ELEMENTO TÉCNICO Nº 02/2018

1. DO OBJETO

O objeto deste Elemento Técnico é a contratação de serviços para disponibilização de infraestrutura de Tecnologia da Informação, com o objetivo de garantir a operação dos serviços de TI do Instituto Hospital de Base - IHB, conforme tabela abaixo:

ITEM	DESCRIÇÃO
1	Infraestrutura como serviço - IaaS
2	Serviço de mensageria e colaboração em nuvem
3	Storage como serviço
4	Infraestrutura para nuvem privada/híbrida
5	Monitoramento e suporte técnico para LAN/WAN e infraestrutura nuvem privada/híbrida
6	Serviços de consultoria em IaaS
7	Disponibilização de software de GRC - Governança, Risco e Compliance
8	Serviços de consultoria em GRC - Governança, Risco e Compliance
9	Disponibilização de software de Gerenciamento de Chaves criptográficas
10	Disponibilização de solução de segurança contra ameaças digitais
11	Links de comunicação

2. DAS CARACTERÍSTICAS DO OBJETO

Para a prestação dos serviços, objeto do presente Elemento Técnica a CONTRATADA deverá atender às necessidades do Instituto Hospital de Base - IHB. Conforme catálogo de serviços, considerando o custo por hora dos ativos e recursos a serem suportados, conforme volumetria, arquitetura de infraestrutura e necessidades que por ventura surgirem.

3. DA JUSTIFICATIVA

Uma preocupação constante da alta direção das organizações é a busca pelo alinhamento estratégico entre a área de Tecnologia da Informação e a área de negócios da Instituição, com o objetivo de atender à demanda pela alta qualidade de seus serviços, economia, confiabilidade, flexibilidade, agilidade e racionalização de seus fluxos de trabalho.
A cada dia, as empresas necessitam automatizar seus processos operacionais e administrativos e para tanto, necessita confiar e a depender cada vez mais de sua infraestrutura tecnológica para viabilizar aplicações de missão crítica e implementar novas soluções que aumentem a agilidade, a capacidade de adaptação, a otimização de custos e a melhoria da qualidade dos serviços prestados aos seus clientes e usuários.
No cenário atual, a complexidade e os riscos inerentes ao ambiente tecnológico têm

gerado aumento nos custos, enquanto a satisfação dos usuários de tecnologia com o suporte e o tempo de resposta para a resolução dos problemas vem decrescendo. Tal constatação é presente, mas nas organizações em geral, tanto públicas quanto privadas.
Diante dessa realidade, é necessário que as áreas de TI das organizações mudem seu enfoque de atendimento aos usuários, de reativo para pró-ativo, alcançando um gerenciamento integrado dos processos envolvidos na entrega e suporte a serviços de tecnologia da informação.
Essa mudança se dá por meio do aumento da aderência das áreas de TI às melhores práticas de mercado, incrementando os processos de gestão dos serviços, aprimorando o controle sobre a infraestrutura tecnológica e implantando um Modelo de Governança Tecnológica que alcance o autogerenciamento e valorize as soluções sob a perspectiva de todas as áreas interessadas.
Esse Modelo de Governança Tecnológica e Gestão dos Serviços devem ser consolidados através da visão de futuro da organização, como base de orientação para a definição dos objetivos e metas estratégicas, que devem ser suportadas pelos serviços e pela infraestrutura de Tecnologia da Informação.
Esta demanda iniciou pelas organizações privadas, mas atualmente até as organizações públicas, tem adotado modelos de governança e de planejamento para as suas áreas de Tecnologia da Informação e Comunicação vem sendo exigida pelos Órgãos de Controle Federais.
O Instituto Hospital de Base - IHB foi instituído por meio do Decreto n° 38.332, de 13 de julho de 2017, obedecendo às cláusulas do contrato de Gestão com a Secretaria de Estado de Saúde do DF, deverá observar os seguintes pontos:

a) informatizar o IHB, na sua totalidade, contemplando toda a infraestrutura tecnológica em equipamentos, sistemas informatizados, migração do legado da Secretaria de Estado da Saúde - SES, suporte técnico, até que se consiga total independência de infraestrutura tecnologia da SES;

b) manter e aperfeiçoar sistemas de coletas e analises de dados relativos à qualidade e aos custos dos serviços prestados, desenvolvendo igualmente modelos estatísticos com base na análise destes dados e estudos comparativos de avaliação de desempenho das atividades profissionais desenvolvidas;

c) atender às demandas relativas à realização de estudos específicos e de incorporação tecnológica epropostas de normas técnicas, elaboração de protocolos e procedimentos, coleta e análise de dados, avaliação de tecnologias e técnicas terapêuticas, e formação de pessoal;

d) alimentar o Sistema de Informações ou qualquer sistema que venha a substituir os anteriores nos prazos previstos pela sua regulamentação, sem gerar créditos ou onerar o teto físico-financeiro de assistência distrital;

Com tal prerrogativa, faz-se necessária a contratação de serviços tecnológicos, através de uma solução abrangente, onde as disponibilizações dos serviços serão sob demanda, flexíveis e a forma de pagamento serão balizadas pelo efetivo serviço realizado.

4. CONDIÇOES DE PAGAMENTO

O pagamento será realizado em até 30 (trinta) dias corridos da certificação da Nota fiscal a entrega definitiva do software/serviço, atestada pela área técnica responsável.

