dados;

o) Os usuários devem possuir restore de arquivos granular sem envolvimento do administrador do cluster;

p) A solução deve suportar nativamente replicação das máquinas virtuais, garantindo a disponibilidade das máquinas virtuais em caso de desastres;

q) A funcionalidade de replicação da solução deve suportar:

- Replicação Síncrona para as 5 principais VMw por nó;
- Replicação Assíncrona com recuperação de até 15 minutos para as demais VMs;
- Proteção de Dados Contínua (CDP) para as 2 VMs principais por nó;

r) Solução deve possuir habilidade de replicação para ambientes tradicionais (não hiperconvergentes);

s) Com a finalidade de automatizar os processos de implementação, manutenção e gerenciamento do cluster, o sistema operacional em execução na solução hiperconvergente deverá oferecer REST APIs;

t) A solução deve possuir console de administração WEB sem necessidade de instalação de qualquer componente adicional para essa finalidade;

u) A console WEB deve ser acessível por browsers que suportam a tecnologia HTML5;

v) A console WEB deve permitir integração com Active Directory da Microsoft para autenticação, ou então, utilizar autenticação local;

w) A console Web deve suportar o acesso via HTTPS utilizando certificados;

x) A solução deve disponibilizar acesso ao sistema operacional da solução através do protocolo padrão SSH (Secure Shell);

y) A interface de administração WEB e SSH deve ser acessível a partir de qualquer dos endereços IPs configurados nas máquinas virtuais controladoras configuradas no cluster. A funcionalidade de alta disponibilidade também deve estar disponível para a interface de administração, garantindo que mesmo em caso de falhas, a interface de administração continue disponível;

5.1.1.8. **A console WEB deve fornecer acesso à, no mínimo, as seguintes opções:**

- Dashboard principal;
- Dashboard da saúde do Sistema (cluster);
- Dashboard das Máquinas Virtuais;
- Dashboard do Storage;
- Dashboard do Hardware;
- Dashboard de Recuperação de Desastres;
- Dashboard de Análise de Performance;
- Dashboard de Alertas e Eventos;
- A solução deve suportar o envio de alertas críticos automaticamente para o fabricante da solução;

5.1.1.9. **Com o objetivo de facilitar o monitoramento e visualização das informações do cluster, ao menos as seguintes informações deverão estar disponíveis no cluster:**

- Sumário do hypervisor;
- Sumário do hardware;
- IOPS do cluster;
- Utilização de banda do cluster;
- Latência do cluster;
- Situação da resiliência dos dados;
- Alertas e eventos.

5.1.1.10. Deve suportar envio de alertas e eventos via SNMP;

5.1.1.11. A solução deverá possuir ferramenta de checagem interna integrada a console de gerenciamento, buscando por problemas de saúde no cluster proativamente;

5.1.1.12. Deverá integrar ou utilizar nativamente o vCenter e executar ações como:

a) Criação de VMs;

b) Leitura das VMs;

c) Atualização das características da VM;

d) Deletar VMs;

e) Plataforma ofertada deve possuir integração com:

- vRealize Automation

5.1.1.13. **Requisitos de segurança de criptografia de dados mínimos que deveram ser contemplados dentro da infraestrutura para salvaguarda dos dados:**

a) Serviço de fornecimento de licença, suporte, manutenção e garantia técnica, de sistema de gerenciamento de chaves (KMS - Key Management System);

b) O sistema de gerenciamento de chaves (KMS - Key Management System), deve cumprir os requisitos abaixo:

- Permitir o controle das chaves de maneira centralizada com suporte para diferentes tipos de chaves, gerenciamento do ciclo de vida das chaves, diferentes tipos de integração com banco de dados, servidores de arquivo e APIs
- Possuir funcionalidade de auditoria e log e integra com diretórios de usuário (LDAP e AD) para controles de autorização e uso de chaves.
- Permitir integração com o SQL, Oracle e DB2, para criptografia de dados na própria base de dados, através de composições de triggers e views, deixando criptografia transparente para as aplicações.
- Criptografia de arquivos de maneira transparente compatível com servidores de arquivo como DAS, SAN e NAS utilizando protocolos CIFS/NFS. Proporciona controle de acesso por usuário, gerenciamento centralizado de chaves e políticas, auditoria e segregação de usuários.
- Gerenciamento de chaves heterogêneas. Gerenciar chaves para uma variedade de produtos de criptografia, incluindo tokenização, e aplicativos, bem como unidades de autocriptografia, arquivos em fita, StorageArea Networks e uma lista crescente de fornecedores que suportam o padrão OASIS Key Management Interoperability Protocol (KMIP).
- Gerenciar centralmente chaves simétricas e assimétricas, dados secretos e certificados X.509 junto com políticas associadas.

c) Suportar Completo à Chave de Ciclo de Vida e Operações Automatizadas. Simplifique o gerenciamento de chaves de criptografia em todo o ciclo de vida, incluindo geração, armazenamento e backup de chaves seguras, distribuição de chaves, desativação e exclusão. Operações orientadas por políticas automatizadas simplificam as principais tarefas de expiração e rotação.

d) Administrar centralizada de acesso granular, controles de autorização e separação de tarefas. Unifique as principais operações de gerenciamento em várias implantações e produtos de criptografia, garantindo aos administradores funções restritas definidas para seu escopo de responsabilidades, a partir de um console de gerenciamento centralizado. Além disso, utilizar diretórios LDAP ou AD existentes para mapear o acesso administrativo e chave para aplicativos e usuários finais.

e) Implantar em configurações flexíveis e de alta disponibilidade em um centro de operações e em centros dispersos geograficamente ou em ambientes de provedores de serviços usando um modo ativo-ativo de clustering.

f) Possuir Registro detalhado e rastreamento de auditoria de todas as mudanças de estado chave, acesso de administrador e mudanças de políticas. As trilhas de auditoria são armazenadas com segurança e assinadas para não-repúdio e podem ser consumidas pelas principais ferramentas de SIEM de terceiros.

g) Criptografar em nível de coluna transparente e eficiente

h) Criptografar de forma transparente os dados sensíveis do banco de dados em nível de coluna

i) Aplicar controles de acesso granular para garantir que somente os usuários ou aplicativos podem visualizar dados protegidos

j) Impedir que administradores de bancos de dados (DBAs) se façam passar por outros usuários para acessar dados confidenciais

k) Implantar em ambientes de nuvem locais, virtuais e públicos

l) Configurar a criptografia na nuvem mais rapidamente com as receitas do Chef para facilitar a automação

m) Possuir Rotação de chave integrada e re-digitação de dados

n) Realizar operações criptográficas localmente ou descarregar para o KeySecure para aproveitar o poder de processamento externo

o) Possuir Pool de conexões integrado, verificação de integridade e balanceamento de carga em várias camadas

p) Atender às exigências de conformidade, como PCI DSS e HIPAA, que exigem criptografia de dados e separação de tarefas

q) Possuir Recursos abrangentes de auditoria e registro para rastrear o acesso a dados e chaves criptografados

r) Possuir Suporte API em Java, C / C ++, .NET, interface aberta XML, gerenciamento de rede padrão KMIP, SNMP (v1, v2 e v3), NTP, verificação de integridade da URL, assinada logs e syslog seguros, rotação automática de logs, backups e atualizações criptografados e verificados por integridade, estatísticas abrangentes;

s) Administrar de aparelhos GUI segura baseada na Web, autenticação de interface de linha de comando, LDAP e Active Directory;

t) Suportar os bancos de dados Oracle, MicrosoftSQLServer e IBM DB2;

u) Suportar as plataformas Microsoft Windows, Linux, Solaris, HP-UX, AIX;

v) Suportar Algoritmos de Criptografia AES 128, 192, 256, 512> 3DES168;

w) Suportar Cloud e Infraestruturas Virtuais;

x) Funcionar com todas as principais plataformas de nuvem, incluindo AWS, Microsoft Azure e VMware;

y) Suportar integração e Gerenciamento de Conteúdo Alfresco Open ECM, Open Text (EMC), Info Archive Stealth Content Store, ServiceNow, Mainframe

z) EncryptionPKware, Big Data Dataguise, DataStax, Hadoop, MongoDB, MariaDB, HANA SAP, Cassandra, Couchbase, Hortonworks, CloudEra, Analytics IBM

aa) Qradar, HPE ArcSight, Splunk, Análise de Segurança RSA, Acima de Segurança;

ab) Suportar Servidores de Aplicativos IBM Web Sphere, Oracle Weblogic, Microsoft IIS, Apache Tomcat, Soluções de Backup RedHat JBoss, Commvault Simpana, Symantec NetBackup (via NetApp), Cloud Storage Nutanix, Amazon Web Services S3, DropBox, Google Cloud Storage, Google Drive, NetApp Cloud ONTAP, NetApp Alta Vault, IBM ICDES, Controlador de Armazenamento Panzura;

ac) Criptografar arquivos e discos PKware, IBM, Dell, AWS, Microsoft, LUKS, Via Sat;

ad) Gerenciar de Identidades Centrify Privilege Service, Lieberman Software;

ae) Suportar Armazenamento físico NetApp NSE, Dell Compellent (SC e XC), MSL HPE / ESL Tape Libraries, HPE 3Par Store Serv, HPE XP7, Hitachi, SP, Hitachi HUS, Hitachi RAID700, IBM XIV SED, Quantum Scalar Series (i6000, i500 & i40 / 80), Viasat, Brocade FS8-18, Huawei Oceanstor, Tintri VMStore, Cisco UCS, Spring Path HyperFlex, NexentaStor 4.5;

5.1.2. **Sub-Item 1.2 - Disponibilização de antivírus para servidores Windows e Linux :**

5.1.2.1. Os softwares (solução) necessários à prestação dos serviços deverão ser instalados, de modo a prover proteção, identificação e gestão de segurança de servidores virtuais do ambiente da **CONTRATANTE**;

5.1.2.2. **Características de Licenciamento da Solução:**

- Estar dimensionada para 150 servidores virtuais.

5.1.2.3. **Funcionalidades e Requisitos Mínimos:**

a) Ser totalmente compatível e homologada para gerenciamento de máquinas virtuais nos ambientes VMware, Citrix XenServer, KVM e HyperV;

b) Para cada plataforma de virtualização haverá uma forma diferente de integração, com ou sem agente, preservando a capacidade de implementação das funcionalidades descritas abaixo.

c) Permitir a integração com todas as versões do VMware vCenter a partir da Versão 6.5, de modo a importar e sincronizar os objetos (hosts VMware e Guests VM) para a console de gerenciamento da solução;

5.1.2.4. **Permitir, no caso de versões anteriores a VMware 6.5 ou superior, integração com as seguintes API's VMware:**

- VMsafe API;
- vShield Endpoint API.

5.1.2.14. **Permitir que as funcionalidades abaixo possam ser executadas simultaneamente no Hypervisor:**

a) Firewall;

b) Inspeção de Pacotes;

c) Monitoramento de Integridade;

d) Inspeção de Log's;

e) Anti-malware e Reputação Web;

f) Controle de Aplicação;

5.1.2.15. Suportar a aplicação das funcionalidades de segurança acima, inclusive para ambientes com versão 6.5 do vCenter/ vSphere, com integração com as novas API's da VMware (NSX);

5.1.2.16. **Permitir a implantação dos módulos de segurança citados, no mínimo para os seguintes sistemas operacionais:**

- Windows Server 2003, 2008, 2012 e 2016 (todas as versões);
- Sistemas Operacionais Linux, no mínimo para as distribuições: RedHat, Suse, CentOs.

5.1.2.17. Possuir a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais e caso o dispositivo esteja offline, deve haver meio de realizar liberações emergenciais da execução de comandos ou elevação de privilégios, sem que a ferramenta tenha que ser desativada;

5.1.2.18. Executar rastreamento nas máquinas virtuais e fornecer lista de todas as

5.1.2.19. recomendações de segurança para os softwares que estiverem instalados nessas máquinas virtuais, bem como do sistema operacional;

5.1.2.20. Proteger de forma automática e transparente contra brechas de segurança descobertas, interrompendo somente o tráfego de rede malicioso;

5.1.2.21. **Funcionalidades de Firewall:**

a) Operar como firewall de host statefull bidirecional, monitorando as comunicações nos servidores protegidos;

b) Possuir a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;

c) Possuir a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

d) Permitir que regras de Firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);

e) Permitir que as regras de Firewall executem as seguintes ações, ou equivalentes: Allow, Log Only, bypass, force allow, deny;

f) Permitir realizar pseudo-statefull em tráfego UDP;

g) Permitir limitar o número de conexões entrantes e de saída de um determinado IP de origem;

h) Permitir a criação de novas regras utilizando templates padrão;

i) Permitir atuar no modo em linha para bloqueio de ataques ou modo escuta para monitoração e alertas.

5.1.2.22. **Funcionalidades de Inspeção de Pacotes:**

a) Possuir a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

b) Possuir a capacidade de varrer o servidor protegido detectando o tipo e versão do SO e demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações;

c) Permitir execução de varreduras sob demanda ou agendada;

d) Possuir a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão.

e) Permitir que a opção de detecção e bloqueio seja implementada de forma global (todas as regras) ou apenas para uma regra ou grupos de regras;

5.1.2.23. **Conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem, no mínimo, os seguintes sistemas operacionais:**

- Windows Server 2003, 2008, 2012 e 2016 (todas as versões);
- Linux RedHat, Suse, CentOS e Debian;

5.1.2.24. Aplicações padrão de mercado, tais como: Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache.

5.1.2.25. Possuir a capacidade de armazenamento do pacote capturado quando detectado um ataque;

5.1.2.26. Possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pela CONTRATADA;

5.1.2.27. Possuir a capacidade de detectar e bloquear ataques em aplicações web tais como: SQL Injection e Cross-Site Scripting;

5.1.2.28. Implementar a customização avançada e criação de novas regras de proteção de aplicações web, permitindo proteger contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

5.1.2.29. Permitir configuração de regras de IDS/IPS diferenciadas de acordo com horário ou dia da semana;

5.1.2.30. Implementar a inspeção de tráfego incoming SSL;

5.1.2.31. Apresentar informações detalhadas das regras de blindagem contra vulnerabilidades, contendo links com referências externas, quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

5.1.2.32. Bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de um determinado web browser ou aplicação de backup;

5.1.2.33. Permitir habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;

5.1.2.34. Permitir que as regras de IPS atuem detectando ou bloqueando os eventos que as violem, de modo que o administrador possa decidir qual ação deva ser tomada;

5.1.2.35. Permitir atuar no modo em linha para bloqueio de ataques ou modo escuta para monitoração e alertas;

5.1.2.36. Permitir que o administrador do sistema tenha a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host.

5.1.2.37. **Funcionalidades de Monitoramento de Integridade:**

a) Possuir a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras e realizar o controle mediante interceptação do comando antes que ele seja executado;

b) Deverá impedir a utilização de técnicas em que um programa autorizado e executado com privilégios permita a execução de outros programas e consequentemente escape dos controles definidos e restringir Shell, impossibilitando que scripts ou shells de sistema executem comandos não permitidos pelas regras definidas na ferramenta;

c) Possuir a capacidade de monitorar o status de serviços e processos do sistema operacional;

d) Possuir a capacidade de monitorar mudanças efetuadas no registro do Windows;

e) Possuir a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e, customização de XML para criação de regras avançadas;

f) Possuir a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura;

g) Permitir execução de varreduras sob demanda ou agendada;

h) Rastrear arquivos por criação, última modificação, último acesso, permissões, owner, grupo, tamanho, SHA1, SHA256, Flags e definir variáveis de ambiente no momento da execução de um comando;

i) Gerar alertas toda vez que uma modificação ocorrer, em tempo real para ambiente Windows e, pseudo tempo real para ambiente Linux utilizando agente;

j) Registrar em relatório todas as modificações que ocorram nos objetos monitorados 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;

k) Classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

l) Possibilitar a escolha do diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;

m) Permitir definir, no mínimo, as variáveis de ambiente PATH, ENV, BASH_ENV, GLOBIGNORE, SHELLOPTS, no momento da execução de um comando, independente da definição realizada pelo usuário ou seu perfil e possibilitar o uso da máscara de usuário na execução dos comandos (valores entre 0000 e 0777).

5.1.2.38. **Funcionalidades de Inspeção de Log's:**

a) Possuir capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;

b) Possuir a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura;

c) Permitir execução de varreduras sob demanda ou agendada;

d) Permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

e) Permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

f) Implementar inteligência de alertas para cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor;

g) Permitir modificar as regras por severidade de ocorrência de eventos;

5.1.2.39. **Funcionalidades de Anti-malware e Reputação Web:**

a) Permitir a proteção em tempo real contra códigos maliciosos, possibilitando a tomada de ações distintas para cada tipo de ameaça;

b) Permitir execução de varreduras sob demanda ou agendada;

c) Possibilitar a criação de listas de exclusão para processos, diretórios ou arquivos do SO;

d) Possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;

e) Implementar a proteção contra acesso a websites ou URLs consideradas maliciosas, de baixa reputação ou não categorizadas;

5.1.2.40. **Funcionalidades de Controle de Aplicação:**

a) A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;

b) O controle de aplicações deverá ser realizado através de Hash, através da verificação de checksum do arquivo, dos parâmetros permitidos e da assinatura de fabricante;

c) O agrupamento dos eventos deverá ser realizado pelo menos por Hash é por máquina;

d) A console deverá exibir eventos de no mínimo 30 dias e possibilitar o monitoramento e a criação de evidência em vídeo de certas execuções de arquivo e de execuções sob certas condições definidas em política;

e) A solução deverá possuir funcionalidades de bloquear e notificar o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente e possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não privilegiados;

f) Permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

g) Permitir a criação de regras de privilégios para cada processo (aplicação) a ser executado com privilégios de administrador, de forma que cada usuário, mesmo com o privilégio de usuário convencional possa instalar programas previamente aprovados para uso com privilégios elevados;

h) Monitorar a atividade dos processos em execução, visando detectar tentativas de roubo de credenciais;

i) 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.

5.1.2.41. **Funcionalidades de Gerenciamento:**

a) Permitir o envio de notificações via SMTP;

b) Permitir o envio de registros de logs a um servidor remoto;

c) Implementar gravação de eventos de auditoria envolvendo todos os eventos e ações realizadas na console de gerenciamento;

d) Permitir que a distribuição de atualizações e novos componentes possa ser efetuada por replicadores espalhados pelo ambiente;

e) Permitir a criação de múltiplos perfis de segurança, que serão vinculados aos diferentes tipos de servidores do ambiente;

f) Permitir a criação de relatórios, sob demanda, ou agendados, com o envio automático via e-mail, no formato PDF;

g) Armazenar políticas e logs em base de dados, suportando, no mínimo, bancos de dados Oracle e MS SQL;

h) Permitir opções de permissionamento, no mínimo, para modos de visualização e edição de políticas;

i) Permitir a atribuição granular de permissões para servidores gerenciados, podendo delimitar quais os servidores que podem ser visualizados e gerenciados para cada usuário ou grupo de usuários;

j) Possuir dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo

administrador em quantidade e período de monitoração;

k) Possuir a capacidade de criar políticas de forma global para todas as máquinas virtuais, por perfis e individualmente para cada host;

l) Prover perfis padrões pré-definidos e aptos a funcionar de acordo com sua denominação;

m) Permitir o envio de eventos da console via SNMP;

n) Permitir o rollback de atualização de regras pela console de gerenciamento;

o) Gerar pacote de auto-diagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;

p) Possuir a capacidade de marcar eventos (tags) de modo a facilitar o gerenciamento, relatórios e visualização;

q) Possuir a capacidade de classificar eventos para facilitar a identificação e a visualização de eventos críticos em servidores críticos.

5.1.3. **Sub-Item 1.3 - Serviço de proteção de endpoints integrado com EDR**

5.1.3.42. 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.

5.1.3.43. **Características Licenciamento:**

a) Estar dimensionada para no mínimo 10000 estações de trabalho.

b) Toda infraestrutura para implantação da solução será provida pelo IGES, baseando-se nas especificaçõe a abaixo:

c) Os seguintes hipervisores devem ser suportados.

d) VMware ESXi 5.0

e) VMware ESXi 5.1

f) VMware ESXi 5.5

g) VMware ESXi 6.0

h) Microsoft Hyper-V Server 2012 R2

i) Hyper-V no Microsoft Windows Server 2012 R2

5.1.3.44. Requisitos máximos de VM Servidor para solução:

- 8 CPUs virtuais
- 200 GB de espaço em disco
- 24 GB de RAM
- 2 portas virtual switched ports

5.1.3.45. **Funcionalidades e Requisitos Específicos:**

- 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);

5.1.3.46. Possuir tecnologia de Machine Learning sendo capaz de detectar variantes de malwares desconhecidos por similaridade de código;

5.1.3.47. Possuir módulo de monitoração de comportamento malicioso de aplicações de forma a bloqueá-las mesmo quando a assinatura não for reconhecida;

5.1.3.48. Possuir regras específicas para detecção de ransonware;

5.1.3.49. Detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

5.1.3.50. **Detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:**

a) Processos em execução em memória principal (RAM);

b) Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

c) Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;

d) Arquivos recebidos por meio de programas de comunicação instantânea (msn messenger, yahoo messenger, google talk, icq, dentre outros).

e) Permitir configurar o consumo de cpu que será utilizada para uma varredura manual ou agendada;

f) 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;

g) 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;

h) 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;

i) Permitir proteção dedicada contra URL's maliciosas voltadas a tecnologia Microsoft Skype for Business e Microsoft Lync Server.

j) 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;

k) Permitir o rollback das atualizações das listas de definições de vírus e engines;

l) Permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações;

m) Permitir proteção dedicada contra códigos maliciosos voltadas a tecnologia Microsoft Skype for Business e Microsoft Lync Server.

n) 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.

5.1.3.51. **Funcionalidades de Controle de Dispositivos:**

a) 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;

b) 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;

c) Possuir a capacidade de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;

d) Possuir a capacidade de controlar drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

e) Permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, CD-ROM) mesmo com a política de bloqueio total ativa

5.1.3.52. **Funcionalidades de Host IPS e Host Firewall:**

a) Possuir a capacidade de 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);

b) Permitir que todas as regras das funcionalidades de firewall e IPS de host atuem apenas em modo detecção ou prevenção;

c) 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;

d) A varredura de segurança deve ser capaz de identificar as regras de Host IPS que não são mais necessárias e desativá-las automaticamente;

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;

f) Permitir a emissão de alertas via SMTP e SNMP;

g) Permitir criação de regras de firewall utilizando os seguintes protocolos: Icmp, icmpv6, igmp, ggp, tcp, pup, udp, idp, nd, raw, tcp+udp.

h) Permitir criação de regras de firewall por origem de ip ou mac ou porta e destino de ip ou mac ou porta;

i) Permitir a criação de contextos para a aplicação para criação de regras de firewall;

j) Permitir o isolamento de interfaces de rede, possibilitando o funcionamento de uma interface por vez.

k) Funcionalidades de Controle de Aplicação:

l) Possuir a capacidade de realizar o controle de aplicações nos seguintes sistemas operacionais: Windows 7 (x86/x64), Windows 8 e 8.1 (x86/x64) e Windows 10 (x86/x64);

m) Permitir a criação de políticas de segurança personalizadas;

n) Permitir o controle do intervalo de envio dos logs e para envio de atualização de cada política;

o) Permitir a definição de qual servidor de gerenciamento o agente de segurança deverá comunicar-se;

p) Permitir as seguintes ações: Permissão de execução; Bloqueio de execução e Bloqueio de novas instalações;

q) Permitir os seguintes métodos para identificação das aplicações: Assinatura sha-1 do executável; Atributos do certificado utilizado para assinatura digital do executável; Caminho lógico do executável e Base de assinaturas de certificados digitais válidos e seguros;

r) Possuir categorias de aplicações e permitir a utilização de múltiplas regras de controle de aplicações;

s) Possuir atualização das categorias de maneira automatizada

5.1.3.53. **Funcionalidades de Proteção contra Vazamento de Informações:**

a) 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) e Windows 10 (x86/x64);

b) Possuir a capacidade de detectar informações, em documentos nos formatos: Microsoft office

(doc, docx, xls, xlsx, ppt, pptx) openoffice, rtf, wordpad, text; xml, html; postscript, pdf, tiff, zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2, unix/linux zip, lzh;

c) Possuir a capacidade de detectar informações, com base em: Dados estruturados; Palavras ou frases configuráveis; Expressões regulares e Extensão dos arquivos;

d) Permitir a configuração de quantas camadas de compressão serão verificadas;

e) Permitir a criação de modelos personalizados para identificação de informações;

f) Possuir a capacidade de identificar e bloquear informações no mínimo para os seguintes meios de transmissão: Cliente de e-mail; Protocolos http, https, ftp; Mídias removíveis e discos óticos cd/dvd; Aplicações de mensagens instantâneas; Tecla de printscreen; Aplicações p2p; Área de transferência do Windows; Webmail; Armazenamento na nuvem (cloud); Impressoras; Scanners; Compartilhamentos de arquivos; Activesync; Portas COM e LPT; Modems.

g) Permitir proteção dedicada contra vazamento de informações voltadas a solução Microsoft Skype for Business e Microsoft Lync Server.

h) 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.

5.1.3.54. **Funcionalidades de Criptografia:**

a) Possuir a capacidade de realizar a criptografia nos seguintes sistemas operacionais: Windows 7 (x86/x64); Windows 8 e 8.1 (x86/x64) e Windows 10 (x86/x64);

b) Possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), permitindo criptografia para: Disco completo (FDE – full disk encryption); Pastas e arquivos; Mídias removíveis; Anexos de e-mails e Automática de disco;

c) Possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

d) Possuir a capacidade de exceções para criptografia automática;

e) Possuir compatibilidade de autenticação por múltiplos fatores;

f) Permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

g) Possuir auto ajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;

h) Possuir mecanismos para wipe (limpeza) remoto;

i) Possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);

j) Possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook;

k) O ambiente de autenticação pré-inicialização deve permitir a conexão a redes sem fio (wireless);

l) Permitir, em nível de política, a indicação de pastas a serem criptografadas;

m) Possibilitar que cada política tenha uma chave de criptografia única;

n) Permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;

o) Possibilitar a desativação de dispositivos de gravação de mídias óticas e de dispositivos de armazenamento USB;

p) Possibilitar apagar todos os dados do dispositivo na ocorrência de um número personalizável de tentativas inválidas de autenticação

5.1.3.55. **Módulo de proteção para smartphones e tablets:**

a) O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais:

b) IOS, Android, Windows Phone;

c) As funcionalidades estarão disponíveis de acordo com cada plataforma

5.1.3.56. **Deve permitir o provisionamento de configurações de:**

a) Wi-fi, Exchange Activesync, vpn, proxy http global e certificados;

b) Deve possuir proteção de anti-malware para Android;

c) Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão sd e após atualização de vacinas;

d) Deve possuir capacidade de detecção de spam proveniente de SMS;

e) Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número bloqueados para recebimento de chamadas;

f) Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número permitidos para efetuação de chamadas;

g) Deve possuir funcionalidade de firewall para bloqueio de tráfego de entrada e saída, com possibilidades de enumeração de regras de exceção;

h) Deve permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL's acessadas;

i) Deve permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;

j) Deve permitir o bloqueio de aplicativos de acordo com sua faixa etária indicativa;

5.1.3.57. **Controle da política de segurança de senhas, com critérios mínimos de:**

- Tempo de expiração;
- Bloqueio automático da tela;
- Bloqueio por tentativas inválidas;
- 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)

5.1.3.58. **Serviços gerenciados de detecção e respostas a ameaças nos terminais/ Endpoints**

a) 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, invalidando sessões e tokens após um período de inatividade.

b) Permitir que usuários não administradores da plataforma executem funções de redefinição de suas senhas, perguntas secretas e atualização de e-mail e auto-reservem as reinicializações de suas credenciais (ex: nome de usuário ou senha esquecidos), ajustem suas preferências, incluindo detalhes de perfil, tais como informações de contato.

c) Deve ter recursos avançados de análise de comportamento e modo de coleta somente para avaliação e validação das políticas criadas.

d) 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.

e) 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.

f) 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.

g) 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.

h) A equipe avançada da proponente precisará fazer uma revisão manual para identificar e capturar ameaças através da infraestrutura **IGES-DF,** à medida que novas tendências e ameaças de ataques são lançadas globalmente.

i) O provedor deve fornecer uma solução/ plataforma que disponibilize um console ou portal para acesso e integração de dispositivos que atendam às seguintes especificações:

j) Solução tecnológica avançada em proteção da camada de endpoint, baseada no controle de aplicações, gestão de privilégios e proteção contra ameaças a credenciais.

k) Implementação, configuração e operação da plataforma de proteção e monitoramento de terminais/ endpoints.

l) O provedor deve fornecer uma solução que suporte a proteção em plataformas com S.O. Windows e Linux.

m) A solução deve ter a capacidade de monitorar a atividade do terminal no nível de identificação de:

- Objetos
- Memória
- Violações de políticas (Hardening)
- Análise de atividades a partir de um conjunto de indicadores de compromisso previamente definidos e estabelecidos entre a proponente e o **IGESDF.**
- Processos em execução, visando detectar e bloquear tentativas de roubo de credenciais armazenadas em browsers e no Windows.
- Intervenção em dispositivos que foram afetados por alguma vulnerabilidade ou ataque.
- Coleta de Evidência e analisar eventos sobre artefatos perigosos na memória e discos rígidos.
- Possibilitar o monitoramento e a criação de evidência em vídeo de certas execuções de arquivo e de execuções sob certas condições definidas em política.
- 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

5.1.3.59. A ativação do serviço de proteção de terminal deve considerar as seguintes fases:

a) **Provisionamento do serviço**: a proponente deve coordenar com o **IGESDF** a integração e a autorização das fontes na solução de monitoramento e detecção, conforme previamente analisado e projetado pelo **IGESDF** e pelo fornecedor.

b) **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.

c) **Intervenção & correção**: A proponente deve executar ações de intervenção nos dispositivos afetados, bem como ações de correção.

d) O fornecedor deve permitir o acesso ao pessoal que **IGESDF**determinar sob as seguintes considerações:

e) 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.**

f) Os controles de acesso devem ser definidos, limitados ao pessoal do provedor e ou **IGESDF** que executa ações de administração da plataforma.

g) O serviço deve fornecer uma visão e acesso à plataforma de gerenciamento, considerando os seguintes aspectos obrigatórios:

- Visão atualizada e histórica dos dados e apresentação da posição no ambiente do CONTRATANTE integrado ao serviço.
- Canal de comunicação seguro com o provedor e a equipe do **IGESDF.**
- Interface para o gerenciamento de **tickets** relacionados ao serviço e relatórios associados aos resultados do monitoramento e detecção de eventos nos terminais do **IGESDF.**
- Painel com as informações de contato da equipe do **IGESDF.**
- Painel com a documentação das políticas de serviço e segurança associadas.
- Painel para criação de relatórios de segurança pelo time de SI do **IGESDF.**
- Painel que mostra o progresso nos processos de integração de fontes à solução.
- O fornecedor deve gerenciar a solução/ plataforma através de sua própria equipe técnica, que inclui os seguintes escopos:

I - Executar gerenciamento da plataforma, monitoramento e status, configurações e desempenho.