5. VIGÊNCIA CONTRATUAL

O prazo de vigência será de 36 meses a partir da data da assinatura, podendo prorrogar-se por mais 24 meses.

6. DO CRONOGRAMA DE IMPLANTAÇÃO E DA MATRIZ DE RESPONSABILIDADE

ETAPA	EVENTO	PROGRAMAÇÃO	RESPONSÁVEL
1ª	Assinatura do Contrato	Dia "D"	CONTRATANTE e CONTRATADA
2ª	Reunião inicial para entrega do cronograma para início de instalação da solução	Até 5 (cinco) dias úteis após a assinatura do contrato	CONTRATANTE e CONTRATADA
3ª	Disponibilização da Solução	Até 45 (quarenta e cinco) dias corridos após a reunião inicial da entrega do projeto de instalação da solução	CONTRATADA
	Aceite provisório	No ato da implantação da solução	CONTRATANTE
4ª	Instalação e configuração da solução	**Início:** Até 45(quarenta e cinco) dias corridos após a instalação e configuração da solução **Fim:** Até 45 (quarenta e cinco) dias corridos contados do início da instalação	CONTRATADA
	Emitir termo de aceite definitivo	Até 30 dias corridos após a conclusão e homologação do serviço de instalação e configuração da solução	CONTRATANTE
5ª	Pagamento	Até 30 dias úteis, contados a partir do termo de aceite definitivo, configurando o término dos serviços e entrega da nota fiscal	CONTRATANTE
6ª	Disponibilização das demandas	Os serviços serão demandados e executados mediante emissão de Ordem de Serviço, após a instalação e configuração da solução	CONTRATANTE
7ª	Serviço de Suporte Operacional	Os serviços serão mensais demandados e executados via nuvem	CONTRATENTE E CONTRATADA

7. DA HABILITAÇÃO E QUALIFICAÇÃO TÉCNICA

Para fins de habilitação ao certame, os concorrentes terão de satisfazer os requisitos relativos à habilitação jurídica, qualificação técnica, qualificação econômico-financeira, regularidade fiscal e trabalhista e outras exigências complementares contidas neste Elemento Técnico, logo após a aceitação da proposta e será apresentado conforme descrito no Anexo III (Check List).

7.1. Relativa à Habilitação Jurídica:

a) Registro comercial, no caso de empresa individual;
b) Ato Constitutivo, Estatuto ou Contrato social em vigor, devidamente inscrito, em se tratando de sociedades empresárias e, quando for o caso, ata de eleição dos gestores;
c) Os documentos mencionados no subitem anterior deverão estar acompanhados de todas as alterações ou da consolidação respectiva;
d) Certidão de inscrição do Ato constitutivo, no caso de sociedades civis, acompanhada da ata de eleição da diretoria em exercício; e
e) Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País e ato de registro ou autorização para funcionamento, expedido pelo órgão competente, quando a atividade assim o exigir, além dos documentos previstos no art. 15 do Decreto nº 5.450/2005.

7.2 Relativa à Regularidade Fiscal:

a) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica - CNPJ;
b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
c) A prova de regularidade fiscal perante a Fazenda Nacional e à Dívida Ativa da União, mediante apresentação de certidão conjunta emitida pela Secretaria da Receita Federal (SRF) e Procuradoria-Geral da Fazenda Nacional (PGFN) com informações da situação do sujeito passivo quanto aos tributos administrados pela SRF e à Dívida Ativa da União;
d) Prova de regularidade para com a Fazenda Estadual e Municipal do domicílio ou sede da licitante, ou outra equivalente, na forma da Lei;
e) Prova de regularidade relativa à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei, mediante a apresentação de:
f) Certidão Negativa de Débito (CND), comprovando a inexistência de débito junto ao Instituto Nacional de Seguro Social – INSS, ou documento equivalente que comprove sua regularidade; e
g) Certificado de Regularidade de Situação perante o Fundo de Garantia do Tempo de Serviço – FGTS, ou documento equivalente, que comprove sua regularidade.

7.3 Relativa à Qualificação Econômico-Financeira:

a) Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da licitante, vedada a sua substituição por balancetes ou balanços provisórios,

podendo ser atualizados por índices oficiais quando encerrados há mais de 3 (três) meses da data de apresentação da proposta;

b) O licitante terá sua situação financeira avaliada, com base na obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), maiores que um (> 1), resultantes da aplicação das seguintes fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}};$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}};$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}; \text{ e}$$

c) As empresas que apresentarem resultado menor do que 01 (um) em qualquer um dos índices referidos no subitem anterior deverão comprovar que possuem patrimônio líquido mínimo, correspondente a 10% do valor total do(s) item(ns) considerado(s) vencedor(es).

d) O disposto no subitem anterior aplica-se, igualmente, quando não for possível a verificação dos índices por meio do SICAF.

e) O fornecedor registrado no SICAF terá sua situação financeira avaliada automaticamente pelo sistema, com base nas fórmulas acima.

f) Certidão Negativa de Falência ou Concordata (art.192, Lei nº 11.101/2005), 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, nos últimos cinco anos, contados da publicação do Elemento Técnico.

7.4 A habilitação jurídica, qualificação econômico-financeira, regularidade fiscal e trabalhista dos licitantes será verificada, online, no SICAF, após a análise, julgamento e aceitabilidade da proposta.

7.5. DA COMPROVAÇÃO DA QUALIFICAÇÃO TÉCNICA

7.5.1. Para comprovação da qualificação técnica deverão ser apresentados os seguintes documentos:

a) As empresas, relativamente à qualificação técnica, deverão apresentar atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado que comprove o fornecimento de:

a.1) Serviços de monitoramento, suporte técnico para LAN/WAN e infraestrutura;

a.2) Serviços de administração e suporte de servidores Windows e Linux,banco de dados, ferramenta de segurança da informação, correio eletrônico e colaboração.

a.3) Solução de segurança corporativa provendo proteção servidores, incluindo análise de vulnerabilidades, garantia de atualização contínua, instalação e configuração;

a.4) Serviços de consultoria em segurança contra ameaças digitais e

a.5) Suporte técnico on-site, disponibilizando Central de atendimento/serviços de TI nos padrões ITIL V3 e Infraestrutura como serviço - IaaS Serviço.

b) Os atestados deverão ser emitidos em papel timbrado e conter:
b.1) Razão Social, CNPJ e Endereço Completo da Empresa Emitente;
b.2) Razão Social da Contratada;
b.3) Número e vigência do contrato se for o caso;
b.4) Objeto do contrato;
b.5) Declaração de que foram atendidas as expectativas do cliente quanto ao cumprimento de cronogramas pactuados;
b.6) Local e Data de Emissão;
b.7) Identificação do responsável pela emissão do atestado, Cargo, Contato (telefone e correio eletrônico);
b.8) Assinatura do responsável pela emissão do atestado;
b.9) Devem ser originais ou autenticados, se cópias, e legíveis;
b.10) No caso de apresentação de atestado de empresas privadas, não serãoconsiderados aqueles apresentados por empresas participantes do mesmo grupo empresarial da contratada. Serão consideradas como de mesmo grupo, empresascontroladas pela contratada, ou que tenham pelo menos uma pessoa física ou jurídica que seja sócia da empresa emitente e da contratada.
b.11) Será aceito o somatório de atestados para comprovar a capacidade técnica e operacional, desde que reste demonstrada a execução concomitante dos contratos.

8. DOS CRITÉRIOS PARA ACEITAÇÃO DAS PROPOSTAS

8.1. A proposta de preços deverá conter o prazo de validade e planilha de custo, discriminando o custo unitário por item e o valor total dos serviços a serem executados no IHB.

8.2. A proposta deverá ser endereçada e enviada ao IHB, através do endereço eletrônico ***ihb.compras.servicos@gmail.com***, no prazo de até 02 (dois) dias úteis a partir da publicação do Ato Convocatório e deverá conter o CNPJ, endereço, responsável e telefone para contato.

8.3. Nos preços apresentados deverão estar incluídas todas as despesas com materiais, mão de obra, deslocamentos, hospedagens, ferramentas, equipamentos, seguros, taxas, tributos, incidências fiscais e contribuições de qualquer natureza ou espécie, encargos sociais, custos diretos e indiretos e quaisquer outros encargos, quando necessários à perfeita execução do objeto da presente solicitação.

9. DO CRITÉRIO DE JULGAMENTO DAS PROPOSTAS:

9.1. Atendidos todos os requisitos estabelecidos neste documento, será contratada a empresa que apresentar o **MENOR PREÇO GLOBAL**, e atenda as qualificações desta Especificação Técnica, nos termos do Regulamento de Compras e Contratações do IHB.

10. PRAZO DE VIGÊNCIA CONTRATUAL:

10.1 O prazo de vigência da contratação é de até 36 meses corridos, havendo a possibilidade de ser prorrogado posteriormente, mediante Termo Aditivo nos termos do Art. 29 do Regulamento Próprio de Compras e Contratações do Instituto Hospital de Base - IHB.

11. DO MODELO DE PLANILHA DE FORMAÇÃO DE PREÇOS E SERVIÇO

11.1 A proposta deverá ser apresentada conforme quadro demonstrativo abaixo:

ITEM	Descrição	Detalhamento	UNIDADE	QTDE.	PREÇO UNITÁRIO
1	Infraestrutura como serviço - IaaS	Instância Virtual 01	Instância/Mensal	2	
		Instância Virtual 02	Instância/Mensal	1	
		Tráfego de saída da nuvem pública	Gigabyte/ mês	5	
2	Serviço de mensageria e colaboração em nuvem	Disponibilização de caixas postais e colaboração	Usuário / mês	1.200	
		Serviços de migração	Horas	400	
3	Storage como serviço	-	TB/mês	2	
4	Infraestrutura para nuvem privada/híbrida	-	Mensal	36	
5	Monitoramento e suporte técnico para LAN/WAN e infraestrutura nuvem privada/híbrida	Serviço de monitoramento	Mensal	36	
		Serviço de Supervisão	Mensal	36	
		Serviço de administração e suporte à infraestrutura de produção	Mensal	36	

		Serviço de administração e suporte à infraestrutura de redes LAN e WAN	Mensal	36	
		Serviço de administração e suporte às ferramentas de mensageria e colaboração	Mensal	36	
		Serviço de administração e suporte às ferramentas de segurança da informação	Mensal	36	
		Serviço de administração e suporte às ferramentas de backup e restauração de dados	Mensal	36	
		-	Horas	1.200	
6	Serviços de consultoria em IaaS		Mensal	36	
7	Disponibilização de software de GRC - Governança, Risco e Compliance	Complexidade baixa	Horas	2.000	
8	Serviços de consultoria em GRC - Governança, Risco e Compliance	Complexidade média	Horas	2.500	
		Complexidade alta	Horas	1.500	
			Mensal	36	