II - O gerenciamento e a manutenção da solução devem ser cobertos por um esquema de serviço 24x7.

III - As solicitações e o gerenciamento das configurações de política devem obedecer aos seguintes requisitos:

- Processo de controle de alterações de fornecedores para terminais integrados a plataforma web.

- Coordenar e avaliar em conjunto entre o provedor e o **IGESDF** as mudanças que podem afetar a operação dos terminais.
- Gerenciar solicitações de controle de alterações através de:
- A plataforma de gerenciamento centralizado do serviço de monitoramento e detecção de ameaças.
- **Contato telefônico**: acesso ao número de telefone para que o **IGESDF.** possa solicitar alterações nas políticas ou dispositivos integrados no serviço.
- **E-mail de contato**: acesso a um e-mail para que o **IGESDF** possa solicitar alterações nas políticas ou dispositivos integrados no serviço

IV - O gerenciamento de disponibilidade da solução deve considerar o seguinte:

- O provedor monitorará a disponibilidade e o nível de serviço da solução
- Se necessário, o contato técnico deve ser coordenado para ações mais avançadas

5.1.3.60. O fornecedor deve executar ações de investigação, análise e resposta que considere:

5.1.3.61. 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.

5.1.3.62. Capacidade 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.

5.1.3.63. Fornecer um modelo de proteção contínua contra ameaças avançadas, considerando:

- **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 .
- **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**.
- **Determine o impacto.** - De acordo com as informações coletadas e analisadas, o escopo do incidente deve ser identificado.
- **Remediação.** - Com as informações sobre o escopo do impacto, o fornecedor deve desenvolver e aplicar um plano de remediação eficaz.
- **Aplicar contramedidas.** - o 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.

5.1.3.64. O fornecedor deve realizar a identificação preventiva contra ameaça.

5.1.3.65. Essas atividades devem se concentrar na detecção de ameaças latentes sob um modelo holístico de identificação de ataques.

5.1.3.66. 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.

5.1.3.67. 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.

5.1.3.68. Nesse caso, um protocolo de notificação de incidentes deve ser definido entre o provedor e o **IGESDF** .

5.1.3.69. 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

Download de arquivos deste endpoint	informações para contenção da vulnerabilidade ou análise.
Excluir arquivos deste terminal	Remover arquivos danificados no endpoint
Acesso a arquivos ou memoria dos hosts	Coletando Arquivos ou Memória do Host

5.1.3.70. ***Sub-Item – 1.4*** **- Disponibilização de Next Generation Firewall em Alta Disponibilidade - TIPO 1**

a) Serviço de fornecimento de appliance, licença, atualização de versão, manutenção e garantia técnica do fabricante de solução de firewall conforme especificações abaixo;

b) A solução de firewall fornecida deve funcionar em alta-disponibilidade com, no mínimo, 2 (dois) equipamentos

5.1.3.71. **Performance:**

a) Throughput de, no mínimo, 32 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independente do tamanho do pacote

b) Suporte a, no mínimo, 8M conexões simultâneas

c) Suporte a, no mínimo, 300K novas conexões por segundo

d) Throughput de, no mínimo, 20 Gbps de VPN IPSec

e) Estar licenciado para, ou suportar sem o uso de licença, 2.000 túneis de VPN IPSEC Site-to-Site simultâneos

f) Estar licenciado para, ou suportar sem o uso de licença, 50.000 túneis de clientes VPN IPSEC simultâneos

g) Throughput de, no mínimo, 5 Gbps de VPN SSL

h) Suporte a, no mínimo, 5000 clientes de VPN SSL simultâneos

i) Suportar no mínimo 5,2 Gbps de throughput de IPS

j) Suportar no mínimo 6,8 Gbps de throughput de Inspeção SSL

k) Throughput de, no mínimo, 4,7 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus, Antispyware e log de tráfego habilitado. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

l) Possuir ao menos 16 interfaces GE SFP (deve ser fornecido com no minimo 02 (dois) Tranceivers SX 01 GE)

m) Possuir ao menos 16 interfaces GE RJ45

n) Possuir ao menos 2 interfaces 10GE SFP+

o) Disco SSD de, no mínimo, 480 GBytes para armazenamento de informações locais

p) Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance

q) Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance

r) Possuir ao menos 2 interfaces GE RJ45 dedicadas à gerenciamento

s) Possuir fonte de alimentação redundante interna ao equipamento 100-240 VAC 60-50 Hz automática

5.1.3.72. ***Sub-Item – 1.5*** **- Disponibilização de Next Generation Firewall em Alta Disponibilidade - TIPO 2**

a) Serviço de fornecimento de appliance, licença, atualização de versão, manutenção e garantia técnica do fabricante de solução de firewall conforme especificações abaixo;

b) A solução de firewall fornecida deve funcionar em alta-disponibilidade com, no mínimo, 2 (dois) equipamentos.

5.1.3.73. **Performance:**

a) Throughput de, no mínimo, 32 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independente do tamanho do pacote

b) Suporte a, no mínimo, 8M conexões simultâneas

c) Suporte a, no mínimo, 300K novas conexões por segundo

d) Throughput de, no mínimo, 20 Gbps de VPN IPSec

e) Estar licenciado para, ou suportar sem o uso de licença, 2.000 túneis de VPN IPSEC Site-to-Site simultâneos

f) Estar licenciado para, ou suportar sem o uso de licença, 50.000 túneis de clientes VPN IPSEC simultâneos

g) Throughput de, no mínimo, 5 Gbps de VPN SSL

h) Suporte a, no mínimo, 10.000 clientes de VPN SSL simultâneos

i) Suportar no mínimo 7.9 Gbps de throughput de IPS

j) Suportar no mínimo 5.7 Gbps de throughput de Inspeção SSL

k) Throughput de, no mínimo, 5.0 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus, Antispyware e log de tráfego habilitado. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

l) Possuir ao menos 8(oito) interfaces GE SFP (deve ser fornecido com no mínimo com 02 (dois) tranceivers SX 01 GE)

m) Possuir ao menos 8 (oito) interfaces GE RJ45

n) Possuir ao menos 2 (dois) interfaces 10GE SFP+

o) Disco SSD de, no mínimo, 480 GBytes para armazenamento de informações locais

p) Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance

q) Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance

r) Possuir ao menos 2 interfaces GE RJ45 dedicadas à gerenciamento

s) Possuir fonte de alimentação redundante interna ao equipamento 100-240 VAC 60-50 Hz automática

5.1.3.74. **Características Gerais Next Generation Firewall do TIPO I e TIPO II:**

a) A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

b) Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

c) As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;

d) A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

e) Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

f) A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;

g) Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;

h) Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;

i) Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;

j) Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

k) Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

l) Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

m) Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

n) Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

o) Deve suportar NAT dinâmico (Many-to-1);

p) Deve suportar NAT dinâmico (Many-to-Many);

q) Deve suportar NAT estático (1-to-1);

r) Deve suportar NAT estático (Many-to-Many);

s) Deve suportar NAT estático bidirecional 1-to-1;

t) Deve suportar Tradução de porta (PAT);

u) Deve suportar NAT de Origem;

v) Deve suportar NAT de Destino;

w) Deve suportar NAT de Origem e NAT de Destino simultaneamente;

x) Deve poder combinar NAT de origem e NAT de destino na mesma política

y) Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

z) Deve suportar NAT64 e NAT46;

aa) Deve implementar o protocolo ECMP;

ab) Deve implementar balanceamento de link por hash do IP de origem;

ac) Deve implementar balanceamento de link por hash do IP de origem e destino;

ad) Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

ae) Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

af) Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do

cluster, ataques e estatísticas de uso das interfaces de rede;

ag) Enviar log para sistemas de monitoração externos, simultaneamente;

ah) Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

ai) Proteção anti-spoofing;

aj) Implementar otimização do tráfego entre dois equipamentos;

ak) Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

al) Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

am) Suportar OSPF graceful restart;

5.1.3.75. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

5.1.3.76. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

5.1.3.77. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

5.1.3.78. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

5.1.3.79. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

5.1.3.80. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

5.1.3.81. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

5.1.3.82. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;

5.1.3.83. A configuração em alta disponibilidade deve sincronizar: Sessões;

5.1.3.84. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

5.1.3.85. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

5.1.3.86. A configuração em alta disponibilidade deve sincronizar:Tabelas FIB;

5.1.3.87. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

5.1.3.88. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;

5.1.3.89. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;

5.1.3.90. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

5.1.3.91. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos)

5.1.3.92. **Controle por Política de Firewall:**

a) Deverá suportar controles por zona de segurança;

b) Controles de políticas por porta e protocolo;

c) Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

d) Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

e) Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Web filtering no mínimo) diretamente às políticas de segurança versus via perfis;

f) Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;

g) Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise);

h) Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);

i) Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não supera a velocidade de upload;

j) Deve suportar o protocolo padrão da indústria VXLAN

5.1.3.93. **Controle de Aplicações:**

a) Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

b) Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

c) Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

d) Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, activedirectory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

e) Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

f) Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

g) Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

h) Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

i) Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;

j) Identificar o uso de táticas evasivas via comunicações criptografadas;

k) Atualizar a base de assinaturas de aplicações automaticamente;

l) Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;

m) Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

n) Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

o) Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

p) Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

q) Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

r) A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;

s) O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

t) Deve alertar o usuário quando uma aplicação for bloqueada;

u) Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

v) Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

w) Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;

x) Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

y) Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client Server, Browse Based, Network Protocol, etc);

z) Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;

aa) Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

5.1.3.94. **Prevenção de Ameaças**

a) Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

b) Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

c) As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber

atualizações ou que não haja contrato de garantia de software com o fabricante;

d) Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

e) Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

f) As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

g) Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

h) Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

i) Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

j) Deve permitir o bloqueio de vulnerabilidades;

k) Deve permitir o bloqueio de exploits conhecidos;

l) Deve incluir proteção contra ataques de negação de serviços;

m) Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de padrões de estado de conexões;

n) Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo;

o) Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo;

p) Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise heurística;

q) Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation;

r) Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP;

s) Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados;

t) Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood, etc;

u) Detectar e bloquear a origem de portscans;

v) Bloquear ataques efetuados por worms conhecidos;

w) Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

x) Possuir assinaturas para bloqueio de ataques de buffer overflow;

y) Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

z) Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

aa) Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

ab) Identificar e bloquear comunicação com botnets;

ac) Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

ad) Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

ae) Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu

contexto, facilitando a análise forense e identificação de falsos positivos;

af) Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

ag) Os eventos devem identificar o país de onde partiu a ameaça;

ah) Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

ai) Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

aj) Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

ak) Fornecer proteção contra ataques de dia zero por meio de integração com solução de sandbox em nuvem do mesmo fabricante

5.1.3.95. **Filtro de URL:**

a) Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

b) Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

c) Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

d) Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

e) Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

f) Possuir pelo menos 60 categorias de URLs;

g) Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

h) Permitir a customização de página de bloqueio;

i) Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);

j) Além do Explicit Web Proxy, suportar proxy Web transparente;

5.1.3.96. **Identificação de Usuários:**

a) Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

b) Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

c) Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2;

d) Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede etc.;

e) Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

f) Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

g) Deve permitir o controle, sem instalação de agente, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

h) Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

i) Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

j) Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;

k) Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;

5.1.3.97. **QoS e TrafficShaping**

a) Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

b) Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

c) Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

d) Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;

e) Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e executáveis de torrent;

f) Suportar a criação de políticas de QoS e Traffic Shaping por porta;

g) O QoS deve possibilitar a definição de tráfego com banda garantida;

h) O QoS deve possibilitar a definição de tráfego com banda máxima;

i) O QoS deve possibilitar a definição de fila de prioridade;

j) Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

k) Suportar marcação de pacotes Diffserv, inclusive por aplicação;

l) Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

m) Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;

5.1.3.98. **Filtro de Dados**

a) Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS

Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

b) Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

c) Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

d) Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

5.1.3.99. **Geo Localização**

a) Suportar a criação de políticas por geo-localização, permitindo o tráfego de determinado País/Países sejam bloqueados;

b) Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

c) Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

5.1.3.100. **VPN:**

a) Suportar VPN Site-to-Site e Cliente-To-Site;

b) Suportar IPSec VPN;

c) Suportar SSL VPN;

d) A VPN IPSEc deve suportar 3DES;

e) A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

f) A VPN IPSEc deve suportar Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;

g) A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

h) A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

i) A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

j) Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

k) Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

l) A VPN SSL deve suportar o usuário realizar a conexão por meio de agente instalado no sistema operacional do equipamento ou por meio de interface WEB;

m) A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

n) Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

o) Atribuição de DNS nos agentes remotos de VPN;

p) Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos agentes remotos conectados na VPN SSL;

q) Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

r) Suportar leitura e verificação de CRL (certificate revocation list);

s) Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

t) Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Antes do usuário autenticar na estação;

u) Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;

v) Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;

w) Deverá manter uma conexão segura com o portal durante a sessão;

x) O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

5.1.3.101. **Relatórios:**

a) Deve suportar receber logs de ao menos 10K dispositivos

b) Possuir capacidade de receber ao menos 1 GBytes de logs diários

c) Possuir ao menos 500 GB de capacidade de espaço em disco

d) Possuir ao menos 4 interfaces vNIC

e) Não deve possuir limitação de vCPUs. Caso tenha limitação, ou seja, licenciado, deve ser entregue com o número máximo de vCPUs

f) Não deve possuir limitação de memória RAM. Caso tenha limitação, ou seja, licenciado, deve ser entregue com quantidade máxima de memória RAM

g) Deve ser appliance do tipo virtual, compatível com VMWare ESX/ESXI 6.5 ou superior

h) Deve suportar acesso via SSH, WEB (HTTPS) e Telnet para o gerenciamento da solução.

i) Possuir comunicação cifrada e autenticada com usuário e senha para solução de relatórios, tanto como para a interface gráfica de usuário e console de administração por linha de comandos (SSH)

j) Permitir acesso simultâneo de administradores permitindo a criação de ao menos 2 (dois) perfis para administração e monitoração

k) Suportar SNMP versão 2 e versão 3 na solução de relatórios

l) Permitir virtualizar a solução de relatórios, onde cada administrador gerencie, visualize e edite apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado

m) Deve permitir a criação de administradores que acessem à todas as instâncias de virtualização da solução de relatórios

n) Deve permitir habilitar e desabilitar, para cada interface de rede da solução de relatórios, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet

o) Autenticação integrada a servidor Radius

p) Geração de relatórios em tempo real, para a visualização de tráfego observado, nos formatos: mapas geográficos e tabela;

q) Geração de relatórios em tempo real, para a visualização de tráfego observado, no formato bolhas;

r) Autenticação integrada ao Microsoft Active Directory

s) Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações

t) Deve possuir um assistente para adicionar dispositivos via interface gráfica usando o IP, login e senha dos mesmo.

u) Deve ser possível visualizar a quantidade de logs enviado de cada dispositivo monitorado.

v) Possuir mecanismo para que logs antigos sejam removidos automaticamente

w) Permitir a importação e exportação de relatórios

x) Deve possuir a capacidade de criar relatórios nos formatos HTML

y) Deve possuir a capacidade de criar relatórios nos formatos PDF

z) Deve possuir a capacidade de criar relatórios nos formatos XML

aa) Deve possuir a capacidade de criar relatórios nos formatos CSV

ab) Deve ser possível exportar os logs em CSV

ac) Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração

ad) Os logs gerados pelos appliances devem ser centralizados nos servidores de gerência, mas a solução deve oferecer também a possibilidade de utilização de um syslog externo ou similar.

ae) A solução deve possuir relatórios pré definidos

af) Possuir envio automático de logs para um servidor FTP externo a solução

ag) Possibilitar a duplicação de relatórios existentes e editá-los logo após

ah) Possuir a capacidade de personalização de capas para os relatórios

ai) Permitir de forma centralizada visualizar os logs recebidos por um ou vários dispositivos externos incluindo a capacidade de uso de filtros nas pesquisas deste log

aj) Logs de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados.

ak) Possuir a capacidade de personalização de gráficos como barra, linha e tabela para inserção aos relatórios

al) Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em realtime;

am) Dever ser possível fazer download dos arquivos de logs recebidos

an) Deve possuir agendamento para gerar e enviar automaticamente relatórios

ao) Permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente pelo administrador, adaptando-o às suas necessidades.

ap) Permitir o envio de maneira automática de relatórios por e-mail

aq) Deve permitir a escolha do e-mail a ser enviado para cada relatório escolhido

ar) Permitir programar a geração de relatórios, conforme calendário definido pelo administrador

as) Deve ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros

at) Permitir que relatórios criados sejam no idioma Português

au) Gerar alertas automáticos via Email e SMS, baseado em alertas de SNMP e Syslog baseados em eventos como ocorrência como log, severidade de log, entre outros

av) Deve permitir o envio automático de relatórios criado a um servidor de SFTP ou FTP externo a solução

aw) Deve ser capaz de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios

ax) Ter a capacidade de visualizar na GUI da solução de relatórios informações do sistema como licenças, memória, disco, uso de CPU, taxa de logs por segundo recebidos, total de logs diários recebidos, alertas gerados entre outros

ay) Deve possuir uma ferramenta para análise de desempenho para cada relatório gerado, com o

objetivo de detectar problemas de performance de sistema de acordo com o relatório criado.

az) Permitir que a solução importe arquivos de log, de dispositivos compatíveis conhecidos e não conhecidos pelo sistema, para posterior geração de relatórios

ba) Deve ser possível definir o espaço que cada instâncias de virtualização poderá utilizar para armazenamento de logs

bb) A solução deve servir como um servidor de syslog e aceitar logs de diferentes fabricantes

bc) Deve possuir a informação da quantidade de logs armazenado e estatística de tempo de retenção restante

bd) Deve suportar duplo fator de autenticação (token) para os administradores do sistema de relatórios

be) Deve permitir aplicar políticas de senhas para os administradores do sistema como tamanho mínimo e caracteres a usar

bf) Deve permitir ver em tempo real os log recebidos

bg) Deve permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

bh) Deve possuir um Indicador de Comprometimento (IoC), que mostre usuários finais com utilização web suspeita, devendo informar no mínimo: endereço ip do usuário, hostname, sistema operacional, veredito (classificação geral de ameaça), número de ameaças detectadas.

bi) Deve possuir relatório de PCI DSS Compliance

bj) Deve possuir relatório de utilização de aplicações SAAS

bk) Deve possuir relatório detalhado de prevenção de perda de dados (DLP)

bl) Deve possuir relatório de VPN

bm) Deve possuir relatório de Sistemas de prevenção de intrusão (IPS)

bn) Deve possuir relatório de reputação do cliente

bo) Deve possuir relatório de análise de segurança do usuário

bp) Deve possuir relatório de avaliação da ameaça cibernética

bq) Deve possuir relatório de WiFi PCI Compliance

br) Deve possuir relatório a informação de AP´s e SSID´s autorizados, também clientes WiFi

bs) Deve possuir relatório de equipamentos terminais de solução de segurança gerenciada

bt) Deve possuir relatório de análise de segurança e uso de web, se há uma plataforma de cache.

bu) Deve possuir relatório de análise aplicações web, se há uma plataforma de segurança web

5.1.3.102. **Gerência:**

a) Deve permitir gerenciar ao menos 20 dispositivos

b) Possuir ao menos 4 interfaces Vnic

c) Suportar mapeamento de ao menos 200 GB de espaço em disco

d) Deve permitir e estar licenciado para operar em alta disponibilidade (HA) sincronizando as mudanças na base de dados entre as estações de gerência

e) Caso a solução seja virtualizada, deverá ser compatível com ambiente VMwareESXi 6.5 ou superior;

f) Caso a solução seja virtualizada, deverá ser compatível com ambiente Microsoft Hyper-V

2008 R2 / 2012 / 2012 R2 / 2016 ou superior

g) Caso a solução seja virtualizada, deverá ser compatível com ambiente Citrix XenServer 6.0+ ou superior

h) Caso a solução seja virtualizada, deverá ser compatível com ambiente Open SourceXen 6.0+ ou superior

i) Caso a solução seja virtualizada, deverá ser compatível com ambiente KVM

j) Caso a solução seja virtualizada, deverá ser compatível com ambiente Amazon Web Services (AWS)

k) Não deve possuir limite na quantidade de múltiplas vCPU caso entregue como appliance virtual;

l) Não deve possuir limite para suporte a expansão de memória RAM caso entregue como appliance virtual;

m) Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

n) O gerenciamento da solução deve suportar acesso via SSH, software proprietário ou WEB (HTTPS) e API aberta;

o) Permitir acesso concorrente de administradores;

p) Possuir interface baseada em linha de comando para administração da solução de gerência

q) Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

r) Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;

s) Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

t) Gerar alertas automáticos via Email

u) Gerar alertas automáticos via SNMP

v) Gerar alertas automáticos via Syslog

w) Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora.

x) Deve ser permitido ao administrador transferir os backups para um servidor FTP.

y) Deve ser permitido ao administrador transferir os backups para um servidor SCP

z) Deve ser permitido ao administrador transferir os backups para um servidor SFTP

aa) As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante

ab) Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS

ac) Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa TACACS

ad) Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de usuários de base externa LDAP

ae) Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa RADIUS

af) Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de Certificado Digital X.509 (PKI)

ag) Deve suportar sincronização do relógio interno via protocolo NTP.

ah) Deve registrar as ações efetuadas por quaisquer usuários

ai) Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade.

aj) Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência

ak) Deve permitir habilitar e desabilitar, para cada interface de rede da solução de gerência, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet

al) Deve permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado.

am) A solução de gerência deve permitir criar administradores que tenham acesso à todas as instâncias de virtualização

an) Deve suportar XML API

ao) Deve suportar JSON API

5.1.3.103. **Funcionalidades de Gerência de UTM/NGFW:**

a) O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;

b) O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

c) O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;

d) Permitir localizar quais regras um objeto está sendo utilizado;

e) Deve atribuir sequencialmente um número a cada regra de firewall;

f) Deve atribuir sequencialmente um número a cada regra de DOS;

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

h) Permitir backup das configurações e rollback de configuração para a última configuração salva;

i) Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

j) Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;

k) Deve permitir que todos os firewalls sejam controlados de forma centralizada utilizando apenas um servidor de gerência.

l) Cada servidor de gerência deve ser hospedado em um equipamento independente, não exercendo funções de firewall.

m) A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta.

n) A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances.

o) Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas.

p) Deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas as mesmas somente sejam aplicadas após aprovação de outro administrador

q) Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos

r) Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência

s) Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horário do sistema e firmware.

t) Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos

u) Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração

v) Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos

w) Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência

x) Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada

y) Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos

z) Deve permitir criar regras de NAT64 e NAT46 de forma centralizada

aa) Permitir criar regras anti-DoS de forma centralizada

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

ac) Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia.

5.1.3.104. **Sub-Item 1.06 - Transceiver para Next Generation Firewall - TIPO 1**

a) GE SFP LX Transceiver

5.1.3.105. **Características:**

a) 1 GE SFP LX transceiver SFP - SFP/SFP+ slots

5.1.3.106. **Sub-Item 1.07 - Transceiver para Next Generation Firewall - TIPO 2**

a) 1 GE SFP RJ45 Transceiver

5.1.3.107. **Características:**

a) 1 GE SFP RJ45 transceiver SFP - SFP/SFP+slots

5.1.3.108. **Sub-Item 1.08 - Transceiver para Next Generation Firewall - TIPO 3**

a) 1 GE SFP SX Transceiver

5.1.3.109. **Características:**

a) 1 GE SFP SX transceiver SFP - SFP/SFP+ slots

5.1.3.110. **Sub-Item 1.09 - Transceiver para Next Generation Firewall - TIPO 4**

a) 10 GE SFP+ Transceiver, Short Range

5.1.3.111. **Características:**

a) 10 GE SFP+ transceiver SFP+, SFP/SFP+ slots

5.1.3.112. **Sub-Item 1.10 - Transceiver para Next Generation Firewall - TIPO 5**

a) 10 GE SFP+ Transceiver, Long Range

5.1.3.113. **Características:**

a) 10 GE SFP+ transceiver, long range SFP+, SFP/SFP+ slots

5.1.3.114. **Sub-Item 1.11 - Transceiver para Next Generation Firewall - TIPO 6**

a) 10 GE SFP+ Active Direct Attach, 10m / 32.8 ft

5.1.3.115. **Características:**

a) 10 GE SFP+ active direct attach, 10m / 32.8 ft, SFP+, SFP/SFP+ slots

5.1.4. **Sub-Item 1.12 - Serviço de controle de acesso seguro a rede LAN e WLAN.**

5.1.4.116. **Pacote de Licenças para usuários**

a) Fornecimento e garantia de pacotes de licenças para gerenciamento de dispositivos externos da rede wireless.

b) Cada pacote deve contemplar licenças para acesso dispositivos simultâneos de acordo com a instância contratada, conforme tabela abaixo;

Serviço de controle de acesso seguro a rede LAN e WLAN.	**Instância Mensal 500 Usuários**

c) Todas as licenças devem ser válidas pelo período de vigência da solicitação e em caráter permanente e contínuo, de forma que a solução funcione mesmo após o término da garantia exigida;

d) Toda solução deve ser instalada e as licenças devem ser instaladas e configuradas sem qualquer ônus adicional, incluindo as licenças de software de virtualização, utilizando as melhores práticas do fabricante.

e) Toda infraestrutura para implantação da solução será provida pelo IGES-DF, baseando-se nas especificações abaixo:

I - Os seguintes hipervisores devem ser suportados.