9	Disponibilização de software de Gerenciamento de Chaves criptográficas	Disponibilização de Next Generation Firewall em Alta Disponibilidade	Mensal	36	
10	Disponibilização de solução de segurança contra ameaças digitais	Disponibilização de antivírus para caixas postais	Usuário/Mês	1.200	
		Disponibilização de antivírus para servidores Windows e Linux	Servidor/Mês	150	
		Disponibilização de antivírus para estações de trabalho Windows	Estação/Mês	1.200	
11	Links de comunicação		mensal	36	

11.2. O preço do valor total deverá ser expresso em numeral e por extenso.

12. DAS SANÇÕES ADMINISTRATIVAS

12.1 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 Hospital de Base - IHB.

13. DA REPACTUAÇÃO CONTRATUAL

13.1 Nos termos do Art. 34 do Regulamento Próprio de Compras e Contratações do Instituto Hospital de Base – IHB, o contrato poderá, mediante justificativa, nas mesmas condições contratuais ser aditados com acréscimos ou supressões que se fizerem nas obras, serviços ou compras até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

13.1.1 O contrato celebrado poderá ser revisado ou ajustado a qualquer momento com a finalidade de otimizar resultados em termos de qualidade e preço em compatibilidade com a realidade de mercado, desde que seja vantajoso para o IHB.

13.2 Nos termos do Art. 36 do Regulamento Próprio de Compras e Contratações do Instituto Hospital de Base – IHB, o contrato poderá ser revisado ou ajustado, unilateralmente, a qualquer momento para:
I - redução de valores;
II - revisão das quantidades, mediante justificativa, vedada a ampliação dos valores unitários;
III - ajuste de prazos de início de etapas de execução, de conclusão e de entrega, quando necessário, em razão de fatos supervenientes;
IV - ajuste do objeto por outros correlatos ou similares, mediante justificativa, quando for mais vantajoso para a gestão e operação das atividades;
V - reequilíbrio econômico-financeiro.

14. DA RESCISÃO CONTRATUAL

14.1 A rescisão do Contrato se dará nos termos Artigos 35 e 38 do Regulamento Próprio de Compras e Contratações do Instituto Hospital de Base.

15. DA FISCALIZAÇÃO

15.1 A fiscalização da prestação dos serviços será exercida pela Superintendência de Tecnologia da Informação da Contratante.

16. OBRIGAÇÕES DO CONTRATANTE

16.1. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta.

16.2. Exercer o acompanhamento e a fiscalização dos serviços, notificando a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção.

16.3. Pagar a Contratada o valor resultante da execução dos serviços, no prazo e condições estabelecidas no Contrato.

16.4; Emitir procuração específica com poderes para representá-lo nas ações que forem confiadas aos advogados da Contratada.

16.5. Fornecer todos os subsídios necessários ao desempenho da atividade da Contratada, encaminhando os documentos necessários à adequada realização dos serviços.

17. DO FORO

17.1 Fica eleito o foro da Circunscrição Judiciária de Brasília/DF para dirimir as dúvidas não solucionadas administrativamente, oriundas do cumprimento das obrigações estabelecidas.

Luciana Torres
Instituto Hospital de Base
Gerência de Gestão de Infraestrutura de TI

Autoridade Imediatamente Superior Responsável pela Aprovação do Elemento Técnico.

Renato Ricardo Alves
Instituto Hospital de Base
Superintendência de Tecnologia da Informação

De acordo.

AUTORIZO o presente Elemento Técnico, em conformidade com o Decreto n° 38.332, de 13 de julho de 2017, conforme autorização da Lei Distrital n° 5.899, de 3 de julho de 2017, tornando público que será realizada Seleção de Fornecedores do dispositivo Pedido de Cotação, observado o Regulamento Próprio de Compras e Contratações do Instituto Hospital de Base do Distrito Federal - IHBDF, publicado no DODF n° 231 de 05 de dezembro de 2017.

Encaminho-o para prosseguimento dos procedimentos necessários à contratação.

Ismael Alexandrino
Instituto Hospital de Base
Diretor – Presidente

ANEXO I

DO DETALHAMENTO DOS SERVIÇOS

1.1 DETALHAMENTO DOS SERVIÇOS DO ITEM 1INFRAESTRUTURA COMO SERVIÇO - IAAS

1.1.1 CARACTERÍSTICAS GERAIS

1.1.1.1 Disponibilizar infraestrutura em nuvem para alocação de servidores virtuais executando sistemas operacionais Windows Server 2016 e/ou Linux e espaço de armazenamento em nuvem.

1.1.1.2 A CONTRATADA deverá provisionar espaço em nuvem para armazenamento e execução de servidores virtuais, conforma tabela abaixo:

Serviços	Componentes	Unidade de Medida	Sistema Operacional
Instância Virtual 1	16vCPU 64GBRAM	vCPU/Mês vRAM/Mês	Microsoft Windows Server
Instância Virtual 2	32vCPU 64GBRAM	vCPU/Mês vRAM/Mês	Microsoft Windows Server

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

1.1.1.4 Para cada servidor provisionado deverá estar disponível uma área de no mínimo 100 GB de disco para carregar o sistema operacional da Instância Virtual (disco de boot);

1.1.1.5 Cada Instância Virtual poderá ter os seguintes sistemas operacionais:

1.1.1.5.1 Microsoft Windows Server (em versões suportadas pelo fabricante);

1.1.1.5.2 RedHat Linux (em versões suportadas pelo fabricante);

1.1.1.5.3 CentOS ou

1.1.1.5.4 Ubuntu.

1.1.1.5.5 A CONTRATANTE indicará para cada provisionamento se a licença do sistema operacional será fornecida por ela ou pela CONTRATADA;

1.1.1.5.6 Servidores/VM’s com diversas configurações de CPU, RAM e disco de acordo com a necessidade.

1.1.1.5.7 Tráfego de saída da rede.

1.2 DETALHAMENTO DOS SERVIÇOS DO ITEM 2 - SERVIÇO DE MENSAGERIA E COLABORAÇÃO

1.2.1 Solução integrada de colaboração e comunicação corporativa baseada em nuvem, com garantia e suporte técnico por 36 (trinta e seis) meses, compreendendo os serviços de correio eletrônico (webmail), comunicação instantânea (chat), videoconferência por envio de vídeo ponto a ponto, armazenamento e compartilhamento de arquivos;

1.2.2 A CONTRATANTE se compromete a iniciar a utilização com 1.200 caixas postais, podendo aumentar a demanda conforme necessidade;

1.2.3 A seguir são especificados os requisitos técnicos gerais para a solução em nuvem:

1.2.3.1 A solução de colaboração em nuvem deverá atender a todos os usuários simultaneamente.

1.2.3.2 A solução deverá contemplar, caso necessário, o fornecimento de todos os softwares envolvidos, sejam eles na condição de servidor ou cliente, atualizações de versões, garantia e suporte por 36 (trinta e seis) meses.

1.2.3.3 A CONTRATADA deverá disponibilizar, sem qualquer ônus financeiro adicional, clientes da solução para smartphones e tablets que possuam os sistemas operacionais Android 4 e IOS 5, ou superiores, instalados.

1.2.3.4 A solução deverá proporcionar disponibilidade, integridade, confidencialidade, autenticidade e segurança de todas as informações do CONTRATANTE.

1.2.3.5 Os dados armazenados pela CONTRATADA serão usados apenas para fornecer os serviços de computação em nuvem e não poderão ser utilizados para qualquer outro fim.

1.2.3.6 A solução deverá possuir desempenho suficiente para atender a quantidade total de usuários, dados e transações demandados, sem degradação até o limite de utilização da capacidade máxima dos serviços contratados.

1.2.3.7 Os dados do CONTRATANTE deverão estar fisicamente armazenados nas dependências de dois ou mais centros de processamento de dados.

1.2.3.8 Obrigatoriamente a solução deve contemplar redundância de dados e serviços.

1.2.3.9 Os serviços prestados deverão estar obrigatoriamente certificados na norma ISO 27001 e, adicionalmente, em uma das normas internacionais: SAS 70 ou SSAE 16 ou ISAE 3402, podendo o CONTRATANTE exigir a apresentação do certificado a qualquer momento da vigência do contrato.

1.2.3.10 Os dados do CONTRATANTE serão armazenados com garantia de criptografia de, pelo menos, 128 (cento e vinte e oito) bits.

1.2.3.11 Suportar autenticação dos usuários em serviços de diretório LDAP, abrangendo, pelo menos, a tecnologia do Microsoft Active Directory.

1.2.3.12 Os clientes, plugins ou quaisquer softwares que necessitem ser instalados na infraestrutura das estações de trabalho do CONTRATANTE devem ser compatíveis com a plataforma Microsoft Windows 7 ou superior. O cliente da solução de colaboração, se necessário, deverá ser fornecido como parte integrante da solução, sem qualquer custo adicional.

1.2.3.13 No término ou na rescisão do contrato, o CONTRATANTE poderá extrair seus dados, autorizando posterior e formalmente, no prazo de 30 dias, a exclusão dos mesmos pela CONTRATADA.

1.2.3.14 Permitir a exportação dos dados referentes aos componentes de e-mail e compartilhamento de arquivos, de forma a viabilizar a migração para as soluções em nuvem Google Apps for Business e Microsoft Office 365 e IBM SmartCloud, pelo menos.

1.2.3.15 Os componentes da solução deverão ser desenvolvidos pelo mesmo fabricante, com a finalidade de garantir a integração entre os componentes.

1.2.3.16 Disponibilizar mecanismos de auditoria que permitam registrar as atividades dos administradores nos componentes da solução.

1.2.4 A seguir são especificados os requisitos técnicos para o correio eletrônico, componentes da solução:

1.2.4.1 Detectar e remover vírus ou spans em e-mails de entrada e saída de qualquer origem automaticamente.

1.2.4.2 Utilização de recursos especiais (agendamento de salas de reunião ou equipamentos) sem qualquer custo financeiro adicional.

1.2.4.3 O acesso aos serviços deverá ocorrer a partir dos navegadores listados abaixo, preferencialmente, sem a instalação de aplicativos nos clientes:

1.2.4.3.1 Internet Explorer;

1.2.4.3.2 Firefox;

1.2.4.3.3 Chrome;

1.2.4.3.4 Safari.

1.2.4.4 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.

1.2.4.5 O componente de correio da solução não deverá restringir o envio e o recebimento de anexos inferiores a 20MB (vinte megabytes).

1.2.4.6 Os endereços eletrônicos das contas de e-mail deverão conter obrigatoriamente o domínio do CONTRATANTE (alias@dominio.com.br – ex.: xyz@dominio.com.br).