- VMware ESXi 5.0
- VMware ESXi 5.1
- VMware ESXi 5.5
- VMware ESXi 6.0
- VMware ESXI 6.5 ou superior

- Microsoft Hyper-V Server 2012 R2 ou superior
- Hyper-V no Microsoft Windows Server 2012 R2 ou superior

Requisitos máximos de VM para 500 à 5.000 usuários

* 2 CPUs virtuais

* 500 GB de espaço em disco

* 4 GB de RAM

* 2 portas virtual switched ports

* Classificação funcional da IOP para um perfil de leitura / gravação de 40 a 60 para leitura / gravação aleatória de 4K = 75

Requisitos máximos de VM para 5.000 à 10.000 usuários

* 8 CPUs virtuais

* Espaço em disco:

* 1000 GB de espaço em disco recomendado para novas implantações

* 8 GB de RAM

* 2 portas virtual switched ports

* Classificação funcional da IOP para um perfil de leitura / gravação de 40 a 60 para leitura / gravação aleatória de 4K = 105

5.1.4.117. **Software de Controle de Acesso**

a) Permitir a criação de páginas personalizadas no portal web para o *captive portal*, com a inclusão de imagens, instruções em texto e campos de texto que possam ser preenchidos pelos usuários;

b) Ser licenciada para permitir o controle de acesso para todos os usuários vinculados às licenças contratadas, simultâneos, com capacidade de expansão futura de acordo com as instâncias contratadas.

c) Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo visitante, em caso de "self-service", especificando quais informações cadastrais dos visitantes são obrigatórias conforme o perfil;

d) Deve exigir que o usuário visitante aceite o "Termo de uso da rede" a cada login ou apenas no primeiro login;

e) Deve implementar um portal web seguro (SSL) a ser apresentado automaticamente aos usuários temporários (visitante/servidor) durante a sua conexão com a rede (hotspot);

f) Deve implementar o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service) ou e-mail ou impressão local;

g) O portal de autenticação deve ser suportado, no mínimo, em um dos seguintes navegadores de Internet: Microsoft Internet Explorer, Mozilla Firefox, Safari e Chrome, operando em PCs e dispositivos móveis;

h) A solução deverá integrar com o Active Directory da Microsoft para identificação e autenticação dos usuários;

i) Possuir capacidade de autenticação dos usuários visitantes através de senhas pré-cadastradas ou vouchers, para cada indivíduo ou grupo, no caso de eventos;

j) Deverá permitir o encaminhamento do tráfego de saída de usuários visitantes (guests) diretamente para a Internet, de forma totalmente separada do tráfego da rede corporativa;

k) Permitir que as contas de visitantes tenham validade controlada com período de validade da senha em quantidade de horas, dias e semanas;

l) Permitir, a configuração do número máximo de conexões simultâneas realizadas por uma mesma conta, possibilitando que um usuário possua mais de um dispositivo na rede com a mesma senha e que contas coletivas sejam utilizadas em eventos. Esta funcionalidade deve ser possível em usuários visitantes autenticados pelo captive portal;

m) Implementar controle de acesso administrativo da solução baseado em função;

n) Implementar protocolo de autenticação para controle do acesso administrativo da solução utilizando servidor Radius ou Microsoft Active Directory;

o) Suportar IEEE 802.1x, com pelo menos os seguintes métodos EAP: EAP: EAP- TLS, PEAP-GTC, PEAP-MSCHAPv2;

p) Permitir a disponibilização ao usuário de um termo de uso, de forma que o usuário possa ler o termo de uso e realizar a aceitação do mesmo previamente a sua conexão à rede.

q) Deve implementar mecanismos de autenticação via integração com LDAP e Captive Portal com suporte a RADIUS Authentication e Accounting.

r) Implementar identificação e autenticação de usuários via integração com Facebook®, Linkedin®, Instagram®, Twitter® e Google®. Deve ainda implementar identificação e autenticação via auto registro, através de formulário customizável ao administrador da solução, a fim de permitir que, sejam criados a quantidade de informações pretendidas, contendo, no mínimo, Nome e E-mail do usuário, bem como mascaras de validações para CPF, Data de Nascimento e Telefone.

s) Implementar mecanismo de autorização, de forma que um patrocinador (sponsor), definido pela CONTRATANTE, possa autorizar o acesso do usuário via e-mail e via FQDN (Full Qualify Domain Name) previamente autorizados pela CONTRATANTE.

t) Implementar funcionalidade de busca por usuários já conhecidos (recorrentes), realizando a identificação do dispositivo móvel no ingresso e permissão de acesso do usuário sem a necessidade de nova autenticação.

u) Permitir que o layout das telas de acesso sejam customizáveis com no mínimo 01 (um) logotipo e 01 (um) fundo de tela, com a utilização de texto e imagens em formatos JPEG ou PNG;

v) Disponibilizar recurso de integração via WebService REST/API para consumo de dados da plataforma em tempo real por meio de acesso direto a API, fornecendo possibilidade de integração a solução de autenticação com os sistemas externos da CONTRATANTE.

w) Deve possuir múltiplos perfis de usuários administrativos com diferentes tipos de permissão.

x) Implementar recurso de liberação de acesso por endereço MAC, onde o endereço do dispositivo pode ser cadastrado manualmente ou adicionado dinamicamente para os usuários que já realizaram acesso ao menos uma vez;

y) Permitir a customização do período (horário) que o serviço estará disponível para os usuários visitantes. Deve permitir ainda as definições de dias durante a semana.

z) Permitir a gestão de tempo, com a definição do limite máximo de uso diário e tempo máximo de inatividade. A obtenção dos dados de conexões dos usuários, para fins de gestão do tempo, deve ser feita a partir da infraestrutura de rede WiFi via o protocolo RADIUS Accounting (contabilidade);

aa) Permitir a exportação de dados da plataforma nos formatos CSV e JSON.

ab) Suporte ao provisionamento automático de dispositivos, através de Portal Captivo para Windows, Mac OSX, iOS e Android. Deve possuir licenças para o provisionamento de 300 dispositivos BYOD.

ac) Para soluções virtualizadas, serão aceitos virtual appliances compatíveis com VMWare;

ad) Suporte a seguintes bases de dados:

- Microsoft Active Directory
- Kerberos
- LDAP-compliant directory
- ODBC-compliant SQL server
- Token servers
- Base SQL interna

ae) Deve implementar funcionalidade de classificação automática de dispositivos ("Device profiling"), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;

af) Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computadora, Smartdevice, impressora, etc.), por sistema operacional (ex. Windows, Linux, MacOS, etc.) e versão do sistema (ex. Windows 7, Windows 2008 Server, etc);

ag) Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, ActiveSync plugin, SNMP, SSH, Subnet Scanner, IF-MAP, sflow ou Netflow, MDM e TCP Fingerprinting;

ah) Deve possuir base de regras e categorias de dispositivos pré-configurada;

ai) Deve suportar mecanismo de atualização das regras e categorias pré-configuradas

5.2. **Item 02 - IAAS – Cloud Pública**

5.2.5. **Serviços de computação em nuvem**

5.2.5.1. 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 Termo de Referência, que atenda todos os serviços da Tabela 1 deste Termo de Referência, disponibilizando-os à CONTRATANTE.

- Todos os serviços apresentados na Tabela 1 somente serão aceitos se forem parte da lista de serviços da nuvem do provedor oferecido pela CONTRATADA, devendo ser contabilizados por meio de USNs. 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.

5.2.5.2. A CONTRATADA deverá disponibilizar uma conta no provedor em nome da CONTRATANTE, por meio da qual serão provisionados os serviços descritos na Tabela 1 deste Termo de Referência.

- 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 Tabela 3 deste Termo de Referência.

5.2.5.3. 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 (CONTRATANTE), colocação em produção, acompanhamento, bilhetagem e faturamento dos serviços mensalmente.

5.2.5.4. 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

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

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

5.2.5.6. O provedor disponibilizado pela CONTRATADA deverá fornecer todos os serviços listados na Tabela 1, de acordo com as descrições e níveis mínimos de serviço respectivos.

5.2.5.7. Os serviços descritos na Tabela 1 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. Todos os serviços técnicos especializados prestados pela CONTRATADA deverão estar aderentes às regras descritas no Guia de Gestão de Riscos de Aplicações em Nuvem Pública, definido no Anexo V deste Termo de Referência.

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

- Planilha de preços: valores praticados pela CONTRATADA com os preços de todos os serviços (em USN); informar também quais serviços do provedor são gratuitos;
- Relatório de Faturamento: relatórios com consumo de serviços do provedor;
- Informações sobre o contrato: detalhamento do contrato, tipos de serviços;
- Relatórios de avaliação de otimização e performance, contendo sugestões de melhorias, ajustes em diversos aspectos da infraestrutura;

5.2.5.9. 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 do Termo de Referência. O serviço estará dentro das responsabilidades da CONTRATADA, não sendo cobrado como serviço adicional.

5.2.5.10. A CONTRATADA fará uso de ferramenta de gestão de nuvem com, no mínimo, as seguintes funcionalidades:

- Definir centros de custos (unidades virtuais às quais podem ser atribuídos projetos, e às quais podem ser associadas despesas) e o orçamento para o projeto, e provisionar todos os recursos a serem utilizados, respeitando o orçamento atribuído;
- Permitir a criação, modificação e exclusão de usuários e grupos de usuários, aos quais poderão ser atribuídas permissões de acesso;
- Isolar financeira e logicamente os recursos computacionais do provedor utilizados em diferentes projetos, de modo a não haver nenhum tipo de interferência entre os projetos;
- Armazenar logs de acesso para fins de auditoria. Os logs deverão ser mantidos durante toda a vigência do contrato, devendo ser entregues à CONTRATANTE quando solicitados e no encerramento do contrato; O prazo de retenção desses logs poderão a qualquer tempo ser alterado de acordo com a determinação da CONTRATANTE.
- Permitir que, a partir de uma interface personalizada, o usuário com as devidas permissões tenha acesso aos recursos disponíveis no provedor e consiga executar ao menos tarefas básicas (criar/alterar/excluir servidores virtuais, volumes de armazenamento, configurações de rede, etc.) relacionadas aos serviços de computação em nuvem, listados na Tabela 1;
- Permitir monitorar as informações sobre a quantidade e o status das instâncias, bem como, o uso de seus recursos computacionais (CPU e RAM) e de outros serviços (tráfego de saída de rede, armazenamento**,** banco de dados, etc.), isoladamente por projeto;
- Permitir o monitoramento dos custos dos serviços;
- Permitir a emissão de alertas de gastos para cada projeto. Os alertas deverão ser apresentados na ferramenta e enviados por **e-mail** para os usuários responsáveis, previamente cadastrados;
- Emitir relatório com todos os custos de recursos relacionados a determinado projeto.
- Emitir relatório gerencial por centro de custos, com informações referentes ao orçamento por projeto, valores utilizados e saldo restante;

5.2.5.11. Todas as ferramentas, soluções, **software** e **scripts** fornecidos pela CONTRATADA deverão ser executados em infraestrutura da CONTRATANTE ou no próprio provedor de nuvem, a ser definido pela CONTRATANTE.

- Sob nenhuma hipótese a CONTRATANTE arcará com custos relacionados ao direito de uso das ferramentas;
- A CONTRATANTE não ficará responsável pela instalação, manutenção e suporte continuado de tais ferramentas, nem emitirá ordens de serviço para esses fins, devendo essa ser uma das responsabilidades da CONTRATADA;
- Ao final do contrato, o direito de uso das ferramentas deverá ser de propriedade da CONTRATADA

5.2.5.12. 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 listadas na Tabela 1 deste Termo de Referência:

- Windows Server 2012 R2 ou superior;
- Linux CentOS 7 ou superior;
- Linux Debian 9 ou superior;
- Linux Ubuntu Server 16.04.2 ou superior;
- Red Hat Server 7 ou superior;
- SQL Server 2016 SP1 Standard ou superior;
- MySQL Community 5.5 ou superior;
- Maria DB 10 ou superior;
- PostgreSQL 9.4 ou superior;
- Oracle 10 ou superior;
- Oracle Linux 6.5 ou superior.

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

5.2.5.14. 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 99,741% para cada período de 1 mês.

5.2.5.15. A CONTRATADA deve oferecer calculadora ou simulador público de preços para cada item da tabela 1 para o provedor que integra a solução.

5.2.5.16. Quando houver alteração na forma de contratação de **on-demand** para **upfront**, não poderá haver qualquer tipo de alteração na infraestrutura.

5.2.5.17. Ao final do período de utilização dos recursos na modalidade **upfront**, a máquina virtual será automaticamente considerada **on-demand**.

5.2.5.18. 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.

5.2.5.19. 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.

5.2.5.20. 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.

5.2.5.21. Todos os serviços prestados pela CONTRATADA devem ser realizados de modo que as aplicações da CONTRATANTE provisionadas na nuvem, afetadas direta ou indiretamente por estes serviços, sejam portáveis para outros provedores, sem nenhuma possibilidade de aprisionamento

(**lock-in)**.

- Para o cumprimento do disposto no item 5.1.21, deverá ser utilizada a ferramenta de gestão de nuvem provida pela CONTRATADA de acordo com os requisitos definidos neste Termo de Referência. Além disso, não deverão ser utilizados serviços, protocolos ou ferramentas nativos de apenas um provedor (proprietários), salvo quando justificável tecnicamente ou por decisão de projeto/operação e autorizados formalmente pela CONTRATANTE.
- Caso seja tomada a decisão de utilizar qualquer serviço, protocolo ou ferramenta que torne uma ou mais aplicações da CONTRATANTE não portáveis para outros provedores de nuvem, nas Matrizes de Riscos e nos Planos de Saída correspondentes deverão ser considerados os riscos inerentes a esta decisão e também indicadas alternativas para que estas aplicações possam, em caso de necessidade, serem reprovisionadas em outros provedores de serviços em nuvem e/ou Infraestruturas.
- Será de responsabilidade da CONTRATADA garantir a portabilidade das aplicações para outros provedores.

5.2.5.22. No momento em que for estudada a possibilidade de renovação do contrato, será facultado à CONTRATANTE e à CONTRATADA propor a substituição do provedor. Tal proposição deverá ser acompanhada de estudo de viabilidade que comprove existir no mercado outros provedores que atendam às condições deste Termo de Referência, de modo que não haja modificações no objeto da contratação. A substituição só poderá ocorrer mediante acordo mútuo entre CONTRATANTE e CONTRATADA, considerando que toda a migração dos sistemas e infraestrutura seja feita pela CONTRATADA sem nenhum ônus para a CONTRATANTE.

5.2.5.23. Tabela 1 – Serviços de computação em nuvem

Item	**Descrição do serviço (por reserva de recurso)**	**Unidade**	**Valor de referência (USN)**
1.	Máquina virtual padrão - adquirida por meio de vCPU, reservada por no mínimo 1 ano.	Unidade de vCPU/hora	
2.	Máquina virtual padrão - adquirida por meio de memória, reservada por mínimo 1 ano.	Gigabyte de memória/hora	
3.	Máquina virtual Windows - adquirida por meio de vCPU, reservada por no mínimo 1 ano .	Unidade de vCPU/hora	
4.	Máquina virtual Windows - adquirida por meio de memória, reservada no mínimo por 1 ano .	Gigabyte de memória/hora	
5.	Máquina virtual com serviço de hospedagem de container gerenciado - adquirida por meio de vCPU, reservada no mínimo por 1 ano.	Unidade de vCPU/hora	
Item	**Descrição do serviço (por demanda)**	**Unidade**	**Valor de referência (USN)**
6.	Máquina virtual padrão - adquirida por meio de vCPU (por demanda)	Unidade de vCPU/hora	

7.	Máquina virtual padrão - adquirida por meio de memória (por demanda)	Gigabyte de memória/hora	
8.	Máquina virtual Windows - adquirida por meio de vCPU (por demanda)	Unidade de vCPU/hora	
9.	Máquina virtual Windows - adquirida por meio de memória (por demanda)	Gigabyte de memória/hora	
10.	Serviço de armazenamento de blocos (SSD)	Gigabyte/mês	
11.	Serviço de armazenamento de blocos (HDD)	Gigabyte/mês	
12.	Serviço de armazenamento de objetos	Gigabyte/mês	
13.	Serviço para coleta de logs (SIEM)	TIER /ano	
14.	Tráfego de saída da rede	Gigabyte/mês	
15.	Tráfego de rede do balanceador de carga	Gigabyte/mês	
16.	Tráfego de rede do CDN	Gigabyte/mês	
17.	Serviço de balanceamento de carga (*)	Unidade/hora	
18.	Serviço de balanceamento de carga utilizando gerenciador de tráfego (*)	DNS Queries Milhão/Mês	
19.	Porta de conexão de fibra 10Gbps	Unidade/hora	
20.	Serviço de DNS – Hospedagem de zonas	Zona/mês	
21.	Serviço de DNS – Consultas	Milheiro de consulta/mês	
22.	Serviço de VPN	Gigabyte/Mês	
23.	VPN Gateway	Hora de Conexão	
24.	Serviço Web Aplication Firewall adquirido por ACL (**)	ACL/hora	
25.	Serviço Web Aplication Firewall adquirido por hora (**)	Gateway/hora	

26.	Serviço de Backup	Instância/mês	
27.	Serviço de armazenamento de Backup	Gigabyte/mês	
28.	Serviço de Autenticação (Integração com AD) adquirido por usuário (***)	Por usuário/Mês	
29.	Serviço de Autenticação (Integração com AD) adquirido por mês (***)	Gigabyte/Mês	
30.	Serviço de Auditoria e Análise de Logs	Gigabyte/Mês	
31.	IP Público	Unidade/Mês	
32.	Serviço de BI	Usuário/Mês	
33.	Serviço de Plataforma de Gerenciamento de BI	Usuário/Mês	

(*) O Serviço de balanceamento de carga deverá ser prestado na métrica definida no subitem 16 ou no subitem 17 a ser indicada pela CONTRATADA na proposta de preços.

(**) Os serviços de *Web Aplication Firewall* deverão ser prestados na métrica definida no subitem 25 ou no subitem 26 a ser indicada pela CONTRATADA na proposta de preços.

(***) Os serviços de Autenticação deverão ser prestados na métrica definida no subitem 29 ou no subitem 30 a ser indicada pela CONTRATADA na proposta de preços.

5.2.5.24. **Sub-Item 2.1 - Máquina virtual Padrão - adquirida por meio de vCPU, reservada por 1 ano.**

a) Máquinas virtuais para utilização do Sistema Operacional (SO) Linux.

b) As máquinas virtuais serão contratadas exclusivamente em função do número de vCPUs solicitado, respeitadas as configurações pré-existentes de máquinas virtuais do provedor, e independente de outros recursos existentes na máquina (como GB de RAM, disco SSD, número de IPs, etc.).

c) As máquinas virtuais devem ser fornecidas com disco destinado ao **boot** e hospedagem do sistema operacional. A capacidade do disco deve ser suficiente para atender aos requisitos de sistema operacional e seus processos de manipulação de memória;

d) As máquinas virtuais serão contratadas e remuneradas na modalidade **upfront**.

e) As máquinas virtuais deverão contar com o serviço de crescimento automático em função da demanda (**autoscaling**).

f) Entende-se por **autoscaling** a escala horizontal automática do serviço, podendo ser atendida por meio de adição ou remoção de instâncias da máquina virtual, conforme definição do projeto.

g) As máquinas virtuais provisionadas utilizando o serviço de **autoscaling** associado a máquinas virtuais contratadas e remuneradas na modalidade **upfront**, serão contratadas e remuneradas na modalidade **on-demand**.

5.2.5.25. **Sub-Item 2.2 - Máquina virtual Padrão - adquirida por meio de memória, reservada por 1 ano.**

h) Máquinas virtuais para utilização do SO Linux.

i) As máquinas virtuais serão contratadas exclusivamente em função do número de **gigabytes** de RAM solicitado, respeitadas as configurações pré-existentes de máquinas virtuais do provedor, e independente de outros recursos existentes na máquina (como vCPUs, disco SSD, número de IPs, etc.).

j) As máquinas virtuais devem ser fornecidas com disco destinado ao **boot** e hospedagem do sistema operacional. A capacidade do disco deve ser suficiente para atender aos requisitos de sistema operacional e seus processos de manipulação de memória;

k) . As máquinas virtuais serão contratadas e remuneradas na modalidade **upfront**.

l) As máquinas virtuais deverão contar com o serviço de crescimento automático em função da demanda (**autoscaling).**

m) Entende-se por **autoscaling** a escala horizontal automática do serviço, podendo ser atendida por meio de adição ou remoção de instâncias da máquina virtual, conforme definição do projeto.

n) As máquinas virtuais provisionadas utilizando o serviço de **autoscaling** associado a máquinas virtuais contratadas e remuneradas na modalidade **upfront**, serão contratadas e remuneradas na modalidade **on-demand**.

5.2.5.26. **Sub-Item 2.3 - Máquina virtual Windows - adquirida por meio de vCPU, reservada por 1 ano.**

a) Máquinas virtuais com o SO Windows Server.

b) As máquinas virtuais serão contratadas exclusivamente em função do número de vCPUs solicitado, respeitadas as configurações pré-existentes de máquinas virtuais do provedor, e independente de outros recursos existentes na máquina (como GB de RAM, disco SSD, número de IPs, etc.).

c) As máquinas virtuais devem ser fornecidas com disco destinado ao **boot** e hospedagem do sistema operacional. A capacidade do disco deve ser suficiente para atender aos requisitos de sistema operacional e seus processos de manipulação de memória;

d) As máquinas virtuais serão contratadas e remuneradas na modalidade **upfront**.

e) O ambiente da máquina virtual deverá permitir implementação em ambiente de alta disponibilidade.

f) As máquinas virtuais provisionadas utilizando o serviço de **autoscaling** associado a máquinas virtuais contratadas e remuneradas na modalidade **upfront**, serão contratadas e remuneradas na modalidade **on-demand**.

5.2.5.27. **Sub-Item 2.4 - Máquina virtual Windows - adquirida por meio de memória, reservada por 1 ano.**

o) Máquinas virtuais com o SO Windows Server.

p) As máquinas virtuais serão contratadas exclusivamente em função do número de **gigabytes** de RAM solicitado, respeitadas as configurações pré-existentes de máquinas virtuais do provedor, e independente de outros recursos existentes na máquina (como vCPUs, disco SSD, número de IPs, etc.).

q) As máquinas virtuais devem ser fornecidas com disco destinado ao **boot** e hospedagem do sistema operacional. A capacidade do disco deve ser suficiente para atender aos requisitos de sistema

operacional e seus processos de manipulação de memória;

r) As máquinas virtuais serão contratadas e remuneradas na modalidade **upfront**.

s) O ambiente da máquina virtual deverá permitir implementação em ambiente de alta disponibilidade.

t) As máquinas virtuais provisionadas utilizando o serviço de **autoscaling** associado a máquinas virtuais contratadas e remuneradas na modalidade **upfront**, serão contratadas e remuneradas na modalidade **on-demand**.

5.2.5.28. **Sub-Item 2.5 - Máquina virtual com Serviço de Hospedagem de container gerenciado - adquirida por meio de vCPU, reservada por 1 ano**

a) Serviço para utilização de máquinas virtuais para fins de instalação e hospedagem de **containers**.

b) O serviço deve permitir a construção e execução de **containers Docker**.

c) As máquinas virtuais serão contratadas exclusivamente em função do número de vCPU solicitado, respeitadas as configurações pré-existentes de máquinas

d) virtuais do provedor, e independente de outros recursos existentes na máquina (como GB de RAM, disco SSD, número de IPs, etc.).

e) As máquinas virtuais devem ser fornecidas com disco destinado ao **boot** e hospedagem do sistema operacional. A capacidade do disco deve ser suficiente para atender aos requisitos de sistema operacional e seus processos de manipulação de memória;

f) As máquinas virtuais serão contratadas e remuneradas na modalidade **upfront**.

g) O ambiente da máquina virtual deverá permitir implementação em ambiente de alta disponibilidade

5.2.5.29. **Sub-Item 2.6 - Máquina virtual Padrão - adquirida por meio de vCPU (por demanda).**

a) Máquinas virtuais para utilização do Sistema Operacional (SO) Linux.

b) As máquinas virtuais serão contratadas exclusivamente em função do número de vCPUs solicitado, respeitadas as configurações pré-existentes de máquinas virtuais do provedor, e independente de outros recursos existentes na máquina (como GB de RAM, disco SSD, número de IPs, etc.).

c) As máquinas virtuais devem ser fornecidas com disco destinado ao **boot** e hospedagem do sistema operacional. A capacidade do disco deve ser suficiente para atender aos requisitos de sistema operacional e seus processos de manipulação de memória;

d) As máquinas virtuais deverão contar com o serviço de crescimento automático em função da demanda (**autoscaling**).

e) Entende-se por **autoscaling** a escala horizontal automática do serviço, podendo ser atendida por meio de adição ou remoção de instâncias da máquina virtual, conforme definição do projeto.

5.2.5.30. **Sub-Item 2.7 - Máquina virtual Padrão - adquirida por meio de memória (por demanda).**

h) Máquinas virtuais para utilização do SO Linux.

i) As máquinas virtuais serão contratadas exclusivamente em função do número de **gigabytes** de RAM solicitado, respeitadas as configurações pré-existentes de máquinas virtuais do provedor, e

independente de outros recursos existentes na máquina (como vCPUs, disco SSD, número de IPs, etc.).

j) As máquinas virtuais devem ser fornecidas com disco destinado ao **boot** e hospedagem do sistema operacional. A capacidade do disco deve ser suficiente para atender aos requisitos de sistema operacional e seus processos de manipulação de memória;

k) As máquinas virtuais deverão contar com o serviço de crescimento automático em função da demanda (**autoscaling).**

l) Entende-se por **autoscaling** a escala horizontal automática do serviço, podendo ser atendida por meio de adição ou remoção de instâncias da máquina virtual, conforme definição do projeto.

5.2.5.31. **Sub-Item 2.8 - Máquina virtual Windows - adquirida por meio de vCPU (por demanda).**

a) Máquinas virtuais com o SO Windows Server.

b) As máquinas virtuais serão contratadas exclusivamente em função do número de vCPUs solicitado, respeitadas as configurações pré-existentes de máquinas virtuais do provedor, e independente de outros recursos existentes na máquina (como GB de RAM, disco SSD, número de IPs, etc.).

c) As máquinas virtuais devem ser fornecidas com disco destinado ao **boot** e hospedagem do sistema operacional. A capacidade do disco deve ser suficiente para atender aos requisitos de sistema operacional e seus processos de manipulação de memória;

d) O ambiente da máquina virtual deverá permitir implementação em ambiente de alta disponibilidade.

5.2.5.32. **Sub-Item 2.9 - Máquina virtual Windows - adquirida por meio de memória (por demanda).**

a) Máquinas virtuais com o SO Windows Server.

b) As máquinas virtuais serão contratadas exclusivamente em função do número de **gigabytes** de RAM solicitado, respeitadas as configurações pré-existentes de máquinas virtuais do provedor, e independente de outros recursos existentes na máquina (como vCPUs, disco SSD, número de IPs, etc.).

c) As máquinas virtuais devem ser fornecidas com disco destinado ao **boot** e hospedagem do sistema operacional. A capacidade do disco deve ser suficiente para atender aos requisitos de sistema operacional e seus processos de manipulação de memória;

d) O ambiente da máquina virtual deverá permitir implementação em ambiente de alta disponibilidade.

5.2.5.33. **Sub-Item 2.10 - Serviço de armazenamento de blocos (SSD)**

a) Serviço para utilização de volume de armazenamento **block-level.**

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

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

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

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

f) 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.

5.2.5.34. **Sub-Item 2.11 - Serviço de armazenamento de blocos (HDD)**

a) Serviço para utilização de volume de armazenamento **block-level.**

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

c) Deverá ser baseado em discos magnéticos (HDD).

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

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

f) 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.

5.2.5.35. **Sub-Item 2.12 - Serviço de armazenamento de objetos**

a) Serviço para utilização de volume de armazenamento de objetos.

b) Deverá ser durável, escalável e seguro.

c) Deverá possuir recurso de versionamento.

d) Deverá possuir **interface web** para inclusão e consultas de informações.

e) Deverá possuir API para **upload** de arquivos via aplicações desenvolvidas por terceiros.

5.2.5.36. **Tráfego de saída da rede**

a) Serviço de transmissão de dados de saída da rede.

b) Nenhum tráfego de entrada para a rede será cobrado.

5.2.5.37. **Tráfego de rede do Balanceador de Carga**

a) Serviço de transmissão de dados do Balanceador de Carga.

5.2.5.38. **Tráfego de rede do CDN**

a) Serviço de transmissão de dados de Rede de Distribuição de Conteúdo (**Content Delivery Network – CDN**).

5.2.5.39. **Sub-Item 2.14 - Tráfego de saída da rede**

a) Serviço de transmissão de dados de saída da rede

b) Serviço de transmissão de dados de saída da rede.

c) Nenhum tráfego de entrada para a rede será cobrado.

5.2.5.40. **Sub-Item 2.15 - Tráfego de rede do balanceador de carga**

a) Serviço de transmissão de dados do Balanceador de Carga.

5.2.5.41. **Sub-Item 2.16 - Tráfego de rede do CDN**

a) Serviço de transmissão de dados de Rede de Distribuição de Conteúdo (Content Delivery Network – CDN).

5.2.5.42. **Sub-Item 2.17 - Serviço de balanceamento de carga (*)**

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

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

c) 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.

d) Deverá permitir uso de serviço de fidelização por **cookies** (**sticky session**).

5.2.5.43. **Sub-Item 2.18 - Serviço de balanceamento de carga utilizando gerenciador de tráfego (*)**

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

b) Deverá fornecer **failover** automático quando um ponto de extremidade ficar inativo;

c) 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 usuário;

d) Deverá permitir operações de manutenção planejada nas aplicações sem tempo de inatividade;

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

5.2.5.44. **Sub-Item 2.19 - Porta de conexão de fibra 10 Gbps**

a) 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.

b) A porta do provedor deverá estar localizada em território nacional.

c) Todos os custos de conexão da CONTRATANTE até a porta de conexão do provedor serão de responsabilidade da CONTRATANTE.

5.2.5.45. **Sub-Item 2.20 - Serviço de DNS – Hospedagem de zonas**

a) 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.

5.2.5.46. **Sub-Item 2.21 - Serviço de DNS – Consultas**

a) 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.

b) 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.

5.2.5.47. **Sub-Item 2.22 - Serviço de VPN**

a) Serviço para uso de Rede Privada Virtual (**Virtual Private Network – VPN**);

b) O serviço será contratado usando a métrica de GB trafegado por mês;

c) 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;

d) Somente o tráfego de saída será contabilizado para cobrança do serviço;

e) 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

f) O tráfego de dados através da conexã o deve ser por túnel VPN utilizando o protocolo IPSec;

g) A taxa de transferência mínima na conexão VPN deve ser de 100 Mbps, podendo, entretanto, ser inferior quando limitada pela capacidade da conexão (**link** de dados) da CONTRATANTE.

5.2.5.48. **Sub-Item 2.23 Serviço de VPN Gateway**

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

b) Possibilitar o envio do tráfego criptografado em uma conexão pública;

c) Permitir a criação de VPN conforme descrito no Serviço de VPN;

d) Estão inclusos nesse serviço os custos do **gateway** por hora de conexão da VPN.

5.2.5.49. **Sub-Item 2.24 - Serviço de Web Aplication Firewall adquirido por Regra de ACL (**)**

a) Serviço para fornecer proteção centralizada dos aplicativos Web, contra vulnerabilidades e eventuais ataques;

b) O serviço será remunerado por Regra de ACL (Access Control List);

c) Deverá fornecer proteção sem modificar o código de back-end;

d) Deverá proteger vários aplicativos Web ao mesmo tempo por trás de um gateway de aplicativo;

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

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

5.2.5.50. **Sub-Item 2.25 - Serviço de Web Aplication Firewall adquirido por hora (**)**

a) Serviço para fornecer proteção centralizada dos aplicativos Web, contra vulnerabilidades e eventuais ataques;

b) O serviço será remunerado por hora de utilização do gateway;

c) Deverá fornecer proteção sem modificar o código de back-end;

d) Deverá proteger vários aplicativos Web ao mesmo tempo por trás de um gateway de aplicativo;

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

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

5.2.5.51. **Sub-Item 2.26 - Serviço de Backup**

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

b) Deverá alocar e gerenciar automaticamente o armazenamento de backup;

c) Deverá permitir a transmissão segura e o armazenamento dos dados criptografados;

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

e) Deverá permitir retenção dos backups, durante vigência do contratos;

f) Deverá permitir transferência de dados ilimitada, tanto para backup quanto para restore;

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

5.2.5.52. **Sub-Item 2.27 - Serviço de armazenamento de backup**

a) Serviço com possibilidade de armazenamento heterogêneo, local ou em nuvem, de cópias de segurança;

b) O serviço de armazenamento de Backup em nuvem, deve prover escala ilimitada e proporcionar alta disponibilidade, sem necessidade de manutenção ou sobrecarga de monitoramento;

c) Os dados devem ser persistidos com redundância, de no mínimo 3 cópias dos dados em equipamentos de **hardware** diferentes, de forma a prevenir perda de dados com falhas de hardware;

d) Deverá permitir retenção de dados por período indeterminado;

e) Deverá permitir a criptografia dos dados.

5.2.5.53. **Sub-Item 2.28 - Serviço de Autenticação (Integração com AD) adquirido por usuário (***)**

a) Serviço para fornecer uma identidade comum para acesso aos recursos na nuvem;

b) O serviço será remunerado por usuário;

c) Deverá sincronizar o serviço de diretório local com o serviço de diretório da nuvem.

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

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

f) Deverá permitir a escolha de quais objetos serão sincronizados.

5.2.5.54. **Sub-Item 2.29 - Serviço de Autenticação (Integração com AD) adquirido por mês (***)**

a) Serviço para fornecer uma identidade comum para acesso aos recursos na nuvem;

b) Deverá sincronizar o serviço de diretório local com o serviço de diretório da nuvem.

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

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

e) Deverá permitir a escolha de quais objetos serão sincronizados.

5.2.5.55. **Sub-Item 2.30 - Serviço de Auditoria e Análise de Logs**

a) Os serviços de segurança da informação deverão ser contratados em conjunto a um módulo de coleta para a proponente possa ter visibilidade remota e ou local dos eventos dos dispositivos do ponto de vista de segurança da informação.

b) O Coletor será sempre considerado como base de visibilidade do ambiente do IGESDF, Hospitais e ou UPA que pode estar em locais diferentes e fica de responsabilidade da Proponente avaliar a melhor arquitetura para coleta de logs dos dispositivos.

c) A proponente deverá disponibilizar recursos para coleta e retenção de dados pelo menos com as seguintes características e com contratação mínima de 12 meses, apenas para retenção de dados.

d) Lista de coletores físicos que poderão ser contratados como serviço:

	Tier 1 (50M EPD)	Tier 2 (100M a 250M EPD)	Tier 3 (500M a 250M EPD)	Tier 4
CPU	Intel E5-2620 6 cores	2X Intel E5-2630v2 6 core	2X Intel E5-2658v2 10 core	2X Intel E5-2650v2 6 core
RAM	32GB	32GB	96GB	64GB
Disk	4X4TB Nearline SAS	4X4TB SAS	8X4TB SAS	2X1TB SATA
	200GB SSD	200GB SSD	400GB SSD	400GB SSD
NIC	1X dual 1GigE Copper	2X dual 1GigE Copper	2X dual 1GigE Copper	2X dual 1GigE Copper
RAID	5	5	5	0
HBA	No	No	No	Qlogic 16GB Dual Port Fiber
Dimensões	19.8 x 17.2 x 1.7 in	25.6 x 17.2 x 1.7 in	25.51 x 17.2 x 3.5 in	25.6 x 17.2 x 1.7 in
	503 x 437 x 43 mm	650 x 437 x 43 mm	648 x 437 x 89 mm	650 x 437 x 43 mm
Form Factor	1U	1U	2U	1U
Peso	37lb 16.8kg	45lb 20.5kg	71lb 32 kg	45 lb 20.5kg

AC Power	350W - 100-240 V, 50-60 Hz, 4.2-1.8 Amp	700W - 100-240 V, 50-60 Hz, 8.5-3.8 Amp	740W - 100-240 V, 50-60 Hz, 9-3.5 Amp	700W - 100-240 V, 50-60 Hz, 8.5-3.8 Amp
Certificações	UL, CUL, TUV, CE	UL, CSA, CE	UL, CSA, CE	UL, CSA, CE
Online Retention (possível desde que recomendada pela Proponente)*	5 years	2.5 years (at 100m epd)	15 months (at 500m epd)	SAN dependent
		1 year (at 250m epd)	10 months (at 750m epd)	

5.2.5.56. **Ficará de responsabilidade da proponente dimensionar o coletor para retenção de dados conforme a necessidade do IGESDF, este estudo será executado através de preenchimento detalhada dos ativos que enviarão os logs.**

5.2.5.57. **Virtual Appliances**

	Tier 1 (50M EPD)	Tier 2 (100M EPD)	Tier 3 (250M EPD)	Tier 4 (500M EPD)	Tier 5 (750M EPD
Host Minimal Requirements					
Hypervisor	VMware ESX/ESXiMicrosoft Hyper-V	VMware ESX/ESXi Microsoft Hyper-V	VMware ESX/ESXi Microsoft Hyper-V	VMware ESX/ESXi Microsoft Hyper-V	VMware ESX/ESXi Microsoft Hyper-V
CPU	Dual Core ServerIntel VT-x or AMD-V	Dual Core ServerIntel VT-x or AMD-V	Dual Core ServerIntel VT-x or AMD-V	Dual Core ServerIntel VT-x or AMD-V	Dual Core ServerIntel VT-x or AMD-V
Guest Recommended Settings					
Virtual Cores	2	4	4	6	8
Memory	32G	32G	32G	96G	96G
Disk	Per data retention requirements				
NIC	2	2	2	2	2

5.2.5.58. **Amazon Web Services (AWS)**

5.2.5.59. **Tipo de instancias**

50M EPD	**100M EPD**	**250M EPD**	**500M EPD**

m4.xlarge	**m4.xlarge**	**m4.2xlarge**	**m4.4xlarge**

5.2.5.60. **Microsoft Azure –**

5.2.5.61. **Tipo de instancias**

50M EPD	**100M EPD**	**250M EPD**	**500M EPD**
E2s_v3	**E4s_v3**	**E8s_v3**	**E8s_v3**

5.2.5.62. As referencias de máquinas virtuais em nuvem devem ser utilizadas como referência e contratadas conforme as especificações desse Edital em formato IaaS.

5.2.5.63. Devido a necessidade do IGESDF a Proponente deverá disponibilizar a contratação de serviços de coleta de forma não centralizada disponibilizando equipamentos para coleta multi-site com as seguintes características mínimas.

5.2.5.64. Coletor de log (Appliance)

5.2.5.65. Lightweight log collector for the Managed Threat Detection service

Coletor/ PHYSICAL APPLIANCE – 250M EPD	
CPU	**Intel E3845**
RAM	**4GB**
Disk	**64G SSD**
RAID	**No**
Dimensions	**1.73 x 9.0 x 5.99 in44 x 231.9 x 152 mm**
High Availability	**No**
Form Factor	**Set-top (with 1U racking kit)**
Weight	**9lb 4.1kg**
DC Power	**12V/5A**

Coletor - VIRTUAL APPLIANCE – 250M EPD	
Hypervisor	**VMWare ESX/ESXiMicrosoft Hyper-V**
CPU	**Intel VT-x or AMD-V**
Guest Recommended Settings	
Virtual Cores	**2**
Memory	**6G**
Disk	**64G**
NIC	**2**

Coletor - AMAZON WEB SERVICES (AWS) – 250M EPD	
Instance Type	**t2.medium**
MICROSOFT AZURE LCA – 250M EPD	
Instance Type	**Standard_B2s**

Para solicitação do coletor de logs o IGESDF preencherá a tabela abaixo e a proponente indicará o coletor ou os coletores que atenderão a densidade de logs que deverão ser retidos no coletor.

Localização	IP	Modelo	Fabricante	Version	Quantidade	

5.2.6. **Sub-Item 2.31 - IP Público**

5.2.6.66. 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.

5.2.6.67. **Sub-Item 2.32 - Serviço de BI:**

a) Serviço de nível profissional para análise de negócios baseado em nuvem com fornecimento de uma exibição de dados de negócios;

b) Deverá permitir a implantação, distribuição e compartilhamento de relatórios interativos;

c) Deverá permitir o acesso aos relatórios pela Web e aplicativos móveis;

d) Deverá permitir conexão a diversas fontes de dados.

5.2.6.68. **Sub-Item 2.33 - Serviço de Plataforma de Gerenciamento de BI:**

a) Solução de nível profissional para Gerenciamento de Serviços de BI.

5.3. **Item 03 – SERVIÇOS DE CLOUD**

5.3.7. **Sub-Item 3.1 - SERVIÇOS DE MENSAGERIA, COMPARTILHAMENTO DE ARQUIVOS E COLABORAÇÃO**

5.3.7.69. Solução integrada de colaboração e comunicação corporativa baseada em nuvem, com garantia e suporte técnico por 12 (dose) meses, compreendendo os serviços de correio eletrônico (webmail), comunicação instantânea (chat), videoconferência por envio de vídeo ponto a ponto, armazenamento e compartilhamento de arquivos;

5.3.7.70. O quantitativo de licenças para mensageria colaborativa, está baseada não quantitativo de usuários administrativos. Distribuidos Conforme tabela abaixo:

Qtd. de usuários administrativos	Qtd. de Licenças TIPO 1	Qtd. de licenças TIPO 2
11500	10000	1500

5.3.7.71. **Disponibilização de caixas postais e colaboração - Tipo 1**

a) Cada usuário cadastrado no sistema com este tipo de licenciamento deverá ter a seu dispor através de navegadores Internet as seguintes funcionalidades:

b) Licença de Comunicação Unificada Tipo I com subscrição para 12 meses;

c) Conta de e-mail com capacidade de armazenamento de pelo menos 50 Gbytes;

d) O correio eletrônico deverá permitir a configuração de resposta automática de ausência;

e) O correio eletrônico deverá ter o recurso que permite um usuário (assistente ou secretária) enviar e-mail em nome de outro usuário (outra conta) no conceito de delegação de acesso à conta;

f) Deverá estar disponível no correio eletrônico a capacidade de acesso a mensagens em modo off sem conexão à Internet;

g) Capacidade de envio de mensagens instantâneas;

h) Funcionalidade de bate-papo por texto, voz e vídeo;

i) Funcionalidade de pesquisa da caixa de e-mail;

j) Capacidade de compartilhamento de contatos entre usuários;

k) Antivírus e filtro de spam no e-mail;

l) Agenda de compromissos com capacidade de compartilhamento de agendas com outros usuários;

m) Acesso e compartilhamento de documentos do texto, planilha eletrônica e apresentação armazenados na nuvem com gerenciamento de permissões de compartilhamento, definidos pelo usuário proprietário do documento, permitindo a edição simultânea e a recuperação de versões anteriores. O ambiente deve ter uma ferramenta de busca de informação;

n) Deve possibilitar a criação e edição de arquivos em formatos Word, Excel, PowerPoint, em um navegador Internet;

o) Unidade de disco virtual na nuvem com capacidade mínima de 25 Gbytes não compartilhado com o correio eletrônico; A solução deve permitir a instalação de a gente no computador que permita o acesso aos arquivos emulando uma unidade de disco local. Os arquivos armazenados na unidade virtual podem ser compartilhados pelo seu proprietário a outros usuários. O ambiente deve ter uma ferramenta de busca de informação;

p) Capacidade de criação de grupos de usuários em fóruns de discussão e blogs;

q) Capacidade de criação de sites colaborativos para divulgação de projetos e trabalho em equipe entre os usuários cadastrados. O administrador de um site é o próprio usuário criador;

r) Para as telas de leitura, criação e edição de mensagens de e-mail, mensagens instantâneas e agenda de compromissos, as interfaces deverão estar disponíveis no idioma Português do Brasil;

s) Para as telas de leitura, criação e edição de mensagens de e-mail, mensagens instantâneas e agenda de compromissos, o acesso deverá ser por meio de interface HTTPS - Hyper Text Transfer Protocol Secure;

t) Os usuários devem ter acesso às funcionalidades com apenas um logon;

u) Deverá existir telas com conteúdo da ajuda para usuários em português;

v) Suporte aos protocolos POP, IMAP;

w) Suporte a dispositivos móveis compatíveis com o ActiveSync;

x) Suporte a SMTPS.

5.3.7.72. **Disponibilização de caixas postais e colaboração - TIPO 2.**

a) Cada usuário cadastrado no sistema com este tipo de licenciamento deverá ter a seu dispor através de navegadores Internet as seguintes funcionalidades:

b) Licença de Comunicação Unificada TIPO 2 com subscrição para 12 meses;

c) Todas as funcionalidades previstas na Licença do TIPO 1;

d) Dispor de recursos avançados de arquivamento e bloqueio legal, combinado com a possibilidade de armazenamento ilimitado para mensagens de correio;

e) Dispor de ferramentas de suporte à conformidade e auditoria, através de pesquisas em sites web e conteúdo de correio eletrônico de qualquer usuário;

f) Dispor de capacidade de correio de voz integrado à plataforma;

g) Capacidade de criação de painéis interativos com conteúdo de várias fontes de dados;

h) Capacidade de armazenamento de mensagens que porventura o usuário apague ou modifique por período ilimitado;

i) Capacidade de proteção de arquivos contra impressão, envio para terceiros e encaminhamento de mensagens;

j) Deve permitir o controle de utilização e distribuição online dos aplicativos do Microsoft Office para até 5 estações de trabalho;

k) Deve permitir a utilização das versões móveis do Office em até 5 telefones Androide ou IPhone;

l) Deve fornecer recursos de DLP (Prevenção de Perda de Dados) como parte da solução de correio eletrônico;

m) A seguir são especificados os requisitos técnicos para o correio eletrônico, componentes da solução:

n) Detectar e remover vírus ou spans em e-mails de entrada e saída de qualquer origem automaticamente.

o) Utilização de recursos especiais (agendamento de salas de reunião ou equipamentos) sem qualquer custo financeiro adicional.

p) O acesso aos serviços deverá ocorrer a partir dos navegadores listados abaixo, preferencialmente, sem a instalação de aplicativos nos dispositivos:

- Mozilla Firefox;
- Google Chrome;
- Opera;
- Microsoft Edge;
- Safari;

q) O acesso aos serviços deverá ser feito sempre através de conexão segura (https). Deverão ser suportadas sempre a versão atual dos browsers e, pelo menos, uma versão anterior.

r) O componente de correio da solução não deverá restringir o envio e o recebimento de anexos inferiores a 20MB (vinte megabytes).

s) Os endereços eletrônicos das contas de e-mail deverão conter obrigatoriamente o domínio do CONTRATANTE (alias@dominio.com.br – ex.: xyz@dominio.com.br).

t) Permitir a abertura simultânea de mais de uma caixa postal pelo mesmo usuário no mesmo computador ou dispositivo móvel.

u) Disponibilizar mecanismos de auditoria que permitam registrar as atividades de acesso à conta, deleção de conteúdo, envio e recebimento de mensagens dos usuários.

v) Todos os registros de auditoria devem permanecer disponíveis ao CONTRATANTE por, pelo menos 7 (sete) dias corridos.

w) Não permitir, sob qualquer hipótese, que os registros de auditoria sejam alterados ou excluídos.

x) O componente de correio da solução deverá propiciar a geração de consultas e relatórios das auditorias, a serem solicitadas apenas por usuários habilitados. Os registros de auditoria poderão, a

cargo do CONTRATANTE, ser exportados para arquivos em formato texto ou “csv”.

y) A CONTRATADA deverá comprovar as políticas de auditorias periódicas permanentes, quando solicitadas pelo CONTRATANTE.

z) O módulo que implementa o serviço de MTA-Mail Transfer Agent deve suportar e ser totalmente aderente às especificações do protocolo SMTP da pilha TCP/IP (RFC 821) e suas atualizações ou correlatos.

aa) O módulo que implementa o serviço de MDA-Mail Delivery Agent deve suportar e ser totalmente aderente às especificações dos protocolos POPv3 e IMAPv4 da pilha TCP/IP (RFC 1939 e 3501 respectivamente) e suas atualizações ou correlatos, pelo menos.

ab) Suportar a utilização de segurança padrão SSL/TLS para todos os protocolos, sem exigir a utilização de VPNs, assegurando desta forma a proteção e o sigilo dos conteúdos transmitidos.

ac) Fornecer de maneira integrada mecanismos de inspeção, filtro e remoção de mensagens indesejadas (spans) ou contaminadas com “malwares”.

ad) O componente de correio da solução deverá possuir servidor de e-mail com ampla capacidade de indexar mensagens, contatos e tarefas para que o usuário consiga obter resultados de pesquisas rapidamente.

ae) Retenção de mensagens/itens apagados por, no mínimo 30 (trinta) dias, com opção de restauração a ser executada pelo próprio usuário.

af) Possuir recurso para notificar falha na entrega de e-mails, fornecendo informações sob o motivo da falha e informações técnicas para diagnóstico do problema pelos administradores.

ag) Permitir restrições no tamanho total de uma mensagem de e-mail, ou nos tamanhos dos componentes individuais da mensagem, como cabeçalho, anexos ou número de destinatários da mensagem, a ser configurado pelo administrador.

ah) Permitir que um usuário do componente de correio da solução tenha 2 (dois) ou mais alias de e-mail.

ai) Suportar o envio de mensagens assinadas e criptografadas digitalmente, via protocolo S/MIME.

aj) Permitir a configuração das caixas de correio para aceitar ou rejeitar e-mails enviados de usuários específicos.

ak) Oferecer a possibilidade de assinar digitalmente as mensagens com certificados digitais ICP Brasil do tipo A3 via soluções de e-mail ou browsers.

al) Permitir a delegação da administração do componente de correio da solução para usuários não administradores do domínio.

am) Suportar criação de listas de distribuição de e-mail dinâmicas.

an) Possuir catálogo de endereços centralizado.

ao) Possuir console de administração centralizada.

ap) Permitir a criação de contatos de e-mails externos no catálogo de endereços.

aq) Incluir ferramentas administrativas que possam ser executadas em browsers e permitir a administração remota do componente de correio da solução.

ar) As conexões ao componente de correio da solução por meio de dispositivos móveis devem ser realizadas, obrigatoriamente, via SSL.

as) Permitir controlar, em níveis amplos e granulares, o que administradores e usuários finais podem fazer.

at) Fornecer aos usuários a possibilidade de delegar acesso de seus recursos a outros usuários, controlando o nível de permissões que será concedido.

au) O componente de correio da solução deverá ter seu ambiente de usuário em idioma

português do Brasil e suportar a acessibilidade no mesmo idioma.

av) Ser acessível através de web browsers e por software proprietário de desktop (MUA – Mail User Agent).

aw) Possuir Webmail acessível através de tablets e smartphones, preservando funcionalidades de acesso compatíveis aos dos browsers.

ax) Permitir o acesso ao correio eletrônico via dispositivos móveis através de interface gráfica, especificamente desenvolvida para tais equipamentos. O componente de correio da solução deve ser compatível, no mínimo, com as seguintes tecnologias: iOS v.5 e Android 4.0.

ay) Oferecer aplicações de gerenciamento de contatos, compromissos (agenda) e tarefas, de maneira individual e compartilhada (colaborativa). Deve ser oferecida a opção de cadastrar lembretes para cada compromisso.

az) Procurar horário livre na agenda de todos os participantes da reunião e com base na pesquisa sugerir horário para a reunião automaticamente.

ba) Enviar e-mail aos participantes da reunião, solicitando confirmação de presença.

bb) Assistente de ausência temporária com encaminhamento automática de e-mail.

bc) Permitir a configuração dos recursos especiais para responderem à solicitação de reserva, possibilitando as seguintes ações: aceitar ou recusar solicitações de reserva automaticamente, selecionar representantes para aceitar ou recusar solicitações de reserva.

bd) Disponibilizar espaço de armazenamento de e-mails de, no mínimo, 50GB (cinquenta gigabytes) por usuário.

be) O fabricante do componente de comunicação colaborativa da solução deverá ser o mesmo do componente de correio da solução, a fim de viabilizar melhor integração entre as plataformas de colaboração e do correio colaborativo, reduzindo os riscos de incompatibilidade ou de descontinuidade das aplicações.

bf) O componente de comunicação colaborativa da solução deverá integrar-se com o webmail, permitindo, pelo menos, a utilização de chat e o status de presença, na mesma interface.

bg) Suportar, pelo menos, a utilização de vídeo em definição padrão (standard definition) no envio de vídeo ponto-a-ponto.

bh) Suportar a exibição simultânea de apresentação colaborativa, videochamada ponto-a-ponto e chat multiponto entre os participantes de uma sessão colaborativa.

bi) Permitir o compartilhamento da tela do usuário apresentador e dos convidados durante uma sessão de colaboração.

bj) Permitir o compartilhamento de uma aplicação do computador do apresentador ou de um convidado durante uma sessão de colaboração.

bk) Permitir a comunicação de áudio ponto-a-ponto durante sessão de colaboração.

bl) Propiciar que o apresentador possa controlar quem são os participantes da reunião, especificando permissões de transmitir conteúdo durante a sessão de colaboração.

bm) Possibilitar a participação em sessões de colaboração para usuários que estejam em locais externos às dependências do CONTRATANTE como convidados. Caso haja necessidade de instalação de software no computador do convidado este deve ser disponibilizado gratuitamente para download.

bn) Propiciar a troca de mensagens instantâneas com múltiplos usuários em uma única sessão.

bo) Fornecer recurso de troca de mensagens instantâneas entre os usuários. Todo o texto transmitido durante a conversação deve ser criptografado.

bp) Permitir o uso de foto pessoal para cada usuário.

bq) Os codecs de áudio e vídeo devem automaticamente se adaptar à velocidade de banda disponível, ou a aplicação deve permitir a marcação de pacotes (QOS) ou deve permitir a restrição de

utilização de banda para um determinado range de IP's.

br) Possuir mecanismos que permitam registrar a comunicação efetuada através da plataforma para posterior rastreabilidade.

bs) Permitir aos usuários armazenar e compartilhar arquivos, documentos, planilhas, apresentações, imagens, em especial nos seguintes formatos:

- Documentos: Microsoft Office Word, BR Office/LibreOffice Writer e PDF.
- Planilhas: Microsoft Office Excel e BR Office/LibreOffice Calc.
- Apresentações: Microsoft Office PowerPoint e BR Office/LibreOffice Impress.
- Imagens: BPM, JPEG, GIF, TIFF e PNG.

bt) Permitir a sincronização automática de arquivos armazenados localmente no computador dos usuários do CONTRATANTE com os arquivos armazenados no componente

bu) Permitir aos usuários controlar as permissões de acessos a suas pastas e arquivos.

bv) Disponibilizar espaço de armazenamento de arquivos de, no mínimo, 5GB (cinco gigabytes), por usuário, em espaço compartilhado, ou não, com os demais componentes da solução em nuvem.

bw) Permitir a criação de documentos de texto, planilhas e apresentações, inclusive com a colaboração em tempo real.

bx) Possibilitar o compartilhamento dos documentos para edição ou somente leitura.

by) Viabilizar a restrição de compartilhamento de arquivos para usuários externos ao ambiente, possibilitando a concessão de acesso somente a usuários internos.

bz) Possibilitar o trabalho offline para sincronização posterior dos arquivos.

ca) Permitir aos usuários a edição on-line de documentos, em navegadores Mozilla Firefox, Google Chrome, Internet Explorer e Safari. Deverão ser suportadas sempre a versão atual dos browsers e pelo menos uma versão anterior.

cb) Disponibilizar mecanismos de auditoria que permitam registrar as atividades de acesso, deleção ou alteração de conteúdo dos usuários

5.4. **Item 04 – SaaS - BUSINESS INTELIGENCE EM CLOUD**

5.4.8. Solução de análise de dados, com licença com subscrição em nuvem que possibilite fazer replicação de dados, criação automatizada de data warehouses e/ou data lakes, a catalogação dos dados, criação de painéis, envio de relatórios e alertas, mapas, publicação de informações em portal da transparência, ambiente de teste, treinamentos e suporte especializado para desenvolvimento, implantação e supervisão da plataforma.

5.4.9. Bens e/ou Serviços

5.4.10. Tabela 1 - Bens e Serviços que Compõem a Solução:

Bens e Serviços que Compõem a Solução			
Item	**Produto**	**Unid.**	**Qtde**
1	Licença sob subscrição, em nuvem que possibilite fazer replicação de dados, criação automatizada de data warehouses e/ou data lakes, a catalogação dos dados, incluindo suporte do fabricante.	Unidade	1
	Licença sob subscrição, em nuvem que possibilite fazer criação de painéis		

2	analíticos, envio de relatórios e alertas, mapas, publicação de portal da transparência e ambiente de teste, incluindo suporte do fabricante.	Unidade	1
3	Treinamento de administração de ambiente, 8 horas (por aluno, turma mínima de 5 pessoas)	Aluno	X
4	Treinamento de desenvolvimento de painéis, 24 horas (por aluno, turma mínima de 5 pessoas)	Aluno	X
5	Serviços técnico especializado para o desenvolvimento, implantação, supervisão de funcionamento na plataforma.	Hora	2000

5.4.10.1. **Sub-Item 4.1 – Serviço de fornecimento de software de analise de dados**

a) **Características gerais que deverão ser aplicadas aos itens 01 e 02**

- Possuir versões para servidor com sistema operacional Windows ou Linux na arquitetura de 64 bits.
- Poder ser instalada e configurada em um provedor de cloud definido pela CONTRATANTE
- Todos os recursos de desenvolvimento e administração devem se providos por uma interface Web em HTML padrão sem a necessidade de instalação de aplicativos ou plugins

b) **Requisitos para replicação de dados**

- Ser capaz de replicar dados near realtime entre plataformas heterogêneas (origem e destino) com mínimo impacto nas origens de dados
- Ser capaz de automaticamente as tabelas na origem de dados e replicar para o destino ajustando os tipos de dados correspondentes entre as origem e destino
- Ser capaz de replicar operações de DML (insert/update/delete) bem como DDL (alteração em tabelas)
- Possuir uma interface web amigável para parametrização das rotinas de replicação
- Possuir uma interface web de administração e acompanhamento das tarefas de replicação
- Possuir uma interface web amigável para parametrização das rotinas de replicação
- Poder se conectar sem instalação de agentes em pelo menos as bases abaixo como destino de dados:

I - Amazon Aurora MySQL / Maria / PostgreSQL

II - Amazon RDS for Oracle

III - Google Cloud SQL for PostgreSQL e MySQL

IV - IBM DB2 for iSeries or z/OS

V - Microsoft SQL Server

VI - MySQL / MariaDB

VII - Oracle 10.3 ou superior

VIII - PostgreSQL

IX - Amazon Redshift

X - SnowFlake

XI - Amazon S3

XII - Amazon EMR

XIII - Google Cloud BigQuery

XIV - Google Cloud Storage

XV - Microsoft Azure SQL Synapse Analytics

XVI - Data Lake Storage Gen2

XVII - Microsoft Azure SQL Database

XVIII - Microsoft Azure Database for MySQL 5.6 and 5.7

XIX - Microsoft Azure Database for PostgreSQL

XX - Microsoft Azure Databricks

XXI - Kafka

XXII - Microsoft Azure Event Hubs

XXIII - Amazon Kinesis Data Streams

XXIV - MapR Streams

5.4.10.2. **Requisitos para criação automatizada de DW/DL**

a) Criar automaticamente as tabelas fato e dimensão segundo as melhores práticas de mercado

b) Criar automaticamente datamarts consolidados baseados nas tabelas fato e dimensão

c) Capaz de importar um modelo de dados do Erwin

d) Capaz de fazer uma descoberta das tabelas de origem que devem popular o DW

e) Retenha logs capazes de verificar a execução das tarefas de extração, tratamento e carga

f) Capaz de criar data warehouses e datamarts em ambientes

- Oracle
- SQL Server
- Amazon Redshift
- Snowflake

g) Capaz de criar datalakes em ambientes

- Hortonworks
- Amazon EMR
- Cloudera
- Microsoft Azure HDInsight
- Google Dataproc
- Databricks

5.4.10.3. **Requisitos para catalogação de dados**

a) Catalogar dados de origens diversas e permitir utilização das mesmas.

b) Suporte para implantação baseada em nuvem ou híbrida, bem como modelos com vários clusters.

c) O produto deve possibilitar fazer gerenciamento de dados de nível corporativo, fazer cumprir e monitorar políticas e uso de dados com segurança robusta, governança, desempenho, interoperabilidade, escalabilidade e confiabilidade.

d) Permitir definir regras de segurança e perfil de usuários para acesso aos dados catalogados.

e) Ter interface totalmente WEB para utilização dos recursos e gestão do ambiente.

f) Possibilitar estruturar, documentar, proteger e gerenciar coleta de dados, garantindo que se tenha uma boa governança além de possuir um repositório de metadados que gerencia e mantém

todos os metadados coletados e gerados ao longo de cada etapa do seu processo de gerenciamento de dados corporativos.

g) Possuir uma estrutura comum de segurança, governança e recursos de metadados para proteger os dados, gerenciar privilégios de acesso do usuário, e acompanhar a atividade dos usuários em todos os momentos.

h) Permitir fazer busca por nome em toda base de dados ou campos catalogados.

i) Possuir informações de data de última atualização, quantidade de registros e campos além de indicadores de qualidade e utilização de cada uma das bases catalogadas

j) Permitir integração, no mínimo com as origens de dados: Arquivos locais, bancos de dados relacionais, XML, JSON, ftp, S3, HDFS, HIVE, Sqoop, KAFKA, ADLS, WASB, conexões JDBC.

k) Possibilitar ofuscar campos, definir especificações de formato de arquivo e definir delimitadores, tipo de arquivo, tipos de carga de dados e mais, com total segurança e controle de dados.

l) Permitir criar fluxos de preparação de dados de forma visual, utilizado recursos de arrastar e soltar para no mínimo recursos como filtros, união entre tabelas, recursos similares ao Join da linguagem SQL, agregações e ordenações

m) Possibilitar renomear os campos ou adicionar nome de campos intuitivos para os usuários de negócios.

n) Permitir catalogar os dados mantendo na origem ou efetuando a cópia do mesmo.

o) Permitir reutilização, colaboração, preservação e catalogação de novos conjuntos de dados à medida que são gerados além de permitir que seus usuários reutilizem recursos criados anteriormente no catálogo de dados disponibilizado.

p) Permitir exportar os dados catalogados para arquivos txt e Parquet.

q) Permitir fazer agendamento de atualização, preparação e publicação dos dados.

r) Permitir que os dados catalogados possam ser exportados para planilhas e para solução de visualização para que possam ser trabalhados.