1.2.4.7 Permitir a abertura simultânea de mais de uma caixa postal pelo mesmo usuário no mesmo computador ou dispositivo móvel.

1.2.4.8 Disponibilizar mecanismos de auditoria que permitam registrar as atividades de acesso à conta, deleção de conteúdo, envio e recebimento de mensagens dos usuários.

1.2.4.9 Todos os registros de auditoria devem permanecer disponíveis ao CONTRATANTE por, pelo menos 7 (sete) dias corridos.

1.2.4.10 Não permitir, sob qualquer hipótese, que os registros de auditoria sejam alterados ou excluídos.

1.2.4.11 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”.

1.2.4.12 A CONTRATADA deverá comprovar as políticas de auditorias periódicas permanentes, quando solicitadas pelo CONTRATANTE.

1.2.4.13 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.

1.2.4.14 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.

1.2.4.15 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.

1.2.4.16 Fornecer de maneira integrada mecanismos de inspeção, filtro e remoção de mensagens indesejadas (spans) ou contaminadas com “malwares”.

1.2.4.17 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.

1.2.4.18 Retenção de mensagens/itens apagados por, no mínimo 30 (trinta) dias, com opção de restauração a ser executada pelo próprio usuário.

1.2.4.19 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.

1.2.4.20 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.

1.2.4.21 Permitir que um usuário do componente de correio da solução tenha 2 (dois) ou mais alias de e-mail.

1.2.4.22 Suportar o envio de mensagens assinadas e criptografadas digitalmente, via protocolo S/MIME.

1.2.4.23 Permitir a configuração das caixas de correio para aceitar ou rejeitar e-mails enviados de usuários específicos.

1.2.4.24 Oferecer a possibilidade de assinar digitalmente as mensagens com certificados digitais ICP Brasil do tipo A3 via clientes de e-mail ou browsers.

1.2.4.25 Permitir a delegação da administração do componente de correio da solução para usuários não administradores do domínio.

1.2.4.26 Suportar criação de listas de distribuição de e-mail dinâmicas.

1.2.4.27 Possuir catálogo de endereços centralizado.

1.2.4.28 Possuir console de administração centralizada.

1.2.4.29 Permitir a criação de contatos de e-mails externos no catálogo de endereços.

1.2.4.30 Incluir ferramentas administrativas que possam ser executadas em browsers e permitir a administração remota do componente de correio da solução.

1.2.4.31 As conexões ao componente de correio da solução por meio de dispositivos móveis devem ser realizadas, obrigatoriamente, via SSL.

1.2.4.32 Permitir controlar, em níveis amplos e granulares, o que administradores e usuários finais podem fazer.

1.2.4.33 Fornecer aos usuários a possibilidade de delegar acesso de seus recursos a outros usuários, controlando o nível de permissões que será concedido.

1.2.4.34 O componente de correio da solução deverá ter seu ambiente de usuário em idioma português do Brasil e suportar a acessibilidade no mesmo idioma.

1.2.4.35 Ser acessível através de web browsers e por cliente de desktop (MUA – Mail User Agent).

1.2.4.36 Possuir Webmail acessível através de tablets e smartphones,preservando funcionalidades de acesso compatíveis aos dos browsers.

1.2.4.37 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.

1.2.4.38 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.

1.2.4.39 Procurar horário livre na agenda de todos os participantes da reunião e com base na pesquisa sugerir horário para a reunião automaticamente.

1.2.4.40 Enviar e-mail aos participantes da reunião, solicitando confirmação de presença.

1.2.4.41 Assistente de ausência temporária com encaminhamento automática de e-mail.

1.2.4.42 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.

1.2.4.43 Disponibilizar espaço de armazenamento de e-mails de, no mínimo, 50GB (cinquenta gigabytes) por usuário.

1.2.5 A seguir são especificados os requisitos técnicos para o componente de comunicação colaborativa da solução:

1.2.5.1 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.

1.2.5.2 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.

1.2.5.3 Suportar, pelo menos, a utilização de vídeo em definição padrão (standard definition) no envio de vídeo ponto-a-ponto.

1.2.5.4 Suportar a exibição simultânea de apresentação colaborativa, videochamada ponto-a-ponto e chat multiponto entre os participantes de uma sessão colaborativa.

1.2.5.5 Permitir o compartilhamento da tela do usuário apresentador e dos convidados durante uma sessão de colaboração.

1.2.5.6 Permitir o compartilhamento de uma aplicação do computador do apresentador ou de um convidado durante uma sessão de colaboração.

1.2.5.7 Permitir a comunicação de áudio ponto-a-ponto durante sessão de colaboração.

1.2.5.8 Propiciar que o apresentador possa controlar quem são os participantes da reunião, especificando permissões de transmitir conteúdo durante a sessão de colaboração.

1.2.5.9 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.

1.2.5.10 Propiciar a troca de mensagens instantâneas com múltiplos usuários em uma única sessão.

1.2.5.11 Fornecer recurso de troca de mensagens instantâneas entre os usuários. Todo o texto transmitido durante a conversação deve ser criptografado.

1.2.5.12 Permitir o uso de foto pessoal para cada usuário.

1.2.5.13 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.

1.2.5.14 Possuir mecanismos que permitam registrar a comunicação efetuada através da plataforma para posterior rastreabilidade.