5.4.10.4. **Características Gerais que deverão ser aplicadas aos usuários e desenvolvedores da solução de criação de painéis analíticos**

a) Possuir versões para servidor com sistema operacional Windows ou Linux na arquitetura de 64 bits.

b) Carregar todos os dados selecionados pelo usuário, em todos os níveis de detalhe possíveis, diretamente na memória RAM do servidor de forma compactada visando à maximização da velocidade de acesso durante a execução das consultas, à minimização do impacto de acesso aos sistemas de disco e à dispensa do uso de banco de dados ou repositório em disco para a execução das consultas.

c) A ferramenta não deve possuir restrições de número de dimensões em um modelo.

d) Não limitar o número de fontes de dados acessadas pela ferramenta nem o relacionamento entre elas.

e) Permitir compactação dos dados, reduzindo os dados de origem para, no máximo, 30% do tamanho original em disco (compactação mínima de 70%).

f) Integrar múltiplas fontes de dados sem necessidade de acesso a módulos adicionais.

g) Possuir as funcionalidades para extração, transformação, carga de dados e desenvolvimento de painéis integradas na mesma solução e com interface única.

h) Possibilitar aos usuários finais conectarem-se aos aplicativos baseados em servidor, com opções de disponibilização via navegador.

i) Ser responsivo de forma que o painel irá se encaixar automaticamente ao tamanho da tela do dispositivo seja ele computador, tablet, smartphone dentre outros. Esse recurso deve ser nativo, sem a

necessidade de criar aplicações diferentes para cada tamanho de tela dos dispositivos e deve não só reduzir ou aumentar os objetos como também reposicionar para melhor visualização e utilização do painel.

j) Possuir todo seu ambiente de desenvolvimento e de uso em português, tanto o conteúdo do que for desenvolvido (painéis de consulta), como também os menus e diálogos da própria ferramenta de desenvolvimento da solução, exceto palavras reservadas de programação.

k) Permitir configuração de cluster e load balance entre produtos servidores adquiridos sem custo adicional com licenças ou funcionalidades para a contratante além dos que estão definidos nesse termo.

l) Prover ajuda on-line, bem como manual de usuário.

m) Prover recursos de escalabilidade horizontal (acréscimo de computador servidor) e escalabilidade vertical (upgrade hardware).

n) A ferramenta deverá permitir que todos os dados extraídos do ambiente transacional fiquem armazenados no próprio servidor da aplicação, sem a necessidade de utilização de servidores de banco de dados adicionais nem de Armazém de Dados – Data Warehouse.

o) Utilizar processamento paralelo (multi-thread) do servidor.

p) Deve permitir que o usuário baixe o painel do servidor e posteriormente utilize a ferramenta off-line, ou seja, sem a necessidade de estar conectado ao servidor.

q) Deve permitir a criação de objetos que não sejam nativos, como também a customização dos objetos nativos nos painéis.

r) **Requisitos de Utilização do Painel:**

s) Permitir fazer filtros, no momento da utilização do painel, através de expressões com operadores do tipo menor que, maior que, menor ou igual, maior ou igual, intervalo de valores, tanto para dimensões de data quanto de conjuntos numéricos.

t) Permitir que valores nas dimensões tipo texto sejam encontrados no documento utilizando-se qualquer parte do texto na pesquisa;

u) Prover ao usuário um mecanismo de filtro através de pesquisa de fragmentos de dados em qualquer dado disponível e mapeado, sendo usado ou não nos objetos disponíveis. A pesquisa deve ter função de auto-completar ou sugerir opções com o fragmento já digitado e, ao selecionar um determinado dado, a seleção deve refletir simultaneamente nas demais dimensões do modelo.

v) Possibilitar que sejam usados expressões e cálculos na definição de filtros.

w) Permitir a utilização de expressões lógicas (maior, menor, igual a, diferente de) para seleção de filtros.

x) Prover funcionalidade de pesquisa que busque, em uma única operação, determinados valores em todos os campos – dimensões, filtros e valores – do documento.

y) Permitir prover pesquisa de fragmentos de textos permitindo que valores nas dimensões tipo texto possam ser encontrados utilizando-se qualquer parte do valor do texto na pesquisa (tipo cláusula like). A pesquisa deve retornar o resultado para qualquer atributo mapeado, indicando o atributo.

z) Permitir verificar informações que tem relação com o filtro e também aquelas que não tem relação.

aa) Permitir o acesso a painéis de informações a partir de dispositivos móveis sem que haja necessidade de desenvolvimento ou custo adicional à contratante.

ab) Reagir automaticamente, sem necessidade de definição prévia de filtros, sempre que o usuário selecionar determinados valores de qualquer dimensão. Tal seleção deve ser propagada nas demais dimensões e métricas do modelo, bem como nos valores calculados, e em todos os painéis do documento, distinguindo os valores relacionados dos não relacionados à seleção de valores do usuário.

ac) Devem possuir uma integração entre os painéis de consulta, de modo que o acionamento de um filtro em um deles interfira automaticamente nos outros que possuam informações relacionadas ao primeiro.

ad) Permitir filtros nas dimensões tipo data (date) por expressão, tais como: cláusula menor, maior que, intervalo de valores.

ae) Permitir que as medidas possuam filtros por expressão, tais como: cláusula menor que, maior que, intervalo de valores.

af) Permitir que o usuário salve um conjunto de filtros mais utilizados, a partir de qualquer dado usado no painel ou dado constante no modelo.

ag) Permitir que os usuários internos e externos possam executar operações de slice and dice sobre os dados, executar operações de pivotagem modificando os eixos e medidas na tabela de forma dinâmica, contrair e expandir linhas e permitir tabelas dinâmicas de tempo (datas), segmentadas pelo menos as seguintes medidas básicas: semanas, meses, trimestres, semestres e anos.

ah) Possuir mecanismo de mudanças de cores e imagens dos objetos em tempo de navegação condicionadas aos dados ou fórmulas.

ai) Possuir assistentes (wizards) para auxiliar no desenvolvimento.

aj) Informar valores e cotas de gráficos e mostradores somente com a passagem do ponteiro do mouse.

ak) Permitir exportar as imagens dos gráficos contidos nos painéis pelo menos nos formatos png e jpeg.

al) Permitir exportar os dados das tabelas dos painéis pelo menos nos formatos PDF, Excel ou imagem.

am) Permitir análise associativa através de navegação e interação com os dados, sem a necessidade de caminhos pré-definidos de análise.

an) Deve efetuar a distribuição de versões de aplicações com dados reduzidos, para os usuários registrados em cada aplicação.

ao) Permitir o acesso a painéis de informações a partir de endereços fornecidos ao browser de internet, bem como que sejam fornecidos parâmetros a esses endereços a fim de filtrar os dados apresentados no respectivo painel de informação segundo os parâmetros informados.

5.4.10.5. **Requisitos de Administração que deverão ser aplicadas aos usuários e desenvolvedores da solução:**

a) Permitir administração do ambiente via browser e através de dispositivos móveis com o recurso de responsividade, tornando as análises totalmente adequadas ao tamanho da tela do dispositivo móvel sem necessidade de acesso ao sistema do servidor da aplicação.

b) Devem possuir indicadores que informem ao administrador se houve alguma falha no processo de ETL e se os dados disponibilizados se encontram íntegros.

c) Oferece distribuição das licenças de forma flexível, como também permitir o monitoramento.

d) Possuir painel para que o administrador possa fazer liberação de acessos, aplicações ou agendamentos de cargas quando necessário.

e) Possuir painel de monitoramento de usuário, aplicação e servidor.

f) A ferramenta deve permitir que seja realizado de uma forma centralizada a análise e controle de toda a instalação e ambiente de desenvolvimento e produção, para, por meio de alertas, identificar onde e quais são os itens que precisam ser corrigidos.

g) Fornecer e gerenciar integração com o Microsoft Active Directory e LDAP, associando nomes de usuário a seus grupos e permitindo a atribuição das tarefas e configuração de permissões a usuários específicos.

h) Permitir agendamento dos processos de atualização de dados, configurar periodicidade, criar processos encadeados que dependam de outro processo para iniciar.

i) Permitir que os agendamentos dos processos de atualização de dados possam ser executados manualmente a qualquer momento.

5.4.10.6. **Requisitos de Segurança, Auditoria e Restrição de Dados que deverão ser aplicadas aos usuários e desenvolvedores da solução:**

a) Permitir a segurança dos dados armazenadas na aplicação, exigindo autenticação com o Active Directory (AD).

b) Permitir restringir visualização de dados por usuário, grupo e/ou perfil a partir de um ou mais campos (colunas) ou registros (linhas.

c) Permitir canais seguros de comunicação (criptografia) entre dispositivos da CONTRATANTE e os servidores de aplicação, servidores de banco de dados ou outros servidores que fazem parte da solução.

d) Permitir a criação de usuários específicos para administração do sistema.

e) Prover o registro da data e horário do acesso, de documentos acessados, do tempo de conexão, do IP, de origem, do usuário de rede, do nome do computador, assim como informações de trilha de auditoria de acesso.

f) A ferramenta deve oferecer análises estatísticas do uso do ambiente e de cada uma das aplicações, nós de servidores, tarefas, sessões e permitir que as atividades e seleções de cada usuário possam ser rastreadas.

g) A ferramenta deve oferecer análises estatísticas do uso do servidor, informando os erros e alertas ocorridos, assim como os eventos de log. Deverá também fornecer um relatório do uso da memória nas últimas 24 horas, além de um relatório do uso máximo de

h) memória por dia, assim como informar quais aplicações estão carregadas na memória num dado momento à escolha do usuário.

i) A ferramenta deve oferecer uma análise estatística das sessões de acesso ao ambiente e às aplicações contendo o número de sessões por hora do dia, assim como os detalhes de log de atividade. Tudo isso deve ser apresentado de forma gráfica, permitindo ao usuário auditor interagir com os dados para permitir a tomada de decisões.

j) A ferramenta deve oferecer uma análise estatística de cada um dos usuários e o seu uso do ambiente a das aplicações. Deverá oferecer para cada nó de servidor informação referente à atividade (sessões, usuários e seleções). Para cada documento/aplicação deverá permitir e oferecer estatísticas das ações dos usuários, das suas seleções, da duração das sessões de acesso e do número de usuários.

k) A ferramenta deve permitir que a frequência de utilização da aplicação seja rastreada, gerando estatísticas de sua utilização na forma de painéis gráficos de análise.

l) Possibilitar a geração de arquivos de log’s em formato TXT para que possam ser utilizados por outras ferramentas caso necessário.

m) Permitir a criação de regras de segurança para habilitar ou proibir que usuários tenham acesso a recursos da solução de acordo com perfil do usuário.

5.4.10.7. **Licenças de uso de software para quantidade ilimitada de usuários com permissão de criação ou visualização de quantidade ilimitada de aplicações de análise estratégica e gerencial e publicação em portal da transparência.**

a) A limitação da quantidade de usuários deverá ser apenas pela capacidade de processamento do servidor.

b) Toda instalação deverá ser feita em ambiente na nuvem indicada pelo IGES, onde ela consiga monitorar todo ambiente e recurso disponibilizados além de garantir o não compartilhamento de recursos contratados.

c) Deve permitir a inclusão de objetos dos painéis em páginas Web de forma que os filtros nas dimensões funcionem de forma nativa;

d) Deve permitir a criação de funções/métodos utilizando um protocolo específico, vinculado a qualquer linguagem de programação, que retornem mensagem com metadados dos painéis dos usuários.

e) Possuir interface 100% Web para visualização e manutenção das aplicações.

f) Possuir funcionalidade de geração automática de modelo de dados, definindo relacionamentos entre fontes de dados tabulares a partir da similaridade de conteúdo dos registros e nome das colunas dessas fontes.

g) Permitir a construção de mashups, que são a combinação de objetos visuais web gerados pela ferramenta com outros objetos visuais web gerados fora dela, compondo assim uma página web heterogênea na origem do conteúdo, mas homogênea na apresentação para o usuário final.

h) Permitir que os objetos gráficos do painel da solução possam ser publicados em páginas web customizadas. Esses objetos podem ser publicados separadamente ou em sua totalidade e também deve possibilitar que objetos de um ou mais painéis ou aplicações diferentes sejam publicados em uma mesma página.

i) Deverá permitir acesso de usuários anônimos, ilimitados aos painéis de acordo com a capacidade de processamento do servidor.

j) A solução não deverá possuir limitação técnica para o crescimento do número de usuários.

5.4.10.8. **Requisitos de Relatórios:**

a) Deverá prover a distribuição de relatórios criados na ferramenta para os usuários.

b) O servidor de relatórios poderá ser instalado em um servidor diferente com objetivo de evitar a concorrência de recursos de hardware entre as aplicações, sem restrição de número de usuários, painéis ou relatórios por painéis que irão utilizar esses recursos.

c) Deverá rodar em sistema operacional Linux ou Windows, plataforma 64 bits, utilizando, no mínimo, 8 núcleos de processamento físicos ou virtuais e toda memória disponível no servidor.

d) Deve permitir a distribuição efetuada de forma automatizada por e-mail.

e) Deve permitir a distribuição de um número ilimitado de relatórios para um número ilimitado de usuários (N relatórios x N usuários).

f) Deve permitir criar relatórios para serem gerados, pelo menos, nos formatos PDF, CSV, DOC, DOCX, PPT, PPTX, XLS, XLSX, JPG, JPEG, PNG e HTML.

g) Deve permitir, para os relatórios que forem desenvolvidos em formato da plataforma Microsoft Office® (Word, Excel e PowerPoint), que seja possível realizar todas as formatações disponíveis na respectiva ferramenta (Word, Excel e PowerPoint).

h) Deve permitir a criação e reutilização de templates nos relatórios.

i) Deve permitir utilizar um ou mais painéis como fonte de dados para confecção de relatórios.

j) Deve permitir utilizar todos os campos existentes nos painéis para a confecção dos relatórios.

k) Deve permitir criar condições de exibição para partes de um determinado relatório somente sejam exibidas se as condições definidas forem atendidas.

l) Deve permitir a criação de filtros para serem utilizados em mais de um relatório.

m) Deve permitir a criação de relatório com redução de dados, ou seja, gerar e enviar um relatório com apenas um subconjunto de informações.

n) Deve permitir a criação de tarefas relacionadas à execução dos relatórios com, no mínimo, as seguintes funcionalidades:

- Tarefa de execução de envio relatório.
- Tarefa de redução de dados.
- Tarefa de importação de contatos.

o) Deve permitir a criação de agendamentos para as tarefas. Estes agendamentos devem permitir a execução das tarefas com, no mínimo, as seguintes periodicidades:

- Execução única.
- Execução diária.
- Execução semanal.
- Execução mensal.
- Execução anual.

p) Deve permitir definição de hora, minuto e segundo exato da execução dos agendamentos.

q) Deve permitir o cadastramento de contatos para o envio programado de relatórios.

r) Deve permitir o cadastramento de grupo de contatos para o envio em lote de relatórios.

5.4.10.9. **Utilização e integração de serviços de mapas.**

a) Prover recursos de georreferenciamento totalmente integrados a solução e do mesmo fabricante.

b) Os mapas poderão ser utilizados de forma ilimitada em todos os painéis desenvolvidos.

c) O servidor de mapa poderá ser instalado em um servidor diferente com objetivo de evitar a concorrência de recursos de hardware entre as aplicações, sem restrição de número de usuários, painéis ou mapas por painéis que irão utilizar esses recursos.

d) Deverá rodar em sistema operacional Linux ou Windows, plataforma 64 bits, utilizando, no mínimo, 8 núcleos de processamento físicos ou virtuais e toda memória disponível no servidor.

e) Possibilitar que dados e informações geográficas carregados e utilizados nos painéis possam ser utilizados também em mapas.

f) A plataforma de mapas deve fazer parte do licenciamento, sem custo adicional.

g) Possibilitar importar dados georreferenciados dos arquivos tipo KML, GML, Shapefiles, GeoJSON, ESRI JSON, AutoCAD DXF e WFS.

h) Possibilitar a criação de uma ou mais camadas de informação em um mesmo mapa sendo que essa camada pode ser uma área, um ponto, mapa de calor, ligação entre pontos ou mesmo gráficos de barra ou pizza que poderão alterar a cor de acordo com alguma métrica definida.

i) Possibilitar em camadas de ligação entre dois pontos incluir setas para deixar claro o de origem é o de destino.

j) Prover recursos para adicionar uma imagem sobre o mapa em determinado ponto georreferenciado.

k) Incorporar nativamente recursos de apresentação de informações em mapas georreferenciados para as informações de medidas e dimensões. Deve ser possível preencher polígonos definidos no mapa de acordo com o valor de variáveis presentes na análise. Também deve ser possível a inclusão de marcadores cuja posição, cor, tamanho e forma sejam determinados por variáveis presentes na análise.

l) O usuário deve ser capaz de adicionar serviços de mapas disponíveis na Internet compatíveis com a estrutura WMS (Web Map Service), permitindo criar análises de diferentes pontos de vista

incluindo as capacidades providas por um fornecedor de mapa externo, a critério do usuário.

m) Ao desenvolvedor deve ser facultada a opção de personalizar os mapas geográficos a partir de informações dos polígonos disponíveis em uma fonte de dados, tornando possível realizar mapas de preenchimento a partir dos agrupamentos que se fizerem coerentes para a análise das informações. Desta maneira, o usuário poderá ser capaz de criar seus próprios conjuntos de áreas preenchidas sobre o mapa, estabelecendo os polígonos que representarem as áreas pretendidas.

n) Possibilitar que filtros efetuados em áreas ou pontos dos mapas reflitam automaticamente nos demais objetos dos painéis que tem relação com a seleção.

o) Prover recursos de visualizar ou ocultar uma camada de informação em um mapa.

p) Apresentar os valores da métrica utilizada no mapa ao passar o mouse sobre o ponto, área ou gráfico.

q) Possibilidade de fazer filtro de uma ou mais áreas ou pontos no mapa circulando a região desejada.

r) Possibilidade de fazer drill down em uma área, que quando selecionada será dividida em áreas menores conforme a necessidade.

s) Ser capaz de acessar e/ou consultar mapas de forma nativa e/ou através de APIs com precisão a nível de ruas.

t) Os mapas preparados pelos usuários no decorrer da análise dos dados devem ser interativos, permitindo operações de ampliação e redução (zoom), rolagem horizontal e vertical, seleção de polígonos ou marcadores para ativar filtros ou operações de drill na análise ou painel sendo visualizado.

u) Permitir integração para carregar dados geográficos a partir do ESRI Shape e ESRI JSON, AutoCad ou outro banco de dados, com a capacidade de ler, extrair e transformar dados via GeoJSON, GML, KML, WMS, WFS ou TMS.

v) Prover flexibilidade na utilização dos dados georreferenciados, podendo ser hospedados internamente na infraestrutura local, na nuvem dentro da infraestrutura do fabricante ou combinando as duas possibilidades.

w) Permitir múltiplas camadas, onde o usuário final consiga habilitar e desabilitar estas em tempo de visualização.

x) Permitir identificar a localização do ponto georreferenciado por meio de seu nome geográfico, mesmo que este não tenha identificação de coordenadas, e caso exista repetição da localização por este nome, permitir então que o usuário possa definir as configurações especificas que o unifique.

y) Prover objetos de dashboard baseado em mapa com indicadores de Bolha, Linha, Área, Pizza, Barra e Calor.

z) Permitir plotar uma medida de cálculo sobre o indicador de mapa.

aa) Prover navegação de filtros direto no objeto gráfico de mapa, inclusive com possibilidade de atender a uma hierarquia de seleções (drill down) a partir da área georreferenciada de forma totalmente customizada, sem a necessidade de respeitar definições prévias de ordem de filtro hierárquico.

ab) Permitir colorir o indicador de forma flexível a partir de uma dimensão ou medida de análise.

ac) Permitir a utilização de imagem ou símbolo nas extensões .jpg, .png e .svn para exibir nos pontos do mapa em substituição a imagem padrão da bolha.

ad) As métricas que definem as regras de negócio devem garantir fácil identificação analítica de seu conteúdo a partir de controle de cores, tamanho e largura de linhas.

ae) Permitir a plotagem de Pontos e Áreas não só de mapas geográficos, mas também de outras divisões administrativas, tais como: aeroportos, shoppings, hipermercados e outros que possam carregar suas plantas baixas.

af) Permitir a exibição de po-pups de informações dos dados visualizados que podem ser customizados, inclusive com opção de incluir um link de endereço eletrônico.

ag) Prover escolha de temas para o mapa de fundo do objeto, com diferentes estilos e cores, com recurso de zoom do maior nível do mundo até o menor nível da rua.

ah) Permitir controle de zoom em qualquer escala, sem nível pré-definidos e posicionamento do objeto gráfico.

ai) Permitir livre escolha de filtro do usuário, por clique sobre a posição georreferenciada, por seleção unitária ou múltipla por meio de desenho com o cursor do mouse nos pontos de interesse a ser selecionado ou mesmo por seleções feitas em outros campos do aplicativo e que sejam aplicados sobre os dados do mapa.

aj) Prover que o acesso do usuário possa ser feito de qualquer dispositivo, tais como Deskopt, laptop, tablet ou smartphone e que o mapa fique adequado as limitações de definição da tela automaticamente, sem a necessidade de instalar recursos adicionais.

ak) Permitir que seleções feitas no mapa, reflitam nas demais análises da plataforma.

al) Permitir que qualquer interação em qualquer objeto da plataforma reflita na análise georreferenciada.

am) Permitir que as funcionalidades georreferenciada esteja disponível a todos usuários da plataforma.

an) A ferramenta de georreferenciamento deve respeitar as regras estabelecidas na plataforma para nível de acesso aos dados conforme perfil do usuário.

5.4.10.10. **Requisitos de alertas**

a) A solução deverá oferecer aos usuários a capacidade de se cadastrarem para receber alertas sobre valores de indicadores.

b) Esses alertas devem ser enviados pela solução via SMS, e-mail ou outros meios de comunicação.

c) O usuário poderá informar os limites dos valores do indicador que deve ser avaliado para envio do alerta.

d) A solução deve oferecer a possibilidade do usuário optar por receber apenas um resumo geral de todos os alertas, diminuindo assim a quantidade de mensagens recebidas.

e) A solução deverá possuir uma console centralizada onde o usuário possa ver os seus alarmes cadastrados com a opção de remover ou alterar estes alarmes.

f) A solução deverá possuir uma console centralizada onde o administrador possa ver todos os alarmes cadastrados com a opção de remover ou alterar estes alarmes

5.4.10.11. **Requisitos de ambiente de teste ou homologação**

a) Esse ambiente deverá espelhar as características de desenvolvimento de painéis do ambiente de produção, contemplando todos os recursos de administração e utilização dos usuários.

b) Deve possuir a capacidade de limitar acesso aos usuários, de forma que apenas aqueles que estão autorizados nesses ambientes possam fazer testes/homologação, mesmo que esses usuários tenham acesso ao ambiente de produção.

c) Não poderá compartilhar recursos do ambiente de produção, podendo ser instalado em outros servidores físicos ou virtuais.

d) Deverá funcionar de forma independente do servidor de produção, inclusive com versões diferentes para teste do ambiente e impacto de versões antes de serem aplicadas ao servidor de produção.

5.4.11. **Sub-Item 4.2 - Treinamentos direcionados de BI**

5.4.11.12. Todos os treinamentos oficiais do fabricante ou distribuidor deverá ser prestado nas dependências do contratante (in company), de forma presencial em endereço informado previamente.

5.4.11.13. As salas, computadores dos alunos, projetores, internet e demais recursos necessários para realização do curso serão de responsabilidade do contratante.

5.4.11.14. Todo material do curso, apostilas, pen drives, arquivos de instalação, pastas, dentre outros serão de responsabilidade da contratada.

5.4.11.15. Para realização dos cursos a turma deverá ter entre 5 a 10 pessoas com carga horária definidas em cada um dos treinamentos. Essa quantidade pode ser alterada havendo consenso entre contratante e contratada previamente.

5.4.11.16. Os profissionais da contratada deverão ser certificados pelo fabricante nos respectivos treinamentos a serem ministrados.

5.4.11.17. Os treinamentos poderão ser ministrados durante a semana, em dias úteis, de segunda a sexta, de 08:00h as 18:00h de acordo com disponibilidade da CONTRATANTE não podendo ter turnos menores que 4 horas por dia.

5.4.11.18. Treinamento de administração de ambiente.

- Treinamento de usuários de infraestrutura com duração mínima de 8 horas.
- Conteúdo programático mínimo:
    - Instalação e configuração do ambiente
    - Navegação no ambiente.
    - Agendamento de processos de carga.
    - Liberação e configuração de perfil de acessos.
    - Monitoramento do ambiente.
    - Verificação de logs.
    - Melhores práticas.
    - Implantação de painéis em produção.

5.4.11.19. Treinamento de desenvolvedores da solução

5.4.11.20. Treinamento para usuário avançados e analistas desenvolvedores com duração mínima de 24 horas.

5.4.11.21. Conteúdo programático mínimo:

- Configuração de ambiente.
- Navegação no ambiente.
- Criação de novos painéis e manutenção de existentes.
- Carga de dados de diferentes origens.
- Criação e manutenção de processos de carga.
- Criação de gráficos tais como gráfico de pizza, barras, linhas, dispersão, gauges, mapas, tabelas, dentre outros que a solução fornecer.
- Melhores práticas.
- Controle de acesso de usuários.

5.4.12. **Sub-Item 4.3 – Serviços Especializados em Business Intelligence (BI).**

5.4.12.22. **Requisitos para os Serviços técnico especializado para o desenvolvimento, implantação, supervisão de funcionamento na plataforma.**

a) Contratação de Serviços Técnicos Especializados para desenvolvimento, implantação, supervisão de funcionamento na plataforma solução.

b) A CONTRATADA deverá atender à solicitação de Horas de Serviços Técnicos Especializados, conforme demandado pela CONTRATANTE, por meio de Ordens de Serviço (OS's), contemplando um total de até 2.000 (duas mil) Horas de Serviços Técnicos Especializados.

c) Estes serviços estarão relacionados/referenciados a utilização de licenças dos softwares em ambientes e estações de trabalho indicadas pela CONTRATANTE. Estas Horas de Serviços Técnicos Especializados deverão ser executado-apropriadas conforme demanda da CONTRATANTE, sem obrigação de contratação de todo o quantitativo durante a vigência do Contrato. As Horas de Serviços Técnicos Especializados requisitadas acima deverão ser dimensionadas/distribuídas, na forma de Horas pela CONTRATADA, conforme as caracterizações apresentadas a seguir.

d) Serviços Técnicos Especializados para desenvolvimento de Analytics:

e) A CONTRATADA deverá prestar Horas de Serviços Técnicos Especializados para desenvolvimento de painéis, interfaces de análise e outros itens que forem necessários para manutenção e desenvolvimento de painéis de gestão e indicadores;

f) Serviços Técnicos Especializados para orientação/explanação dos usuários finais nas novas funcionalidades disponibilizadas pelos novos painéis, incluindo as inovações existentes na ferramenta, como também a possibilidade de criação facilitada de novos painéis utilizando-se para isso Dimensões e Medidas padronizadas.

g) Serviços Técnicos Especializados para Instalação/Configuração.

h) Serviços Técnicos Especializados, com Monitoração e Validação, para a configuração dos parâmetros de segurança de acesso, notadamente a integração com os Administradores de Diretórios (Microsoft Active Directory ou outra ferramenta padrão LDAP) existentes, além do acesso seguro via protocolo “https”;

i) Serviços Técnicos Especializados, com Monitoração e Validação, para a configuração dos clusters de servidores, caso estes existam ou venham a ser implantados pela CONTRATANTE, inclusive com recursos de replicação automática do repositório de metadados;

j) Todos estes Serviços Técnicos Especializados deverão ser executados, apropriados e faturados de forma mensal, ou seja, por Horas demandadas e executadas em cada período mensal de vigência do respectivo contrato.

k) Nos casos em que o catálogo de serviços não ofereça estimativa que possa ser utilizada na medição de esforço requerido por determinado projeto, o **IGESDF** e a CONTRATADA buscarão o consenso, utilizando os seguintes critérios, sucessivamente:

- Analogia com outros itens do catálogo.
- A critério do **IGESDF**, será realizada aferição empírica da dimensão do escopo por meio de projeto piloto de reduzida duração, com acompanhamento em tempo integral, por gestor técnico da CONTRATANTE, do trabalho da CONTRATADA;
- O resultado advindo do processo acima poderá, a critério do **IGESDF**, ser incorporado ao catálogo de serviço para utilização em demandas futuras.
- O **IGESDF** é o responsável final por definir o tamanho da dimensão em Horas. As justificativas da CONTRATADA deverão ser consideradas e respondidas, ainda que não acatadas.

l) Todos os serviços técnicos deverão ser executados por profissionais certificados pelo fabricante.

m) A Contratada deverá garantir o sigilo absoluto das informações que eventualmente irá manipular durante a prestação do serviço especializado, mediante assinatura de Acordo de Confidencialidade quando do início das atividades.

n) Todos os serviços poderão ser executados nas dependências da contratante ou de forma remota a depender da necessidade do projeto e acordo prévio entre as partes.

o) O atendimento será realizado em dias úteis (7 x 5), em horário comercial (das 8:00 às 18:00 horas).

p) Para atendimento, a contratada deve alocar profissionais compatíveis com a complexidade e especificidade da demanda apresentada.

q) A contratante avaliará a proposta de atendimento do chamado e poderá solicitar adequações

nos itens que considerar inapropriados ou julgar estarem em desacordo com a solicitação.

r) A execução do serviço somente poderá ser iniciada pela contratada após aprovação e autorização da ordem de serviço.

s) Tabela de Horas de Serviços Técnicos Especializados.

Nº Ordem	Complexidade	Descrição das Atividades	Produto	Horas de Esforço
1	**Baixa**	Criar conexões a fontes de dados /conexão;	conexão	1
2		Criar conexões a fontes de dados de arquivos texto	conexão	1
		Estruturados/conexão;		
3		Criar conexões a fontes de dados de arquivos	conexão	1
		XML/conexão;		
4		Criar conexões a fontes de dados (csv, xls, xlsx, etc) existentes em páginas da	conexão	1
		internet/conexão;		
5		Download das mídias/conexão;	conexão	1
6		Importar Extensões da solução de BI	conexão	1
7		Criação de fluxo de trabalho (Stream)	conexão	1
8		Criar conexões a bancos de dados padrão ODBC ou OLE DB/conexão;	conexão	1
9		Criação de contas adicionais de Serviço/licença	licença	2
10		Reinstalação .Net ramework/licença;	licença	2
11		Implementar correções de Painéis de Análise Genéricos com as Dimensões e Medidas de uma Tabela de Fatos identificadas na fase de homologação ou implantação /objeto (gráficos, tabelas, mapas, etc);	objeto (gráficos, tabelas, mapas, etc)	2

12		Implementar Correções de Dashboards específicos com predominância de mostradores identificadas na fase de homologação ou implantação/objeto;	objeto (gráficos, tabelas, mapas, etc)	2
13		Implementar Correções de Painel de Relatório onde o usuário possa escolher as Dimensões e Medidas numa Tabela identificadas na fase de homologação ou implantação/objeto;	objeto (gráficos, tabelas, mapas, etc)	2
14		Implementar Correções de Painel de EIS com botões e comportamento específico conforme caso de uso predeterminado, identificadas no período de homologação ou implantação/objeto;	objeto (gráficos, tabelas, mapas, etc)	2
15	**Média**	Entrevistar usuários e equipe de TI (até 2hs) para mapear o modelo de dados com as tabelas que formam os indicadores chave de performance/por entrevista;	Entrevista	2
16		Entrevistar usuários (até 2hs) para definição de templates WEB	Entrevista	2
17		Exploração de oportunidades de uso da solução/painel (.qvf);	painel (.qvf)	2
18		Orientações equipe interna (hands on)/demanda;	demanda	2
19		Desenvolver Painel de Relatório onde o usuário possa escolher as Dimensões e Medidas numa Tabela /Dimensões ou Medidas;	Dimensões/Medidas	2
20		Customização da solução ou criação de relatórios e visões de informação /Relatórios ou Visões;	Relatórios/Visões	2
21		Dimensionar infraestrutura de hardware e software /demanda;	demanda	2
22		Configuração de Backup /servidor;	servidor	6
		Incluir e configurar contadores de		

23		sistema operacional de performance /servidor;	servidor	6
24		Analisar e documentar indicadores de performance /servidor;	servidor	6
25		Realizar diagnóstico de performance por painel (.qvf);	painel (.qvf)	6
26		Criação documentação final/painel (.qvf);	painel (.qvf)	6
27		Desenvolver rotinas de ETL para os indicadores chave de performance/painel (.qvf);	painel (.qvf)	6
28	**Mediana**	Desenvolver Painéis de Análise customizados para mostrar os indicadores chave de performance/painel (.qvf);	painel (.qvf)	6
29		Configurar controle de acesso à objetos, campos e registros conforme as definições de segurança/painel (.qvf);	painel (.qvf)	6
30		Desenvolver rotinas de ETL para Validação Automática dos Dados carregados/Rotina	Rotina	6
31		Configurar Jobs Automatizados de Carga de Dados no Publisher/demanda;	demanda	6
32		Desenvolver Dashboards específicos com predominância de mostradores/Dashboards;	Dashboards	6
33		Criar Templates de Design de aplicações e Orientações Base para aplicações/template;	template	6
34		Operação assistida à servidores da contratante/demanda;	demanda	6
35		Realizar transferência de tecnologia dos projetos para a equipe técnica da CONTRATANTE /painel (.qvf);	painel (.qvf)	8
		Realizar treinamento para (até 5		

36	**Alta**	usuários) os usuários finais no uso das aplicações desenvolvidas /painel (.qvf);	painel (.qvf)	8
37		Desenvolver rotinas de ETL para a interligação através de LinkTable/painel (.qvf);	painel (.qvf)	8
38		Apoio técnico no uso de funcionalidades novas ou avançadas da solução de BI//painel (.qvf);	painel (.qvf)	8
39	**Especialista**	Instalação e alocação das licenças/servidor;	servidor	10
40		Configurações avançadas solução de BI/Servidor;	servidor	10
41		Criação tarefas de recarga /Servidor;	servidor	10
42		Configuração de acesso aos repositórios de usuários	servidor	10
43		Configuração de autorização de usuário com WEBTICKET	servidor	10
44		Configurar certificado digital no ambiente / servidor	servidor	10
45		Implementação de redução de dados (Section Access)	painel (.qvf)	10
46		Interno/Externo/Servidor;	servidor	10
47		Testes de carga Externo Interno/Externo/Servidor;	servidor	10
48		Mapear modelo de dados dos sistemas transacionais fontes de dados identificando Fatos e Dimensões/painel (.qvf)	painel (.qvf)	10
49		Entrevistar usuários e equipe de TI para mapear o modelo de dados com as tabelas que formam os indicadores chave de performance/Entrevista;	Entrevista	10
50		Desenvolver Extensões com novos objetos para serem utilizadas em aplicações na plataforma /painel (.qvf);	painel (.qvf)	10

51		Executar avaliação de garantia de qualidade quanto ao uso de melhores práticas no modelo de dados da aplicação /painel (.qvf);	painel (.qvf)	10
52		Executar avaliação de garantia de qualidade quanto ao uso de melhores práticas nos scripts da aplicação /painel (.qvf);	painel (.qvf)	10
53		Configuração da solução em momento posterior à implantação, inclusive para melhoria de performance da ferramenta; (Tunning)/painel (.qvf);	painel (.qvf)	10
54		Desenvolver Scripts Java, css, .net para Web templates	Página Web	10
55		Desenvolver templates Web para incorporar objetos BI em soluções de portais	Página Web	10

5.5. **Item 05 –SERVIÇOS ESPECIALIZADOS**

5.5.13. **CARACTERÍSTICAS GERAIS:**

5.5.13.1. Os serviços de serão prestados no ambiente da CONTRATANTE;

5.5.13.2. A CONTRATADA deverá prover os serviços de acordo com as especificações que seguem a cada serviço específico.

5.5.13.3. **SOLICITAÇÃO DOS SERVIÇOS**

- As ações serão executadas a partir da emissão de Ordem de Serviço que deverá ser aceita em comum acordo entre CONTRATANTE e CONTRATADA;
- A CONTRATANTE enviará a Ordem de Serviço à CONTRATANTE com descrição das atividades a serem realizadas e o prazo desejado para término das atividades;
- A CONTRATADA terá o prazo de 24 horas para revisar a Ordem de Serviço, propor sugestões de mudança e dar o aceite na O.S.;
- Todos ajustes na Ordem de Serviço devem ser realizados no prazo citado acima;
- A CONTRATADA poderá solicitar extensão no prazo de revisão e aceite da Ordem de Serviço que será avaliada pelo COTRATANTE;
- Caberá ao unicamente CONTRATANTE aceitar ou não a extensão de prazo;

5.5.13.4. **Sub-Item 5.1 - Serviços de Monitoramento de infraestrutura IaaS**

a) Ao contratar o serviço, por intermédio de emissão de Ordem de Serviço, a CONTRATANTE irá demandar, no mínimo, 12 (doze) meses de execução.

b) A CONTRATADA deverá monitorar toda a infraestrutura disponibilizada em nuvem em regime de 24x7x365;

c) A CONTRATADA deverá disponibilizar Central de Serviços para registro e acompanhamento dos chamados técnicos da CONTRATANTE;

d) O monitoramento deve ocorrer nas instalações da CONTRATADA através de interface WEB a ser disponibilizada pela CONTRATANTE.;

e) A CONTRATADA deverá tratar todos os eventos da infraestrutura e identificar quais eventos são incidentes;

f) A equipe de monitoramento irá executar procedimentos operacionais indicados pela CONTRATANTE visando a resolução de incidentes;

g) A equipe de monitoramento deverá abrir chamados para todos incidentes e indicar a resolução adotada em cada chamado;

h) 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;

i) A CONTRATANTE irá indicar quais são os caminhos para escalonamento dos chamados.

5.5.13.5. **Sub-Item 5.2 – Serviços Especializados em IaaS**

a) Os serviços de especializados em IaaS serão demandados para a realização de todas as atividades referentes a disponibilização de serviços na nuvem contratada;

b) Serão incluídos nesse serviço as seguintes atividades:

- Planejamento de migração de servidores e/ou serviços e/ou dados para a nuvem pública;
- Preparação do ambiente da nuvem pública para receber servidores e/ou serviços e/ou dados da CONTRATANTE;
- Instalação, configuração e suporte técnico de ferramenta(s) para orquestração dos serviços entre as nuvens privada e pública;
- Serviços sobre o uso dos recursos da nuvem privada;
- Serviços de tunning, ajustes, correção de falhas, detecção de problemas na infraestrutura de nuvem pública;

5.5.13.6. **NÍVEIS DE SERVIÇO PARA SERVIÇOS ESPECIALIZADOS EM IAAS**

a) A contratada deve prestar um serviço de qualidade. Para tanto, são estabelecidas nesse termo de referência metas para os serviços prestados. Os serviços serão medidos com base em indicadores de níveis de serviço específicos.

b) A apuração dos indicadores relativos ao tempo de atendimento das Ordens de Serviços será calculada sempre com base na data e hora de registro inicial e final da O.S. No cálculo serão desconsiderados os períodos em que as Ordens de Serviço estiveram suspensas ou não estiveram sob a responsabilidade da contratada.

c) 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.

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

e) 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.

f) Tabela de níveis de serviço

Indicadores de níveis de serviço/mês	Unidade de medida	Meta exigida	Glosa aplicável

Revisão e aceite de nova Ordem de Serviço	Horas	24h após solicitação formal	0,0% + (0,1% para cada 24 horas acima do prazo negociado).
Resolução de Ordem de serviço.	Prazo negociado (1)		0,1% + (0,1% para cada 4 dias acima do prazo negociado).
Para cada Ordem de Serviço será negociado o prazo de entrega de acordo com a complexidade da solicitação			

5.5.13.7. **SERVIÇOS ESPECIALIZADOS EM IaaS:**

a) Os serviços especializados em IaaS serão demandados para a realização de todas as atividades referentes a disponibilização de serviços na nuvem contratada;

b) Serão incluídos nesse serviço as seguintes atividades:

- Planejamento de migração de servidores e/ou serviços e/ou dados para a nuvem pública;
- Preparação do ambiente da nuvem pública para receber servidores e/ou serviços e/ou dados da CONTRATANTE;
- Instalação, configuração e suporte técnico de ferramenta(s) para orquestração dos serviços entre as nuvens privada e pública;
- Serviços sobre o uso dos recursos da nuvem privada;
- Serviços de tunning, ajustes, correção de falhas, detecção de problemas na infraestrutura de nuvem pública;

5.5.13.8. **Sub-Item 5.3 – Serviços de Plataforma integrada (Managed Security Services)**

a) A CONTRATANTE já possui em seu roll de soluções, solução de proteção contra ameaças internas e auditoria para ambiente computacional não estruturado **(VARONIS)**. Devido a necessidade de se ter o mesmo nível de monitoramento e segurança para os dados estruturados, se faz necessário que a CONTRATADA forneça uma plataforma de serviços gerenciados de Monitoramento de Segurança e detecção de ameaças que deva ser capaz de receber dados não estruturados fornecidos pela solução já existente **(VARONIS)** na CONTRATANTE.

b) O fornecedor deve enviar dados de eventos das fontes / dispositivos do **IGESDF** para uma plataforma SOC gerenciada para coleta, mapeamento, armazenamento e relatório (especifica para informações de dados estruturados).

c) **Fontes de infraestrutura de segurança da informação:**

- **Router**
- **Switches**
- **Firewalls**
- **Proxies**
- **IDS/IPS**
- **Network Access Control**
- **Web Application Firewall**
- **Filtros de conteudos.**
- **Balanceadores de carga**
- **Antivirus/Antispam**
- **Servidores**
- **Estações de Trabalho**
- **Sistemas de armazenamento**
- **Antivirus de sistemas**
- **Antivirus/Antispam de correio**
- **Gestão de identidade**

- **Gestão de logs**
- **Gestão de vulnerabilidades**

d) O provedor deve oferecer serviços gerenciados de monitoramento e detecção de ameaças, considerando os locais Cloud e on-premisses.

c) O **IGESDF**contratará os serviços sempre mencionando os locais de coletas de logs quando e se responsabilizando pela envio de logs ao repositório local ou na nuvem, não se limitando as locais mencionados a baixo, ou seja, o serviço poderá ser contratado em um endereço novo, porém será avaliado junto a proponente a melhor solução para coleta on-premisses ou na nuvem Pública sempre na modalidade Opex.

d) O provedor deve fornecer uma plataforma centralizada Web responsiva e que possua múltiplos acessos, ou seja, não restringindo o número de acessos da contrante ou contratada, essa plataforma deve conter toda a metodologia e processos do time de segurança da informação seguindo protocolos de boas práticas, **além de visibilidade total** de todos os ativos suportados pelo contrato sem nenhum tipo de restrição, esta plataforma ainda deverá fornecer modelos de relatórios e estes podem ser criados/modificados para permitir que métricas gráficas e relatórios de comparação de dados sejam produzidos ao longo do tempo.

e) A plataforma de gerencia única para todos os serviços de segurança da informação especificado neste Edital, ou seja, a proponente deverá ter capacidade de integrar todos os serviço em uma pagina Web de forma granular, a medida que o IGESDF contrate cada serviço, não será aceito ferramentas não integradas e que possua módulos de gerências em URL diferentes.

f) A proponente deverá comprovar que possui um sistema de gerenciamento próprio através de Prova de conceito tendo que instalar um ambiente em nuvem e demostrar nessa interface todos os serviços descritos nesse Edital.

g) A Proponente deverá comprovar que sua plataforma Web possui integração com os principais vendedores de Tecnologia e nuvem citadas neste Edital Switches, Roteadores, endpoint, Servidores, MS Azure e AWS.

h) Caso a proponente não possua integração nativa pontual a um dispositivo/ Ativo a mesma precisa comprovar e integrar este dispositivo ou vendor em no máximo 45 dias a contar da solicitação do IGESDF.

i) Cabe ao IGESDF avaliar a capacidade da Proponente e qualifica-lo ou não tecnicamente.

5.5.13.9. **A solução deve permitir no mínimo os seguintes relatórios (Esses templates devem ser apresentados na Prova de conceito):**

a) Eventos de bloqueio de contas

b) Eventos de autenticação com falha

c) Eventos completos do sistema de arquivos

d) Eventos reinicializados (ações)

e) Eventos excluídos e ou apagados

f) Eventos de trilha de auditoria excluídos

g) Eventos de modificação de privilégio de contas

h) Eventos de erro de sincronização de horário

i) Eventos de anomalias de tráfego de rede

j) Eventos de erro do sistema de auditoria

k) Eventos de tentativa de autenticação por força bruta

l) Eventos de troca de configuração

m) Eventos de auditoria de segurança excluídos

n) Múltiplos ataques suspeitos da mesma fonte

o) Múltiplos ataques suspeitos para o mesmo alvo

p) Falha no login (mesmo usuário) em muitos Hosts

q) Escalonamentos específicos de origem por ID do evento

r) A origem/ fonte ou destino, se estiver na lista de observação ATOR MALICIOSO conhecido (THREAT INTELLIGENCE CROSSOVER)

s) Deverá permitir a geração de um relatório completo mostrando as configurações de todas as políticas de monitoramento.

t) O provedor deve oferecer, como parte do serviço gerenciado de monitoramento e detecção de ameaças, a correlação de ataques (vários eventos identificados como um único ataque) em conformidade com os dados/ informações de vulnerabilidades.

u) O serviço deve ter a capacidade de executar análises baseadas em contexto de ameaças **globais**. O provedor do serviço gerenciado de detecção e monitoramento de ameaças e deve ser capaz de coletar, filtrar e analisar mais de um milhão de eventos por dia que seriam gerados pela infraestrutura atual do **IGESDF**.

v) O serviço de monitoramento e detecção de ameaças gerenciadas deve incluir, para análise, informações detalhadas de uma ameaça sobre a vulnerabilidade para a qual a ameaça é direcionada. Uma descrição da vulnerabilidade, **dos ativos que podem ser afetados**, informações sobre CVEs, recomendações de correção e referências externas associadas à descoberta devem ser incluídas, quando aplicável.

w) O serviço gerenciado de segurança e detecção de ameaças deve fornecer uma interface de interação com os administradores internos do **IGESDF** para a consulta das informações do serviço; é necessário:

x) A console deve fornecer recursos de acesso remoto com uma interface gráfica Web, sob protocolo seguro (HTTPS).

y) A console deve fornecer acesso alternativo por meio de dispositivos móveis, como tablets ou celulares Androide e IOs.

z) A versão "móvel" portátil da console deverá permitir efetuar consultas e modificações nos painéis a partir de qualquer dispositivo móvel.

aa) A console deverá ter autenticação de dois fatores é obrigatório.

ab) O console deve ter um módulo de controle de usuário para as partes interessadas no serviço, que pode permitir diferentes funções de permissões, como: **Administrador**, **Manutenção**, **Usuário Básico**, **Usuário de Política**, **Geração de Relatórios**, etc .; que limitam o uso/ acesso as informações por privilégios de usuário.

5.5.13.10. **A solução deve armazenar as atividades realizadas pelos usuários e permitir auditorias das atividades realizadas.**

a) A solução deve mostrar graficamente e em **tempo real** informações de histórico nos painéis associados a eventos de segurança, dispositivos, ameaças / vulnerabilidades, ativos associados a eventos, categorização de riscos.

b) A tela inicial do console deve permitir a personalização de resumos (Resumo), ou seja, o usuário deve poder personalizar o resumo do conteúdo dos dados do evento coletados nos bancos de dados, aplicando filtros por endereço IP, segmento de rede, protocolo, tipo de evento, nome do evento,

status do dispositivo, principais eventos, usuário por evento ou qualquer outro elemento que o usuário considere relevante para manter o monitoramento de segurança adequado.

c) O serviço de monitoramento e detecção de ameaças gerenciadas terá opções para responder a ameaças detectadas ou ataques direcionados, por alertas automatizados ou detecção pela operação de inteligência de ameaças que o provedor deve possuir.

d) **Serviço de monitoramento e detecção de ameaças gerenciadas deve permitir a integração com o serviço de gerenciamento de vulnerabilidades gerenciado fornecido como parte do serviço.**

e) A coleta, correlação e análise dos dados de registro dos componentes dentro do escopo da infraestrutura do **IGESDF**, conforme definido no escopo dos serviços contratados para esse fim, devem ser realizados através do serviço contratado, para o qual devem ser incluídos. um processo de:

f) Avaliação e desenho de casos de uso.

g) Diretriz com os regulamentos de segurança dos padrões que se aplicam ao **IGESDF**

h) Documentação dos Processos

i) O serviço SOC do provedor deverá apresentar as certificações para corroborar práticas e procedimentos de serviço (mínimo).

j) AICPA & SOC 2

k) PCI DSS 3.2

l) FIRST for SOC CSIRT

m) O fornecedor deve ter procedimentos aprovados com as melhores práticas internacionais;

n) Deverá fornecer uma descrição da metodologia para coletar, relatar e analisar dados e vulnerabilidades ou possíveis ataques coletar, relatar e analísar dados de vulnerabilidades ou possíveis ataques.

o) A proponente deve especificar o tempo de recuperação esperado no caso de uma falha de MTRR (Mean Time to Recovery) em que a substituição do equipamento é necessária, deve constar no documento listado no item (Item acima).

p) O provedor do serviço de monitoramento e detecção de ameaças gerenciadas deve ter localizações geográficas globais para fornecer o serviço em um esquema ininterrupto, além deste modelo que oferece capacidade redundante na execução dos serviços gerenciados.

q) O provedor de serviços gerenciados de monitoramento e detecção de ameaças deve ter equipes de especialistas que fazem parte do serviço, além de indicar o número e as certificações que o pessoal do SOC possui, incluindo o seguinte:

r) A Proponente deverá indicar claramente os diferentes modelos em relação aos contratos de nível de serviço (SLAs) para monitoramento e administração, correlação de eventos e revisão detalhada por analistas especializados e atendimento a contingências.

s) O serviço contratado deve ter a capacidade de normalizar os dados de registro para eventos das fontes do **IGESDF.**

t) A padronização deve estar alinhada às melhores práticas, tomando como ponto de partida a situação atual de acordo com o nível de operação e configuração das plataformas, que através de uma avaliação de seu estado atual, determinarão as melhorias a serem habilitadas na **IGESDF.**

u) Também deverá ser disponibilizado serviço de identificação de maturidade de segurança e deve ser executado nos processos atualmente executados nas plataformas deste escopo, o que permite;

v) A CONTRATADA deve ter o entendimento da infraestrutura e serviços atual da CONTRATANTE.

w) Identificar Gaps e recomendar ações a **IGESDF** que eleve seu nível de maturidade de segurança da informação e maturidade.

x) O objetivo a ser definido como entrega para o **IGESDF** nesta sessão é selecionar em uma base de dados casos de uso do provedor de serviços de monitoramento de ameaças, um conjunto eficaz de casos de uso e procedimentos com base nas fontes de dados da CONTRATANTE, descrito no escopo deste Elemento Técnico.

y) Maturidade

z) O fornecedor deve ter experiência e capacidade de analisar em processos de identificação, avaliação, coleta de informações, entendimento e definição de casos de uso sob uma metodologia que permita desenvolver eficientemente os fluxos e processos que permitam a **IGESDF** alto padrão de serviço gerenciado avançado de detecção e detecção de ameaças, juntamente com os processos de mitigação e **resposta a incidentes**;

aa) O processo de avaliação e identificação de maturidade do **IGESDF** deve ser suportado pelos processos certificados pelo ITIL do provedor de serviços gerenciados e todos os pontos de entrega associados a cada plataforma, processos e pessoas do **IGESDF** devem ser desenvolvidos e documentados

ab) A proponente precisará identificar e desenvolver indicadores-chave de desempenho e execução de serviços.

ac) Os serviços associados à definição de fluxos, processos e casos de uso devem atender a pelo menos três níveis de integração:

- **Identificação/ Integração ao serviço de monitoramento e detecção de ameaças.**
- **Detecção e prevenção de ameaças internas/ externas.**
- **Mitigação, resposta e investigação a incidentes.**

ad) A solução deve fornecer acesso 24x7 a relatórios, painéis, inventário de ativos e funcionalidade de pesquisa interativa por meio do Portal Web ofertado pela Proponente.

ae) O serviço de monitoramento de ameaças avançadas deve ter suporte telefônico em formato 24x7.

af) O serviço de monitoramento de ameaças gerenciadas deve enviar notificações automáticas por e-mail de alertas de segurança detectados por regras automatizadas de detecção de ameaças através do serviço contratado para detecção automática de ameaças.

ag) O serviço de monitoramento de ameaças gerenciadas deve - se realizar a análise e notificação de alertas de eventos e segurança pela equipe de **Operações Globais** de Ameaças, de acordo com os procedimentos de escalação que serão estabelecidos no início das operações, além de executar a classificação de incidentes em segurança através de uma equipe de engenheiros avançados no campo da pesquisa de ameaças que fornece:

ah) Equipe avançada de investigação de ameaças Globais.

ai) Base de dados de conhecimento que permite o cruzamento de eventos na infraestrutura **IGESDF** contra tendências de ataques, ameaças de níveis globais.

aj) Base de dados de conhecimento que permite o cruzamento de eventos na infraestrutura do **IGESDF** contra tendências de ataques, ameaças de níveis globais.

ak) O SOC do fornecedor deve obedecer obrigatoriamente a um esquema de redundância global em que possui pelo menos 5 SOCs em diferentes continentes e pelo menos 2 no continente regional onde estão localizadas as localidades a serem integradas.

al) Sob esse modelo de cobertura global, o provedor deve fornecer e cumprir o modelo de monitoramento globais, identificação e investigação de ataques, ameaças e campanhas maliciosas sob o esquema “Follow - the Threat”, para certificar que está em conformidade com as boas práticas globais, deve incluir em sua equipe equipamentos/ soluções avançadas, incluindo o seguinte:

am) Deve ter recursos humanos para a investigação, intervenção, mitigação e resposta a incidentes.

an) A equipe global de pesquisa de ameaças do provedor de SOC deve demonstrar informações sobre publicações sobre questões de segurança cibernética, publicações de vulnerabilidades descobertas e / ou explorações desenvolvidas pela equipe de pesquisa do provedor de SOC ou parceiro comercial.

ao) A equipe global de pesquisa de ameaças deve demonstrar que faz ativamente contribuições públicas no campo da segurança, como pesquisa, publicação, desenvolvimento, treinamento e apresentações; Seu trabalho deve ser publicado em um site, livro, artigo, conferência e similares.

ap) A equipe global de investigação de ameaças do provedor de SOC deve demonstrar que descobriu vulnerabilidades, com um CVE ID atribuído emitido por uma CVE Numbering Authority (CNA)

aq) A equipe global de pesquisa de ameaças do fornecedor SOC deve demonstrar que é um membro expositor em conferências de classe mundial como BlackHat, Defcon.

5.5.13.11. **Sub-Item 5.4 - Serviço de scan de vulnerabilidades em Bases de dados.**

a) O provedor deve fornecer o serviço de verificação de vulnerabilidades na rede da CONTRATANTE, com um escopo mínimo de identificação de níveis de configuração, usuários, funções e privilégios existentes, recursos definidos, nível de patch, entre outros.

b) O nível de teste deve propor os seguintes requisitos técnicos:

- Tier 0
- Scan único
- Semanal
- Mensal
- Trimestral
- O processo para esta ação deve ser realizado pela CONTRATADA e fornece uma visão dos indicadores com o nível de conformidade em cada recurso, dentro do escopo do ambiente da CONTRATADA.