1.2.6 A seguir são especificados os requisitos técnicos para o componente de compartilhamento e armazenamento de arquivos da solução:

1.2.6.1 Permitir aos usuários armazenar e compartilhar arquivos, documentos, planilhas, apresentações, imagens, em especial nos seguintes formatos:

1.2.6.1.1 Documentos: Microsoft Office Word, BR Office/LibreOffice Writer e PDF.

1.2.6.1.2 Planilhas: Microsoft Office Excel e BR Office/LibreOffice Calc.

1.2.6.1.3 Apresentações: Microsoft Office PowerPoint e BR Office/LibreOffice Impress.

1.2.6.1.4 Imagens: BPM, JPEG, GIF, TIFF e PNG.

1.2.6.2 Permitir a sincronização automática de arquivos armazenados localmente no computador dos usuários do CONTRATANTE com os arquivos armazenados no componente.

1.2.6.3 Permitir aos usuários controlar as permissões de acessos a suas pastas e arquivos.

1.2.6.4 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.

1.2.6.5 Permitir a criação de documentos de texto, planilhas e apresentações, inclusive com a colaboração em tempo real.

1.2.6.6 Possibilitar o compartilhamento dos documentos para edição ou somente leitura.

1.2.6.7 Viabilizar a restrição de compartilhamento de arquivos para usuários externos ao ambiente, possibilitando a concessão de acesso somente a usuários internos.

1.2.6.8 Possibilitar o trabalho offline para sincronização posterior dos arquivos.

1.2.6.9 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.

1.2.6.10 Disponibilizar mecanismos de auditoria que permitam registrar as atividades de acesso, deleção ou alteração de conteúdo dos usuários.

1.2.7 Serviço de migração do conteúdo de caixas postais do sistema de correio eletrônico atual para a solução contratada.

1.2.7.1 Os serviços de migração serão divididos em lotes. Os lotes serão compostos de caixas postais, cujas quantidades e critérios serão definidos pelo CONTRATANTE no PROJETO EXECUTIVO.

1.2.7.2 A CONTRATADA deverá prover configuração e migração do sistema de correio eletrônico e das caixas postais do sistema atual, conforme PROJETO EXECUTIVO contemplando a quantidade de horas necessárias para execução destes serviços aprovado pelo CONTRATANTE.

1.3 DETALHAMENTO DO SERVIÇOS DO ITEM 3 - STORAGE COMO SERVIÇO

1.3.1 CARACTERÍSTICAS GERAIS

1.3.1.1 A CONTRATADA deverá fornecer espaço em nuvem em storage com disponibilidade que atenda os Níveis de Serviço deste projeto;

1.3.1.2 O storage deve estar disponível para acesso pelos servidores provisionados na nuvem privada e híbrida.

1.4 DETALHAMENTO DOS SERVIÇOS DO ITEM 4- INFRAESTRUTURA PARA NUVEM PRIVADA/HIBRIDA

1.4.1 Disponibilizar infraestrutura para nuvem privada e híbrida e serviços de consultoria, monitoramento e suporte técnico.

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

1.4.3 A CONTRATADA deverá fornecer *hypervisor* para toda a solução de Hiperconvergência;

1.4.4 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.

1.4.5 ESPECIFICAÇÕES DO HARDWARE

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

1.4.5.2 O cluster deve ser composto por um mínimo de 3 (três) nós (servidores de rede);

1.4.5.3 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

1.4.5.4 Cache de no mínimo 800GB;

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

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

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

1.4.6 ESPECIFICAÇÃO FUNCIONAL DA SOLUÇÃO HIPERCONVERGENTE

1.4.6.1 A solução deverá prover uma estrutura hiperconvergente de alta disponibilidade em configuração de cluster para ambiente de virtualização composta de 4 (quatro) servidores físicos (nós), cada qual com sua respectiva capacidade de processamento, armazenamento e comunicação de rede.

1.4.6.2 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;

1.4.6.3 Permitir adição de um nó por vez;

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

1.4.6.5 Permitir remover nós do cluster sem parada no ambiente;

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

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

1.4.6.8 Suporte a Hypervisor *VMware ESX 6.5*

1.4.6.9 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:

1.4.6.9.1 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;

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

1.4.6.9.3 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).

1.4.6.10 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;

1.4.6.11 Deverá suportar a troca dos discos sem parada dos servidores;

1.4.6.12 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;

1.4.6.13 Deve possuir criptografia através de discos específicos ou software;

1.4.6.14 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;

1.4.6.15 A solução deve manter os dados das VMsespalhados 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

1.4.6.16 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;

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

1.4.6.18 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;

1.4.6.19 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;

1.4.6.20 A solução deve suportar, via software, desduplicaçãoe compressão de dados;

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

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

1.4.6.23 A funcionalidade de replicação da solução deve suportar:

1.4.6.23.1 Replicação Síncrona para as 5 principais VMw por nó;

1.4.6.23.2 Replicação Assíncrona com recuperação de até 15 minutos para as demais VMs;

1.4.6.23.3 Proteção de Dados Contínua (CDP) para as 2 VMs principais por nó;

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

1.4.6.25 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;

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

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

1.4.6.28 A console WEB deve permitir integração com Active DIrectory da Microsoft para autenticação, ou então, utilizar autenticação local;

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

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

1.4.6.31 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;