5.5.13.12. **Serviço de retenção para a Resposta a Incidentes e investigação forense**

a) O provedor deve incluir um esquema de serviço de detecção e contenção de incidentes que inclua o seguinte como escopo:

b) A equipe proposta deve ter vasta experiência e conhecimento em análise, design de cenário de teste, avaliação de processos, implementação de medidas preventivas e ampla experiência nas seguintes áreas:

c) Exfiltração de dados e intrusões avançadas

d) Investigações relacionadas a fraudes com cartões bancários

e) Brechas de segurança

f) Roubo de dados

g) Ameaças internas

h) Ataques de malware

i) Sequestro virtual de informações (Ransomware)

j) A proponente deve ter capacidade para ação preventiva contra essa ameaça e os canais de detecção e geração de relatórios implementados para o serviço de contenção e neutralização de uma ameaça identificada

k) A proponente deverá identificar efetivamente os processos ou recursos que não estão suficientemente protegidos, bem como responder a incidentes associados às lacunas identificadas.

l) Como parte das funções de resposta e contenção a incidentes, o mesmo serviço deve ter

capacidade para realizar investigações forenses, a fim de identificar a origem e as causas de possíveis violações de segurança.

m) Avaliação do processo interno atual da CONTRATANTE para gerenciamento de incidentes.

n) As investigações forenses dos incidentes detectados, para esse fim, devem incluir as seguintes atividades como parte da execução do serviço de investigação:

- Determinar a causa da intrusão
- Determinar a fonte da intrusão
- Forense sobre telefones móveis
- Forense sobre laptops/Desktops/Servidores
- Aquisição de imagem forense dos discos dos dispositivos
- Análise avançada de malware
- Busca por palavras chaves
- Recuperação dos correio/ e-mail e dados eliminados
- Monitoramento de atividades na rede

o) O provedor deve ter os seguintes cenários de tempo de resposta ao solicitar um serviço de resposta a incidentes emergente:

- Respostas emergências:
  - **Até 2 horas em resposta por chamada de solicitação.**
  - **Transferência dos equipamentos do fornecedor para as instalações do IGESDF, no máximo 24 horas, se necessário.**

5.5.13.13. **Serviço de provas de penetração em Aplicações**

a) O provedor deve fornecer o serviço de verificação de vulnerabilidade interna / externa na rede do IGESDF.

b) O nível de evidência deve propor entre os seguintes requisitos técnicos

Serviço	Frequência de execução	Alcance Inicial (Primeiro pedido)	Descrição	Entregáveis
Pentest Aplicativo	3 Testes + 3 retestes para uma periodo de 12 meses (mínimo)	**2 aplicações**	**Validação em caixa preto e branco do nível de segurança no código do aplicativo.**	**Relatório detalhando as revisões e recomendações de ferramentas, aplicativos, bibliotecas ou serviços comerciais existentes usados e controles de segurança existentes**

5.5.13.14. **Serviço de penetração em Bases de dados (BD)**

a) O provedor de serviços gerenciados do SOC deve incluir uma solução de segurança de banco de dados IGESDF que ofereça os seguintes recursos:

- Scan e Provas de penetração
- Descoberta de ativos e usuários

- Avaliação dos direitos e privilégios de acesso do usuário
- Avaliação de vulnerabilidades e sua categorização
- Mitigação e auditoria de riscos
- Monitoramento e alerta on-line
- Respostas a ameaças/incidentes

b) Ambiente do BD:

c) A seguir, é apresentada uma descrição do ambiente do servidor de banco de dados no qual o IGESDF deseja usar apenas uma ferramenta de avaliação de vulnerabilidade de banco de dados ou uma ferramenta de avaliação de vulnerabilidade de banco de dados bem como uma ferramenta de auditoria de dados. Essa descrição deve ser usada para fornecer preços d**e** itens de linha para cada um dos servidores / instâncias identificados. Cada um dos servidores foi identificado como uma das três categorias funcionais possíveis e deve ter um preço correspondente:

- **Produção -** esses servidores são usados para cargas de trabalho de produção
- **Não produção** - esses servidores são usados para cargas de trabalho de desenvolvimento, testes etc
- **DRP**: esses servidores são reservados e usados exclusivamente para fins de recuperação de desastre ou teste de recuperação de desastre.

5.5.13.15. **Requerimentos da solução:**

- A solução deve ser baseada no host ou no sensor de rede
- A solução deve estar em software
- A solução deve poder ser instalada em ambientes virtuais
- Deve suportar um cenário de implantação distribuído para cobrir várias localizações geográficas.
- O repositório de armazenamento local deve permitir que você mantenha todas as informações coletadas online por um período mínimo de 12 meses
- A solução deve permitir escalabilidade flexível.

5.5.13.16. **Administração e manutenção de soluções**

a) A solução deve fornecer uma única interface de administração central para acessar todas as funções dos bancos de dados listados no ambiente para os vários locais no escopo.

b) A solução deve incluir um gerenciador de políticas de auditoria centralizado e uma plataforma de alerta fácil de configurar e gerenciar.

c) A solução deve ter um mecanismo de autenticação de usuário por meio do LDAP.

d) A solução deve permitir definir e criar um perfil do acesso do usuário a novos usuários do sistema (incluindo quem controla, a capacidade de definir funções específicas e direitos de acesso diferenciais, tempo de entrega necessário, notificações, etc.).

e) A solução deve ter a capacidade de descobrir bancos de dados.

f) A solução deve manter um inventário de instâncias e dispositivos de banco de dados em cada infraestrutura da CONTRATANTE, onde pode localizar ativos de banco de dados em qualquer lugar da organização que possua vários endereços IP usando portas padrão.

g) A solução deve poder aplicar políticas de gerenciamento de configuração a instâncias recém-descobertas.

h) A solução deve realizar a avaliação da vulnerabilidade e priorizar as descobertas, que devem incluir, no mínimo, uma avaliação abrangente dos riscos da infraestrutura do banco de dados de destino, que inclui, entre outros:

- Software sem patches
- Senhas fracas e padrão

- Avaliação da segurança da senha
- Usando a expiração de senha das portas padrão
- Configurações incorretas do banco de dados
- Configurações da conta do usuário, permissões excessivas, etc

i) A solução deve permitir avaliações programáveis, como diária, semanal, mensal, anual e personalizada, e descrever os destinatários para os quais os relatórios de descoberta são direcionados, por exemplo:

- Relatórios para auditoria
- Relatórios para Segurança
- Relatórios para infraestrutura
- Relatórios executivos / comerciais
- Relatórios de conformidade
- Relatórios de desvio / abuso de privilégios

j) A solução deve atualizar periodicamente o banco de dados quanto a vulnerabilidades (por exemplo, teste de um problema de configuração recém-descoberto) e defesas contra comportamentos maliciosos conhecidos como ataque.

k) **Remediação**

- A solução deve ter mecanismos através dos quais a solução possa facilitar a correção e mitigação de riscos automaticamente
- A solução deve fornecer uma maneira de acabar com USER IDs inativos.
- A solução deve mapear vulnerabilidade residual
- A solução deve estabelecer uma linha de base de segurança do banco de dados, rastreando vulnerabilidades ao longo do tempo.
- A solução deve monitorar todas as atividades do banco de dados (DDL, DML, DCL) em tempo real.
- A solução deve ter recursos para monitorar usuários privilegiados e atividades administrativas privilegiadas na rede.
- A solução deve capturar toda a atividade SQL, independentemente de como o usuário esteja conectado ao banco de dados, por exemplo: usando soquetes, pipes nomeados, conexões locais ou remotas.
- A solução deve ter mecanismos e opções de política para descobrir e alertar contra essa atividade privilegiada.
- A solução deve ter auditoria nativa.
- A solução deve fornecer recursos de auditoria que podem ser facilmente implantados em qualquer aplicativo corporativo sem comprometer o desempenho, independentemente da plataforma de banco de dados de back-end.
- A solução deve incluir modelos predefinidos de regras ou políticas que podem ser implementadas rapidamente.
- A solução deve fornecer a capacidade exclusiva de cumprir várias regulamentações (por exemplo, Sarbanes-Oxley, PCI, HIPAA, etc.)
- A solução deve incluir políticas predefinidas.
- A solução deve permitir a personalização de políticas, a granularidade dos controles / opções de políticas por meio de um Assistente.
- A solução deve fornecer uma solução alternativa para instâncias com falhas de correção desatualizadas (definidas como o período entre a descoberta de vulnerabilidades e a implantação de correções).
- A solução deve ser baseada no comportamento de aprendizagem.

5.5.13.17. **Relatórios, incluindo personalização e publicação.**

- A solução deve fornecer relatórios e gráficos detalhados para uso de usuários técnicos e não técnicos (executivos).
- A solução deve gerar relatórios automáticos regulares de privilégios de usuário do banco de dados para ajudar a garantir que os privilégios existentes sejam apropriados para o usuário e estejam em conformidade com a política de segurança.
- A solução deve registrar e relatar falhas e tentativas bem-sucedidas de login nos bancos de

dados.

- A solução deve gerar relatórios periódicos que listam os servidores de banco de dados que se afastam da política de configuração padrão.
- A solução deve gerar uma lista de todos os usuários de todos os bancos de dados, incluindo seus direitos e privilégios de acesso.
- A solução deve incluir uma plataforma centralizada de relatórios e alertas que possa ser usada por auditores internos e administradores de segurança de acordo com o perfil de acesso definido para cada usuário / departamento.
- A solução deve incluir relatórios predefinidos para demonstrar conformidade com vários regulamentos e normas do setor (SOX, PCI, HIPAA, Basileia II, etc.)
- Ele também deve ter capacidade para configurar auditorias personalizadas e relatórios de conformidade.
- A solução deve automatizar e agendar relatórios
- Em tempo de solicitação de OS serão acordados os prazos de execução.

5.5.13.18. **Sub-Item 5.5 – Serviço de pen test em redes corporativas**

a) O provedor deve fornecer o serviço Pentesting interno / externo na rede do IGESDF, o exercício para o perímetro externo da rede do IGESDF deve ser fornecido por meio de um esquema gerenciado por meio de uma plataforma centralizada com acesso remoto.

b) Para testes no perímetro interno, ele deve ser realizado a partir do serviço gerenciado do provedor e executado através de um scanner virtual que deve ser fornecido pelo provedor.

c) A execução do Pentesting, devera ser agendada e acordado com a CONTRATANTE.

d) O nível de teste deve propor os seguintes requisitos técnicos:

- A contratação do serviço de pentest deverá ser contratado na modalidade de serviço anual, este escopo deve seguir as seguintes premissas.

Serviço	Frequência de execução	Alcance Inicial (Primeiro pedido)	Descrição	Entregáveis
Prova de Intrusão (Pentest Interno)	3 Testes + 3 retestes para uma período de 12 meses (mínimo)	X Redes interna Corporativa Clase C	1. Planejamento de teste 2. Execução de teste 3. Redação e geração de relatórios	a) Análise interna de penetração e segmentação para o escopo do PCI, anualmente. b) Geração e apresentação formal do relatório obtido.

5.5.13.19. **Sub-Item 5.6 - Serviço de provas de penetração em Aplicações**

a) O provedor deve fornecer o serviço de verificação de vulnerabilidade interna / externa na rede do IGESDF.

b) O nível de evidência deve propor entre os seguintes requisitos técnicos:

Serviço	Frequência de execução	Alcance Inicial (Primeiro pedido)	Descrição	Entregáveis
Pentest Aplicativo	3 Testes + 3 retestes para uma periodo de 12 meses (mínimo)	**2 aplicações**	**Validação em caixa preto e branco do nível de segurança no código do aplicativo.**	**Relatório detalhando as revisões e recomendações de ferramentas, aplicativos, bibliotecas ou serviços comerciais existentes usados e controles de segurança existentes**

5.5.13.20. **Sub-Item 5.7 - Serviço de penetração em Bases de dados (BD)**

a) O provedor de serviços gerenciados do SOC deve incluir uma solução de segurança de banco de dados da CONTRATANTE que ofereça os seguintes recursos:

- Scan e Provas de penetração
- Descoberta de ativos e usuários
- Avaliação dos direitos e privilégios de acesso do usuário
- Avaliação de vulnerabilidades e sua categorização
- Mitigação e auditoria de riscos
- Monitoramento e alerta on-line
- Respostas a ameaças/incidentes

b) Ambiente do BD:

c) A seguir, é apresentada uma descrição do ambiente do servidor de banco de dados no qual o IGESDF deseja usar apenas uma ferramenta de avaliação de vulnerabilidade de banco de dados ou uma ferramenta de avaliação de vulnerabilidade de banco de dados bem como uma ferramenta de auditoria de dados. Essa descrição deve ser usada para fornecer preços d**e** itens de linha para cada um dos servidores / instâncias identificados. Cada um dos servidores foi identificado como uma das três categorias funcionais possíveis e deve ter um preço correspondente:

- **Produção -** esses servidores são usados para cargas de trabalho de produção
- **Não produção** - esses servidores são usados para cargas de trabalho de desenvolvimento, testes etc
- **DRP**: esses servidores são reservados e usados exclusivamente para fins de recuperação de desastre ou teste de recuperação de desastre.

5.5.13.21. **Requerimentos da solução:**

- A solução deve ser baseada no host ou no sensor de rede
- A solução deve estar em software
- A solução deve poder ser instalada em ambientes virtuais
- Deve suportar um cenário de implantação distribuído para cobrir várias localizações geográficas.
- O repositório de armazenamento local deve permitir que você mantenha todas as

informações coletadas online por um período mínimo de 12 meses
- A solução deve permitir escalabilidade flexível.

5.5.13.22. **Administração e manutenção de soluções**

5.5.13.23. A solução deve fornecer uma única interface de administração central para acessar todas as funções dos bancos de dados listados no ambiente para os vários locais no escopo.

5.5.13.24. A solução deve incluir um gerenciador de políticas de auditoria centralizado e uma plataforma de alerta fácil de configurar e gerenciar.

5.5.13.25. A solução deve ter um mecanismo de autenticação de usuário por meio do LDAP.

5.5.13.26. A solução deve permitir definir e criar um perfil do acesso do usuário a novos usuários do sistema (incluindo quem controla, a capacidade de definir funções específicas e direitos de acesso diferenciais, tempo de entrega necessário, notificações, etc.).

5.5.13.27. A solução deve ter a capacidade de descobrir bancos de dados.

5.5.13.28. A solução deve manter um inventário de instâncias e dispositivos de banco de dados em cada infraestrutura da CONTRATANTE, onde pode localizar ativos de banco de dados em qualquer lugar da organização que possua vários endereços IP usando portas padrão.

5.5.13.29. A solução deve poder aplicar políticas de gerenciamento de configuração a instâncias recém-descobertas.

5.5.13.30. A solução deve realizar a avaliação da vulnerabilidade e priorizar as descobertas, que devem incluir, no mínimo, uma avaliação abrangente dos riscos da infraestrutura do banco de dados de destino, que inclui, entre outros:

- Software sem patches
- Senhas fracas e padrão
- Avaliação da segurança da senha
- Usando a expiração de senha das portas padrão
- Configurações incorretas do banco de dados
- Configurações da conta do usuário, permissões excessivas, etc

A solução deve permitir avaliações programáveis, como diária, semanal, mensal, anual e personalizada, e descrever os destinatários para os quais os relatórios de descoberta são direcionados, por exemplo:

- Relatórios para auditoria
- Relatórios para Segurança
- Relatórios para infraestrutura
- Relatórios executivos / comerciais
- Relatórios de conformidade
- Relatórios de desvio / abuso de privilégios

A solução deve atualizar periodicamente o banco de dados quanto a vulnerabilidades (por exemplo, teste de um problema de configuração recém-descoberto) e defesas contra comportamentos maliciosos conhecidos como ataque.

5.5.13.31. **Remediação**

- A solução deve ter mecanismos através dos quais a solução possa facilitar a correção e mitigação de riscos automaticamente
- A solução deve fornecer uma maneira de acabar com USERIDs inativos.
- A solução deve mapear vulnerabilidade residual
- A solução deve estabelecer uma linha de base de segurança do banco de dados, rastreando vulnerabilidades ao longo do tempo.
- A solução deve monitorar todas as atividades do banco de dados (DDL, DML, DCL) em tempo real.
- A solução deve ter recursos para monitorar usuários privilegiados e atividades administrativas privilegiadas na rede.

- A solução deve capturar toda a atividade SQL, independentemente de como o usuário esteja conectado ao banco de dados, por exemplo: usando soquetes, pipes nomeados, conexões locais ou remotas.
- A solução deve ter mecanismos e opções de política para descobrir e alertar contra essa atividade privilegiada.
- A solução deve ter auditoria nativa.
- A solução deve fornecer recursos de auditoria que podem ser facilmente implantados em qualquer aplicativo corporativo sem comprometer o desempenho, independentemente da plataforma de banco de dados de back-end.
- A solução deve incluir modelos predefinidos de regras ou políticas que podem ser implementadas rapidamente.
- A solução deve fornecer a capacidade exclusiva de cumprir várias regulamentações (por exemplo, Sarbanes-Oxley, PCI, HIPAA, etc.)
- A solução deve incluir políticas predefinidas.
- A solução deve permitir a personalização de políticas, a granularidade dos controles / opções de políticas por meio de um Assistente.
- A solução deve fornecer uma solução alternativa para instâncias com falhas de correção desatualizadas (definidas como o período entre a descoberta de vulnerabilidades e a implantação de correções).
- A solução deve ser baseada no comportamento de aprendizagem.

5.5.13.32. **Relatórios, incluindo personalização e publicação.**

- A solução deve fornecer relatórios e gráficos detalhados para uso de usuários técnicos e não técnicos (executivos).
- A solução deve gerar relatórios automáticos regulares de privilégios de usuário do banco de dados para ajudar a garantir que os privilégios existentes sejam apropriados para o usuário e estejam em conformidade com a política de segurança.
- A solução deve registrar e relatar falhas e tentativas bem-sucedidas de login nos bancos de dados.
- A solução deve gerar relatórios periódicos que listam os servidores de banco de dados que se afastam da política de configuração padrão.
- A solução deve gerar uma lista de todos os usuários de todos os bancos de dados, incluindo seus direitos e privilégios de acesso.
- A solução deve incluir uma plataforma centralizada de relatórios e alertas que possa ser usada por auditores internos e administradores de segurança de acordo com o perfil de acesso definido para cada usuário / departamento.
- A solução deve incluir relatórios predefinidos para demonstrar conformidade com vários regulamentos e normas do setor (SOX, PCI, HIPAA, Basileia II, etc.)
- Ele também deve ter capacidade para configurar auditorias personalizadas e relatórios de conformidade.
- A solução deve automatizar e agendar relatórios

5.5.13.33. **Integração com outras soluções de segurança / gerenciamento.**

a) A solução deve ter integração com outras soluções de terceiros por meio do SIEM, etc.

5.5.13.34. **Sub-Item 5.8 - Serviço gerenciado na Busca Proativa de Ameaças (Proactive Threat Hunting) e serviços especializados em Cyberintelligence.**

a) O provedor deve fornecer um serviço de busca de ameaças para identificar os ATPs na infraestrutura **IGESDF**, a fim de encontrar e eliminar qualquer ameaça e erradicar os atacantes envolvidos.

b) Além disso, você deverá ser fornecido os seguintes recursos

- Visibilidade de fraquezas anteriores desconhecida
- Software vulnerabilidade
- Violações de políticas
- Ameaça interna (atacantes)
- Bases de dados não protegidas

c) Além disso, o fornecedor deve ter a experiência, a infraestrutura e a capacidade de recursos verificáveis (equipe técnica) para fornecer os seguintes serviços, conforme necessário:

- Red Team
- Purple team
- Pen Test para aplicações móveis
- Revisão de segurança (Lógica/física) para ATMs e pentest
- Revisão de código de aplicações
- Engenharia social, contendo:
- Segurança Física
- Phishing
- PenTest para WiFi
- Avaliação de segurança para AWS
- Avaliação de segurança para Azure
- Avaliação de segurança para Active Directory
- Proteção corporativa / de marca:
- Investigações na exposição de dados no Dark / Deep Web

d) O Serviço deverá sempre ser contrato em conjunto com item ou itens desta especificação, devido a operacionalização dos serviço contratados pelo IGESDF e o mesmo deve ser compatível e atender a todas as necessidade deste termo parcial ou na sua totalidade.

- Preposto do Contrato, responsável pelas questões nominais (recursos humanos, infraestrutura, contratação, revisões, etc.) da equipe atribuída ao fornecedor.
- Analista, que gerenciará a operação correta dos serviços de segurança gerenciados fornecidos pelo proponente e será responsável por manter os níveis de serviço (SLAs) e coordenará o grupo de engenheiros de operações.
- Grupo de acompanhamento e atenção a incidentes, que será responsável por coordenar a atenção e acompanhamento de incidentes ou falhas de alto nível que são escalados pelo grupo de operação dentro dos limites de atenção dos SLAs.
- Grupo de Operações, será o preposto, este encarregado da administração, monitoramento e suporte dos serviços recorrentes de segurança de computadores gerenciados no perímetro em um esquema de gestão de monitoramento.
- O Preposto deve ter pelo menos uma das certificações :
- CISSP
- CISA
- CISM
- CEH
- A equipe de inteligência cibernética e investigação deverá atuar em modalidade 24x07x365

5.5.13.35. **DA MIGRAÇÃO OBRIGATÓRIO DOS SERVIÇOS ATUAIS**

a) Os serviços de migração de infraestrutura **On-Premises / Hyperconvergência / Cloud atuais serão obrigatórios a nova CONTRATADA.**

b) 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;**

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

f) Os serviços não podendo ultrapassar o limite de 10 (dez) dias corridos dedicado in-loco no IGESDF.

6. DO SUPORTE TÉCNICO

6.1. A CONTRATADA deverá obter suporte técnico, no regime de 24 (vinte e quatro) horas, durante os 7 (sete) dias da semana, nos 365 (trezentos e sessenta e cinco) dias do ano.

6.2. 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 esta em operação o suporte técnico descrito neste item.

6.3. Os serviços de Suporte Técnico compreendem todos os chamados relativos 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.

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

6.5. Os chamados de suporte técnico serão classificados por severidade, de acordo com o impacto no ambiente computacional da CONTRATANTE. Os possíveis níveis de severidade são:

a) Severidade 1 - Deveremos entender como Severidade **1** um serviço totalmente fora de operação

b) Severidade 2 - Deveremos entender como Severidade **2** incidentes que não impeçam o uso do equipamento ou consultas em geral sobre o uso dos equipamentos

c) Severidade 3 - Deveremos entender como Severidade **3** os testes funcionais e consultas gerais do equipamento.

6.6. 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

Tabela 01 – SLA de atendimento da solução de telefonia

Nível de severidade	Descrição	Prazo para início de atendimento	Prazo para conclusão de atendimento	Desconto por não atendimento no prazo
Severidade 1	Deveremos entender como Severidade **1** um serviço totalmente fora de operação	10 minutos após abertura do chamado	2 horas após abertura do chamado	2%
Severidade 2	Deveremos entender como Severidade **2** incidentes que não impeçam o uso do equipamento ou	10 minutos após abertura do chamado	4 horas após abertura do chamado	1,50%

	consultas em geral sobre o uso dos equipamentos			
Severidade 3	Deveremos entender como Severidade **3** os testes funcionais e consultas gerais do equipamento.	10 minutos após abertura do chamado	6 horas após abertura do chamado	1%
Observação	Troca de Equipamento defeituoso	30 minutos após abertura do chamado	O fornecedor deverá providenciar equipamento de reserva em caso de falhas e este equipamento deverá estar disponível no período a ser negociado com a CONTRATADA	2%

6.7. A CONTRATADA não será responsabilizada pelo prazo máximo estabelecido na Tabela 1, quando o chamado for originado por falha, interrupção ou qualquer outra ocorrência nos serviços de telecomunicações ou energia elétrica que atendem à infraestrutura interna da CONTRATANTE; indisponibilidade de dados, inconsistência de dados e informações geradas pela CONTRATANTE; infraestrutura e capacidade de ambiente de tecnologia da CONTRATANTE, não se caracterizando, nesses casos, a indisponibilidade dos serviços ou inadimplemento da CONTRATADA.

6.8. Deverá possuir SLA mínimo de aceitável de **99,9%** (noventa e nove vírgula nove por cento) de disponibilidade do item 01 e para os demais serviços de 99,8% (noventa e nove vírgula oito por cento).

6.9. Toda e qualquer intervenção no ambiente produtivo resultante de serviços de suporte técnico deve ser executada somente mediante prévia autorização da CONTRATANTE, a partir de informações claras dos procedimentos que serão adotados/executados pela CONTRATADA.

6.10. No final do atendimento e resolução da ocorrência, o técnico da CONTRATADA realizará, em conjunto com representantes da CONTRATANTE, testes para verificação dos resultados obtidos, certificando-se do restabelecimento à normalidade e/ou resolução do problema.

6.11. Ao término dos testes e do atendimento (fechamento do chamado), a CONTRATADA deverá registrar, detalhadamente, por e-mail, as causas do problema e a resolução adotada.

6.12. Nos casos em que o atendimento não se mostrar satisfatório, a CONTRATANTE fará reabertura do chamado, mantendo-se as condições e prazos do primeiro chamado.

7. DAS CONDIÇÕES DE PAGAMENTO, LOCAL DE EXECUÇÃO DOS SERVIÇOS E DA FISCALIZAÇÃO

7.1. O pagamento será realizado em até 30 (trinta) dias uteis da certificação da Nota fiscal referente a Ordem de Serviço **(anexo III)**e apresentação de relatório mensal dos serviços prestados na Ordem de serviço, todos os itens, devem ser atestado pela área técnica responsável.

7.2. A disponibilização de Itens referentes a este Elemento Técnico, deve ser utilizada a Ordem de Fornecimento (**anexo IV**)

7.3. Os serviços deverão ser prestados nas dependências das unidades do IGESDF (Hospital de Base do Distrito Federal - HBDF, Hospital Regional de Santa Maria – HRSM, nas UPAs da Ceilândia, Núcleo Bandeirante, Recanto das Emas, Samambaia, São Sebastião, Sobradinho, e nas unidades do

Edifício PO700 e SIA).

7.4. A Fiscalização da prestação dos serviços será exercida pela Gerência de Infraestrutura da Superintendência de Tecnologia da Informação.

8. DOS CRITÉRIOS PARA ACEITAÇÃO DAS PROPOSTAS

8.1. A proposta de preços deve conter o prazo de validade e planilha de custo, discriminado o custo total do fornecimento.

8.2. A proposta deve vir acompanhada de detalhamento técnico da solução proposta, apresentando lista com todos os elementos (hardware/software/licenças) que serão fornecidos para a funcionamento da solução. A lista deve apresentar a marca, modelo, versão e quantidade de todos os elementos fornecidos.

8.3. Deve possuir topologia completa da solução fornecida.

8.4. A não apresentação da proposta técnica com o detalhamento técnico da solução proposta resultará na desclassificação.

8.5. A proposta deve ser endereçada e enviada ao IGESDF, em meio eletrônico para o e-mail compras.servicos@igesdf.org.br, no prazo a ser estipulado pelo pregoeiro do certame e deve conter o CNPJ, endereço, responsável e telefone para contato.

9. DO CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

9.1. Atendidos todos os requisitos estabelecidos neste Elemento Técnico, será contratada a empresa que apresentar o **MENOR PREÇO GLOBAL DO LOTE** e atenda as qualificações deste instrumento, nos termos do Regulamento de Compras e Contratações do IGESDF.

10. DA SELEÇÃO

10.1. A seleção da empresa deste Pedido de Cotação será feita da seguinte forma:

10.1.1. O recebimento das propostas comerciais será conforme prazo estabelecido neste Elemento Técnico.

10.1.2. Após selecionadas as propostas pelo IGESDF, será realizada a análise técnica e classificadas justificadamente, conforme estabelecido no Regulamento Próprio de Compras e Contratações do IGESDF.

11. DA HABILITAÇÃO

11.1. Será solicitada documentação de Habilitação somente ao(s) Concorrente(s) vencedor(es), através do endereço eletrônico compras.servicos@igesdf.org.br, para verificar o atendimento das condições de Habilitação.

11.2. O fornecedor que não enviar a documentação SERÁ INABILITADO.

12. DA HABILITAÇÃO E QUALIFICAÇÃO TÉCNICA

12.1. O Fornecedor deverá apresentar os documentos referentes à regularidade fiscal, jurídica e técnica, conforme relacionados abaixo:

12.1.1. **RELATIVA À REGULARIDADE FISCAL:**

a) CNPJ – Comprovante de inscrição e de situação cadastral no Cadastro Nacional de Pessoa Jurídica;

b) União – Certidão Negava de regularidade com a Fazenda Federal, mediante certidão conjunta negava de débitos, ou positiva com efeitos de negava, relativos aos tributos federais e à Dívida Ativa

da União;

c) CNDT – Certidão Negava de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante Certidão Negava de Débitos Trabalhistas, ou certidão positiva com efeitos de negativa;

d) FGTS – Certidão Negava de regularidade relava ao Fundo de Garantia do Tempo de Serviço, mediante Certificado de Regularidade;

e) Certidão Negava de regularidade perante as Fazendas Municipal, Estadual ou Distrital da sede do fornecedor;

f) CEIS – Cadastro Nacional de Empresas Inidôneas e Suspensas, mando pela Controladoria Geral da União;

g) CNJ – Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrava, mantido pelo Conselho Nacional de Justiça;

h) TCU – Lista de Inidôneos, manda pelo Tribunal de Contas da União; e Certidão Negava de Falência ou Concordata (art.192, Lei nº11.101/2005), Recuperação Judicial ou Extrajudicial e Execução patrimonial, expedidas pelo setor de distribuição da Justiça Comum, Justiça Federal e Justiça do Trabalho do domicílio ou domicílios da pessoa física ou jurídica.

12.1.2. **RELATIVA À HABILITAÇÃO JURÍDICA:**

a) Cópia da Cédula de identidade, quando se tratar de empresa Pessoa Física;

b) No caso de empresa individual: registro empresarial na junta comercial;

c) No caso de sociedades comerciais: Ato Constitutivo, Estatuto ou Contrato Social em vigor, devidamente registrado na junta comercial. Os documentos deverão estar acompanhados de todas as alterações ou da consolidação respectiva;

d) Documento comprobatório autenticado de seus administradores reconhecido nacionalmente (CNH, carteira de identidade, registro profissional ou outro);

e) No caso de sociedades por ações: Ato Constitutivo, Estatuto ou Contrato Social em vigor, devidamente registrado, acompanhado de documentos de eleição de seus administradores, em exercício;

f) No caso de sociedades civis: inscrição do Ato constitutivo e alterações subsequentes no Registro civil das Pessoas Jurídicas, prova de diretoria em exercício; acompanhada de prova de diretoria em exercício;

g) No caso de empresa ou sociedade estrangeira em funcionamento no país: decreto de autorização e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir; e

h) Para todos os efeitos, considera-se como Ato Constitutivo, Estatuto ou Contrato Social em vigor, o documento de constituição da empresa, acompanhado da (s) última (s) alteração (ões) referente (s) à natureza da atividade comercial e à administração da empresa, ou a última alteração consolidada.

12.1.3. **QUANTO À REPRESENTAÇÃO**

a) Se representante legal apresentar procuração por instrumento particular ou público, com poderes para praticar os atos pertinentes da Seleção de Fornecedores;

b) Na hipótese de procuração por instrumento particular, deverá vir acompanhada do documento constitutivo do proponente ou de outro documento em que esteja expressa a capacidade/competência do outorgante para constituir mandatário; e

c) O representante legal constante na procuração deverá apresentar documento comprobatório autenticado reconhecido nacionalmente (CNH, carteira de identidade, registro profissional ou outro), assim como do sócio outorgante.

12.1.4. COMPROVAÇÃO DA QUALIFICAÇÃO TÉCNICA

a) 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 projeto básico.

b) 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 IaaS com complexidade semelhante, com disponibilização por unidades em números compatíveis com as unidades de atendimentos do IGESDF.

c) 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 mensageria com no mínimo de 5.000 caixas de e-mail contemplados em um único contrato no período de 12 meses.

d) 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 em quantidades e métricas semelhantes com o nível de sla mínimo de 99%.

e) 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 de end point com no mínimo 3.000 dispositivos em um único contrato no período de 12 meses.

f) 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 de storage como serviço contemplando no mínimo a disponibilização de 160 TB (terabytes) em um único contrato no período de 12 meses.

g) Os Atestado(s) de Capacidade Técnica-Operacional deverá(ão) ser emitido(s) por entidade da Administração Federal, Estadual ou Municipal, direta ou indireta e/ou empresa privada que comprove ter a empresa licitante executado serviços de características técnicas semelhantes ao objeto desta contratação.

h) 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.

i) Os atestados deverão ser emitidos em papel timbrado e conter:

j) Razão Social, CNPJ e Endereço Completo da Empresa Emitente;

k) Razão Social da Contratada;

l) Número e vigência do contrato se for o caso;

m) Objeto do contrato;

n) Declaração de que foram atendidas as expectavas quanto ao cumprimento de cronogramas pactuados;

o) Local e Data de Emissão;

p) Identificação do responsável pela emissão do atestado,

q) Cargo, Contato (telefone e correio eletrônico);

r) Assinatura do responsável pela emissão do atestado;

s) Devem ser originais ou autenticados, se cópias, e legíveis;

t) 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.

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

13. DA SUBCONTRATAÇÃO

13.1. Não será admitida a subcontratação do objeto deste instrumento.

14. PRAZO DE VIGÊNCIA CONTRATUAL

14.1. O contrato terá sua vigência pelo prazo de 12 (doze) meses, a contar de sua assinatura, podendo ser prorrogado, por acordo entre as partes, mediante a Termo Aditivo e não poderá ultrapassar o limite máximo de 60 (sessenta) meses, conforme preconiza o parágrafo único, do art. 29, do Regulamento Próprio de Compras e Contratação do Instituto de Gestão Estratégica de Saúde IGESDF.

15. DO PRAZO DE INICIO DE FORNECIMENTO

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

15.2. Devido a imprescindibilidade do fornecimento da solução, os equipamentos deverão ser entregues no prazo máximo de 30 (trinta) dias corridos após a emissão de Ordem de Fornecimento (anexo IV).

15.3. Caso haja alguma impossibilidade no cumprimento do prazo do item 15.1, a CONTRATADA deverá emitir justificativa formal para obtenção da extensão do prazo, sendo prorrogável por igual período.

16. DAS SANÇÕES ADMINISTRATIVAS

16.1. Pelo descumprimento de quaisquer cláusulas ou condições presentes nesta Especificação Técnica, serão aplicadas as sanções estabelecidas nos Arts 41 e 42 do Regulamento Próprio de Compras e Contratações do Instituto de Gestão Estratégica de Saúde do Distrito Federal – IGESDF descritos no item 22 deste Elemento Técnico.

17. DA GARANTIA

17.1. Exigência de Garantia de Execução do Contrato será limitada a 10% (dez por cento) do valor do contrato conforme estabelecidas nos Art 30 do Regulamento Próprio de Compras e Contratações do Instituto de Gestão Estratégica de Saúde do Distrito Federal – IGESDF, e à escolha do prestador, consistirá em:

I. caução em dinheiro;
II. fiança bancária; ou
III. seguro garantia. "

18. DA RESCISÃO CONTRATUAL

18.1. A rescisão do contrato se dará nos termos dos Artigos 35 e 38 do Regulamento Próprio

de Compras e Contratações do Instituto de Gestão Estratégica de Saúde do Distrito Federal - IGESDF.

19. OBRIGAÇÕES DA CONTRATADA

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

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

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

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.

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

19.6. Substituir, sempre que exigido pelo IGESDF, qualquer empregado cuja atuação, permanência e/ou comportamento sejam prejudiciais, inconvenientes, insatisfatórios à disciplina da repartição ou ao interesse do serviço, ou ainda, incompatíveis com o exercício das funções que lhe forem atribuídas.

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

19.8. 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.

19.9. Responder pelo cumprimento dos postulados legais vigentes de âmbito federal, estadual ou municipal.

19.10. 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.

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

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

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

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

19.15. 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.

19.16. Indicar um preposto para acompanhar a execução do contrato e responder perante o Contratante.

19.17. 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 CONTRATADA.

19.18. 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.

19.19. 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.

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

20. OBRIGAÇÕES DA CONTRATANTE

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

20.2. Exigir o cumprimento de todas as obrigações assumidas pela contratada, de acordo com as cláusulas contratuais e os termos de sua proposta.

20.3. Exercer o acompanhamento e a fiscalização do fornecimento, notificando a Contratada por escrito da ocorrência de eventuais imperfeiçoes no curso da execução dos serviços, fixando prazo para sua correção.

20.4. Pagar à contratada o valor resultante do valor do fornecimento da solução, no prazo e condições estabelecidas no Contrato.

20.5. Emitir procuração específica com poderes para representá-lo nas ações que forem confiadas aos advogados da Contratada.

20.6. Fornecer todos os subsídios necessários ao desempenho da atividade da Contratada, encaminhando os documentos necessários à adequada realização dos serviços.

20.7. Responder os recursos apresentados pelos candidatos, recebidos no site da Contratada.

21. DO FORO

21.1. Fica eleito o foro da Cidade de Brasília/DF para dirimir as dúvidas não solucionadas administrativamente oriundas do cumprimento das obrigações estabelecidas.

22. PENALIDADES

22.1. O atraso injustificado na entrega do(s) serviço(s) e produto(s), objeto do presente Elemento Técnico, sujeitará o fornecedor, sem prejuízo das sanções previstas nos artigos 35, 41, 42 e 43 do Regulamento Próprio de Compras e Contratações do IGESDF, às seguintes multas:

a) 0,1% (um décimo por cento) ao dia, sobre o valor total da aquisição, até o limite de 30 (trinta) dias;

b) 10% (dez por cento), cumulativamente, sobre o valor total da aquisição, após 30 (trinta) dias, podendo ainda o IGESDF, a seu critério, impedir o fornecedor de participar de novas cotações com este Instituto.

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

22.3. O atraso injustificado na execução do Contrato sujeitará a Contratada à multa de mora no valor de 0,3% (três décimo por cento) do valor do Contrato, sem prejuízo das outras penalidades decorrentes da mora.

22.4. Compete ao Gestor ou à Comissão Gestora do Contrato sugerir pela rescisão ou aplicação de penalidade, encaminhando os autos a autoridade competente para a tomada de decisão.

22.5. A violação das obrigações descritas neste termo repercute na penalidade de advertência.

22.6. A violação das obrigações descritas neste termo repercute na penalidade de multa, por infração, de, no mínimo 0,1% (um décimo por cento) a, no máximo, 0,5% (cinco décimo por cento) do valor total do item do lote contratado.

22.7. A reincidência, no período de 12 meses, de infração passível de advertência, repercute na penalidade de multa correspondente a 0,05% cinco centésimos por cento) do valor máximo do lote, por conduta infracional, posterior à que ensejou a reincidência.

22.8. No caso de reincidência, no período de 12 meses, das violações passíveis de multa, as penalidades posteriores àquela que ensejou a reincidência, serão punidas com multa correspondente ao dobro do valor da última penalidade.

22.9. De acordo com a repercussão econômica, social, moral ou, ainda, a reiteração da violação cometida, poderá ser aplicada penalidade mais severa ou branda, ressaltando que a inidoneidade só pode ser declarada pela autoridade competente;

22.10. As penalidades de multas recaem primeiro sobre o valor depositado a título de garantia contratual previsto no item 21, depois sobre os valores devidos ao licitante por conta do contrato e, por fim, deverão ser cobrados pela via judicial;

22.11. As penalidades de multa poderão ser cumuladas com as demais sanções, conforme determinação do Gestor do Contrato.

22.12. A aplicação de penalidade depende de prévio processo administrativo

23. LOCAL E DATA

Brasília/DF, 18/agosto/2020.

Identificação do Responsável pela elaboração do Elemento Técnico nº 17/2020:

Thiago de Lacerda Chaves

Chefe do Núcleo de Rede

00004166

Na atribuição de autoridade imediata superior responsável pela Superintendência de Tecnologia da Informação, APROVO e AUTORIZO o presente Elemento Técnico, em observância ao Art. 2º, §1º do Regulamento Próprio de Compras e Contratações do IGESDF.

Sergio Gustavo Evangelista da Mata

Gerente Geral de Tecnologia

00006880

24. ANEXO I - ENDEREÇOS DAS UNIDADES DO IGESDF

Local	Endereço
Hospital de Base – HBDF	SMHS - Área Especial, Q. 101 - Asa Sul, Brasília - DF, 70330-150
Hospital Regional de Santa Maria – HRSM	AC 102, Blocos, Conj. A/B/C - Santa Maria, Brasília - DF, 72502-100

UPA da Ceilândia	Área Especial D, Via P1 Norte - Ceilândia, Brasília - DF, 72225-270
UPA - Núcleo Bandeirante	DF-075, Km 180, Área Especial, EPNB, Brasília - DF, 71705-510
UPA Recanto das Emas	Quadra 400-600 s/n, Área Especial, Brasília - DF, 72630-250
UPA São Sebastião	QD 102 conj 1 LT 1, Residencial Oeste, São Sebastião
UPA Samambaia	QS 107 Conjunto 04 Área especial 01 – CEP: 72301-524
UPA Sobradinho	DF 420, em frente a AR 13, próximo ao COER Sobradinho II DF
PO700	SRTV 702, Via W5 Norte, Brasília - DF, 70723-0400
SIA	SIA TRECHO 17, RUA 06, LOTE 115 - SETOR DE INDÚSTRIA E ABASTECIMENTO/BRASÍLIA-DF

25. ANEXO II - PROPOSTA COMERCIAL

Ao _____ de _____do _____

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	SUB ITEM	DETALHAMENTO	UNIDADE	QTDE	PREÇO UNITÁRIO	PREÇO MENSAL	PREÇO ANUAL
		1.1	Infraestrutura como Serviço - Hiperconvergência, reservada por 1 ano *	Node/ Ano	5	R$	R$	R$
		1.2	Disponibilização de antivírus para servidores Windows e Linux	Servidor/Mês	150	R$	R$	R$
		1.3	Serviço de proteção de endpoints integrados com	Estação/Mês	10000	R$	R$	R$

			EDR *					
		1.4	Disponibilização de Next Generation Firewall em Alta Disponibilidade - TIPO 1	Unidade/Mês	2	R$	R$	R$
		1.5	Disponibilização de Next Generation Firewall em Alta Disponibilidade - TIPO 2	Unidade/Mês	13	R$	R$	R$
	1 - IaaS On-premises	1.6	Transceiver para Next Generation Firewall - TIPO 1	Unidade/Mês	30	R$	R$	R$
		1.7	Transceiver para Next Generation Firewall - TIPO 2	Unidade/Mês	30	R$	R$	R$
		1.8	Transceiver para Next Generation Firewall - TIPO 3	Unidade/Mês	30	R$	R$	R$
		1.9	Transceiver para Next Generation Firewall - TIPO 4	Unidade/Mês	30	R$	R$	R$
		1.10	Transceiver para Next Generation Firewall - TIPO 5	Unidade/Mês	30	R$	R$	R$
		1.11	Transceiver para Next Generation Firewall - TIPO 6	Unidade/Mês	30	R$	R$	R$
		1.12	Serviço de controle de acesso seguro a rede LAN e WLAN, reserva por 1 ano.	Instância 500 Usuários	5	R$	R$	R$
	ITEM	**SUB ITEM**	**DESCRIÇÃO DO SERVIÇO (POR RESERVA DE RECURSO)**	**UNIDADE**	**QTDE**	**PREÇO UNITÁRIO**	**PREÇO MENSAL**	**PREÇO ANUAL**
		2.1	Máquina virtual padrão - adquirida por meio de vCPU, reservada por 1 ano	Unidade de vCPU/hora		R$	R$	R$
		2.2	Máquina virtual padrão - adquirida por meio de memória, reservada por 1 ano	Gigabyte de memória/hora		R$	R$	R$
		2.3	Máquina virtual Windows - adquirida por meio de vCPU, reservada por 1 ano	Unidade de vCPU/hora		R$	R$	R$
		2.4	Máquina virtual Windows - adquirida por meio	Gigabyte de		R$	R$	R$

		2.4	de memória, reservada por 1 ano	memória/hora		R$	R$	R$
		2.5	Máquina virtual com serviço de hospedagem de container gerenciado - adquirida por meio de vCPU, reservada por 1 ano	Unidade de vCPU/hora		R$	R$	R$
		2.6	Máquina virtual padrão - adquirida por meio de vCPU (por demanda)	Unidade de vCPU/hora		R$	R$	R$
		2.7	Máquina virtual padrão - adquirida por meio de memória (por demanda)	Gigabyte de memória/hora		R$	R$	R$
		2.8	Máquina virtual Windows - adquirida por meio de vCPU (por demanda)	Unidade de vCPU/hora		R$	R$	R$
		2.9	Máquina virtual Windows - adquirida por meio de memória (por demanda)	Gigabyte de memória/hora		R$	R$	R$
		2.10	Serviço de armazenamento de blocos (SSD)	Gigabyte/mês		R$	R$	R$
		2.11	Serviço de armazenamento de blocos (HDD)	Gigabyte/mês		R$	R$	R$
1	**2 - IaaS Cloud Pública**	2.42	Serviço de armazenamento de objetos	Gigabyte/mês	1986000	R$	R$	R$
		2.13	Tráfego de saída da rede	Gigabyte/mês		R$	R$	R$
		2.14	Tráfego de rede do balanceador de carga	Gigabyte/mês		R$	R$	R$
		2.15	Tráfego de rede do CDN	Gigabyte/mês		R$	R$	R$
		2.16	Serviço de balanceamento de carga (*)	Unidade/hora		R$	R$	R$
		2.17	Serviço de balanceamento de carga utilizando gerenciador de tráfego (*)	DNS Queries Milhão/Mês		R$	R$	R$
		2.18	Porta de conexão de fibra 10Gbps	Unidade/hora		R$	R$	R$
		2.19	Serviço de DNS – Hospedagem de	Zona/mês		R$	R$	R$

	zonas						
2.20	Serviço de DNS – Consultas	Milheiro de consulta/mês		R$	R$	R$
2.21	Serviço de VPN	Gigabyte/Mês		R$	R$	R$
2.22	Serviço de VPN Gateway	Hora de Conexão		R$	R$	R$
2.23	Serviço Web Aplication Firewall adquirido por regra de ACL (**)	ACL/hora		R$	R$	R$
2.24	Serviço Web Aplication Firewall adquirido por hora (**)	Gateway/hora		R$	R$	R$
2.25	Serviço de Backup	Instância/mês		R$	R$	R$
2.26	Serviço de armazenamento de Backup	Gigabyte/mês		R$	R$	R$
2.27	Serviço de Autenticação (Integração com AD) adquirido por usuário (***)	Por usuário/Mês		R$	R$	R$
2.28	Serviço de Autenticação (Integração com AD) adquirido por mês (***)	Gigabyte/Mês		R$	R$	R$
2.29	Serviço de Auditoria e Análise de Logs	Gigabyte/Mês		R$	R$	R$
2.30	IP Público	Unidade/Mês		R$	R$	R$
2.31	Serviços de BI	Unidade/Mês		R$	R$	R$
2.32	Serviços de Plataforma de Gerencia para BI	Unidade/Mês		R$	R$	R$

ITEM	SUB ITEM	DETALHAMENTO	UNIDADE	QTDE	PREÇO UNITÁRIO	PREÇO MENSAL	PREÇO ANUAL
3 - Serviços de Cloud	3.1	Disponibilização de caixas postais e colaboração TIPO I	Usuário / mês	10000	R$	R$	R$
	3.2	Disponibilização de caixas postais e colaboração TIPO II	Usuário / mês	1500	R$	R$	R$

ITEM	SUB ITEM	DETALHAMENTO	UNIDADE	QTDE	PREÇO UNITÁRIO	PREÇO MENSAL	PREÇO ANUAL
4 - SaaS - Business Inteligence em Cloud	4.1	Serviço de fornecimento de software de análise de dados , reservado 1 ano	Servidor	1	R$	R$	R$
	4.2	Treinamentos direcionados de BI	Turma	2	R$	R$	R$
		Serviços					

		4.3	Especializados em Business Intelligence (BI).	Horas	1080	R$	R$	R$
	ITEM	**SUB ITEM**	**DETALHAMENTO**	**UNIDADE**	**QTDE**	**PREÇO UNITÁRIO**	**PREÇO MENSAL**	**PREÇO ANUAL**
	5 - Serviços Especializados.	5.1	Serviços de Monitoramento de infraestrutura IaaS, reservado 1 ano	Mensal	12	R$	R$	R$
		5.2	Serviços Especializados em IaaS.	Horas	25000	R$	R$	R$
		5.3	Serviços de Plataforma integrada (Managed Security Services), reservado 1 ano	Mensal	12	R$	R$	R$
		5.4	Serviço de scan de vulnerabilidades em Bases de dados, reservado 1 ano	Mensal	12	R$	R$	R$
		5.5	Serviço de pentest em redes corporativas, reservado 1 ano	Mensal	12	R$	R$	R$
		5.6	Serviço de provas de penetração em Aplicações, reservado 1 ano	Mensal	12	R$	R$	R$
		5.7	Serviço de penetração em Bases de dados (BD), reservado 1 ano	Mensal	12	R$	R$	R$
		5.8	Serviço gerenciado no Proactive Threat Hunting e serviços especializados em Cyberintelligence, reservado 1 ano	Mensal	12	R$	R$	R$

Valor Total Mensal	**R$**
Valor Total Anual	**R$**

a) Prazo de validade da proposta é de 90 (noventa) dias corridos, contados a partir da sua assinatura.

b) Declaramos estar cientes de todas as cláusulas do instrumento convocatório, bem como de seus anexos.

c) Apresentamos, conforme exigido no Ato Convocatório, os dados bancários para pagamento mediante depósito bancário em conta corrente, constando:

- Nome e número do Banco:
- Agência:
- Número da conta concorrente

d) 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

26. ANEXO III - ORDEM DE 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:	
E-mail:	_____@igesdf.org.br
Telefone:	(61) 3550-8900 **RAMAL:** 9236
Objeto:	Contratação de empresa especializada na prestação de serviços para provimento de infraestrutura de tecnologia nas modalidades on-premises, em cloud pública, serviços de cloud, SaaS, Segurança da Informação e Serviços Especializados para atendimento às demandas do IGESDF. Todos os itens contidos neste objeto deverão ser fornecidos na modalidade as a service, ou seja, como serviços, considerando o custo por hora dos ativos e recursos a serem suportados, conforme volumetria, arquitetura de infraestrutura e necessidades que porventura surgiremde computação em nuvem, disponibilização de solução contra ameaças digitais e serviço de mensageria e colaboração em nuvem distribuídos, necessários para garantir a operação dos serviços de TI do Instituto de Gestão Estratégica de Saúde do Distrito Federal – IGESDF.

LOTE	ITEM	SUB ITEM	DETALHAMENTO	UNIDADE	QTDE	PREÇO UNITÁRIO	PREÇO MENSAL	PREÇO ANUAL
	1 - IaaS On-premises	1.1	Infraestrutura como Serviço - Hiperconvergência, reservada por 1 ano *	Node/ Ano		R$	R$	R$
		1.2	Disponibilização de antivírus para servidores Windows e Linux	Servidor/Mês		R$	R$	R$
		1.3	Serviço de proteção de endpoints integrados com EDR *	Estação/Mês		R$	R$	R$
		1.4	Disponibilização de Next Generation Firewall em Alta Disponibilidade - TIPO 1	Unidade/Mês		R$	R$	R$
		1.5	Disponibilização de Next Generation Firewall em Alta Disponibilidade - TIPO 2	Unidade/Mês		R$	R$	R$
		1.6	Transceiver para Next Generation Firewall - TIPO 1	Unidade/Mês		R$	R$	R$
		1.7	Transceiver para Next Generation Firewall - TIPO 2	Unidade/Mês		R$	R$	R$
		1.8	Transceiver para Next Generation Firewall - TIPO 3	Unidade/Mês		R$	R$	R$

		1.9	Transceiver para Next Generation Firewall - TIPO 4	Unidade/Mês		R$	R$	R$
		1.10	Transceiver para Next Generation Firewall - TIPO 5	Unidade/Mês		R$	R$	R$
		1.11	Transceiver para Next Generation Firewall - TIPO 6	Unidade/Mês		R$	R$	R$
		1.12	Serviço de controle de acesso seguro a rede LAN e WLAN, reserva por 1 ano.	Instância 500 Usuários		R$	R$	R$
	ITEM	**SUB ITEM**	**DESCRIÇÃO DO SERVIÇO (POR RESERVA DE RECURSO)**	**UNIDADE**	**QTDE**	**PREÇO UNITÁRIO**	**PREÇO MENSAL**	**PREÇO ANUAL**
		2.1	Máquina virtual padrão - adquirida por meio de vCPU, reservada por 1 ano	Unidade de vCPU/hora		R$	R$	R$
		2.2	Máquina virtual padrão - adquirida por meio de memória, reservada por 1 ano	Gigabyte de memória/hora		R$	R$	R$
		2.3	Máquina virtual Windows - adquirida por meio de vCPU, reservada por 1 ano	Unidade de vCPU/hora		R$	R$	R$
		2.4	Máquina virtual Windows - adquirida por meio de memória, reservada por 1 ano	Gigabyte de memória/hora		R$	R$	R$
		2.5	Máquina virtual com serviço de hospedagem de container gerenciado - adquirida por meio de vCPU, reservada por 1 ano	Unidade de vCPU/hora		R$	R$	R$
		2.6	Máquina virtual padrão - adquirida por meio de vCPU (por demanda)	Unidade de vCPU/hora		R$	R$	R$
		2.7	Máquina virtual padrão - adquirida por meio de memória (por demanda)	Gigabyte de memória/hora		R$	R$	R$

1	**2 - IaaS Cloud Pública**	2.8	Máquina virtual Windows - adquirida por meio de vCPU (por demanda)	Unidade de vCPU/hora		R$	R$	R$
		2.9	Máquina virtual Windows - adquirida por meio de memória (por demanda)	Gigabyte de memória/hora		R$	R$	R$
		2.10	Serviço de armazenamento de blocos (SSD)	Gigabyte/mês		R$	R$	R$
		2.11	Serviço de armazenamento de blocos (HDD)	Gigabyte/mês		R$	R$	R$
		2.42	Serviço de armazenamento de objetos	Gigabyte/mês		R$	R$	R$
		2.13	Tráfego de saída da rede	Gigabyte/mês		R$	R$	R$
		2.14	Tráfego de rede do balanceador de carga	Gigabyte/mês		R$	R$	R$
		2.15	Tráfego de rede do CDN	Gigabyte/mês		R$	R$	R$
		2.16	Serviço de balanceamento de carga (*)	Unidade/hora		R$	R$	R$
		2.17	Serviço de balanceamento de carga utilizando gerenciador de tráfego (*)	DNS Queries Milhão/Mês		R$	R$	R$
		2.18	Porta de conexão de fibra 10Gbps	Unidade/hora		R$	R$	R$
		2.19	Serviço de DNS – Hospedagem de zonas	Zona/mês		R$	R$	R$
		2.20	Serviço de DNS – Consultas	Milheiro de consulta/mês		R$	R$	R$
		2.21	Serviço de VPN	Gigabyte/Mês		R$	R$	R$
		2.22	Serviço de VPN Gateway	Hora de Conexão		R$	R$	R$
		2.23	Serviço Web Aplication Firewall adquirido por regra de ACL (**)	ACL/hora		R$	R$	R$
		2.24	Serviço Web Aplication Firewall adquirido por hora (**)	Gateway/hora		R$	R$	R$
		2.25	Serviço de Backup	Instância/mês		R$	R$	R$
		2.26	Serviço de armazenamento de Backup	Gigabyte/mês		R$	R$	R$
			Serviço de Autenticação	Por				

	2.27	(Integração com AD) adquirido por usuário (***)	Por usuário/Mês		R$	R$	R$
	2.28	Serviço de Autenticação (Integração com AD) adquirido por mês (***)	Gigabyte/Mês		R$	R$	R$
	2.29	Serviço de Auditoria e Análise de Logs	Gigabyte/Mês		R$	R$	R$
	2.30	IP Público	Unidade/Mês		R$	R$	R$
	2.31	Serviços de BI	Unidade/Mês		R$	R$	R$
	2.32	Serviços de Plataforma de Gerencia para BI	Unidade/Mês		R$	R$	R$
ITEM	**SUB ITEM**	**DETALHAMENTO**	**UNIDADE**	**QTDE**	**PREÇO UNITÁRIO**	**PREÇO MENSAL**	**PREÇO ANUAL**
3 - Serviços de Cloud	3.1	Disponibilização de caixas postais e colaboração TIPO I	Usuário / mês		R$	R$	R$
	3.2	Disponibilização de caixas postais e colaboração TIPO II	Usuário / mês		R$	R$	R$
ITEM	**SUB ITEM**	**DETALHAMENTO**	**UNIDADE**	**QTDE**	**PREÇO UNITÁRIO**	**PREÇO MENSAL**	**PREÇO ANUAL**
4 - SaaS - Business Inteligence em Cloud	4.1	Serviço de fornecimento de software de análise de dados , reservado 1 ano	Servidor		R$	R$	R$
	4.2	Treinamentos direcionados de BI	Turma		R$	R$	R$
	4.3	Serviços Especializados em Business Intelligence (BI).	Horas		R$	R$	R$
ITEM	**SUB ITEM**	**DETALHAMENTO**	**UNIDADE**	**QTDE**	**PREÇO UNITÁRIO**	**PREÇO MENSAL**	**PREÇO ANUAL**
	5.1	Serviços de Monitoramento de infraestrutura IaaS, reservado 1 ano	Mensal		R$	R$	R$
	5.2	Serviços Especializados em IaaS.	Horas		R$	R$	R$
	5.3	Serviços de Plataforma integrada (Managed Security Services), reservado 1 ano	Mensal		R$	R$	R$
		Serviço de scan de					

		5.4	vulnerabilidades em Bases de dados, reservado 1 ano	Mensal		R$	R$	R$
	5 - Serviços Especializados.	5.5	Serviço de pentest em redes corporativas, reservado 1 ano	Mensal		R$	R$	R$
		5.6	Serviço de provas de penetração em Aplicações, reservado 1 ano	Mensal		R$	R$	R$
		5.7	Serviço de penetração em Bases de dados (BD), reservado 1 ano	Mensal		R$	R$	R$
		5.8	Serviço gerenciado no Proactive Threat Hunting e serviços especializados em Cyberintelligence, reservado 1 ano	Mensal		R$	R$	R$

ARTEFATOS / PRODUTOS	
A serem gerados e/ou atualizados	
ITEM 1 - IaaS On-primeses	Todos os relatórios de entrega, devem ser alinhados com a Gerencia de TI e Fiscal do Contrato
Item 2 - IaaS Cloud Pública	
Item 3 - Serviço de Cloud	
Item 4 - SaaS Business Inteligence em Cloud	
Item 5 - Serviços Especializados	

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 2020

Gestor de Contratos

27. ANEXO IV - 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 .

ITEM	Sub-Item	Descrição	Qntde.	Local de entrega
1				
2				
3				
4				
5				

Brasília, _____ de _____ de 20__.

_____

NOME:

Cargo:

Matrícula:

Documento assinado eletronicamente por **THIAGO DE LACERDA CHAVES - Matr.0000416-6**, **Chefe de Núcleo**, em 18/08/2020, às 18:00, 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 **SÉRGIO GUSTAVO EVANGELISTA DA MATA - Matr. 0000688-0**, **Gerente**, em 18/08/2020, às 18:38, 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= **45558271** código CRC= **DF36B2D8**.