1.4.6.32 A console WEB deve fornecer acesso à, no mínimo, as seguintes opções:

1.4.6.32.1 Dashboard principal;

1.4.6.32.2 Dashboard da saúde do Sistema (cluster);

1.4.6.32.3 Dashboard das Máquinas Virtuais;

1.4.6.32.4 Dashboard do Storage;

1.4.6.32.5 Dashboard do Hardware;

1.4.6.32.6 Dashboard de Recuperação de Desastres;

1.4.6.32.7 Dashboard de Análise de Performance;

1.4.6.32.8 Dashboard de Alertas e Eventos;

1.4.6.33 A solução deve suportar o envio de alertas críticos automaticamente para o fabricante da solução;

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

1.4.6.34.1 Sumário do hypervisor;

1.4.6.34.2 Sumário do hardware;

1.4.6.34.3 IOPS do cluster;

1.4.6.34.4 Utilização de banda do cluster;

1.4.6.34.5 Latência do cluster;

1.4.6.34.6 Situação da resiliência dos dados;

1.4.6.34.7 Alertas e eventos.

1.4.6.35 Deve suportar envio de alertas e eventos via SNMP;

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

1.4.6.37 Deverá integrar ou utilizar nativamenteovCenter e executar ações como:

1.4.6.37.1 Criação de VMs;

1.4.6.37.2 Leitura das VMs;

1.4.6.37.3 Atualização das características da VM;

1.4.6.37.4 Deletar VMs;

1.4.6.37.5 Plataforma ofertada deve possuir integração com:

1.4.6.38 *vRealize Automation*

1.5 DETALHAMENTO DOS SERVIÇOS DO ITEM 5 - MONITORAMENTO E SUPORTE TÉCNICO PARA LAN/WAN E INFRAESTRUTURA NUVEM PRIVADA/HÍBRIDA

1.5.1 CARACTERÍSTICAS GERAIS

1.5.1.1 Os serviços de serão prestados no ambiente da CONTRATANTE;

1.5.1.2 A CONTRATADA deverá prover os serviços de suporte técnico em regime 24x7x365 que atendam os níveis de serviços.

1.5.1.3 Os serviços serão organizados nos subitens abaixo:

1.5.1.3.1 Serviço de monitoramento;

1.5.1.3.2 Serviço de Supervisão;

1.5.1.3.3 Serviço de administração e suporte à infraestrutura de produção;

1.5.1.3.4 Serviço de administração e suporte à infraestrutura de redes LAN e WAN;

1.5.1.3.5 Serviço de administração e suporte à infraestrutura de banco de dados;

1.5.1.3.6 Serviço de administração e suporte às ferramentas de mensageria e colaboração;

1.5.1.3.7 Serviço de administração e suporte às ferramentas de segurança da informação;

1.5.1.3.8 Serviço de administração e suporte às ferramentas de backup e restauração de dados.

1.5.2 SERVIÇO DE MONITORAMENTO

1.5.2.1 Ao contratar o serviço, por intermédio de emissão de Ordem de Serviço, a CONTRATANTE irá demandar, no mínimo, 36 (trinta e seis) meses de execução.

1.5.2.2 A CONTRATADA deverá monitorar toda a infraestrutura disponibilizada em nuvem em regime de 24x7x365;

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

1.5.2.4 O monitoramento deve ocorrer nas instalações da CONTRATADA;

1.5.2.5 A CONTRATADA deverá tratar todos os eventos da infraestrutura e identificar quais eventos são incidentes;

1.5.2.6 A equipe de monitoramento irá executar procedimentos operacionais indicados pela CONTRATANTE visando a resolução de incidentes;

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

1.5.2.8 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;

1.5.2.9 A CONTRATANTE irá indicar quais são os caminhos para escalonamento dos chamados;

1.5.3 SERVIÇO DE SUPERVISÃO

1.5.3.1 O profissional deste serviço não precisa ficar alocado nas dependências da CONTRATANTE por todo o horário de serviço;

1.5.3.2 Ao contratar o serviço, por intermédio de emissão de Ordem de Serviço, a CONTRATANTE irá demandar, no mínimo, 36 (trinta e seis) meses de execução.

1.5.3.3 Responsável por verificarse as tarefas estão sendo executadas de acordo com os níveis de serviço contratados;

1.5.3.4 Responsável pela interação com o gestor e fiscais de contrato da CONTRATANTE, comunicando expectativas, problemas, prioridades e atividades;

1.5.3.5 Deve organizar e controlar turnos de trabalhos;

1.5.3.6 Deve assistir sob todos os aspectos o contingente alocado, orientando, coordenando, acompanhando, supervisionando, gerenciando e dando ordens às equipes técnicas que atuam no ambiente CONTRATANTE para a execução dos serviços;

1.5.3.7 Deve controlar processos, atividades e a qualidade dos serviços prestados, realizando planejamento e controle da execução dos serviços;

1.5.3.8 Deve apresentar propostas de mudanças nas rotinas e procedimentos técnicos visando a otimização dos custos, a racionalização, inovação, e melhoria dos processos;

1.5.3.9 Deve zelar pela segurança da informação;

1.5.3.10 Deve responder aos questionamentos e solicitações da CONTRATANTE;

1.5.3.11 Deve participar de reuniões relativas às atividades sob sua gestão, quando solicitado pela CONTRATANTE;

1.5.3.12 Deve acompanhar, avaliar e validar os resultados das atividades sob sua gestão;

1.5.3.13 Deve assegurar que a prestação dos serviços obedeça aos processos e políticas de segurança adotadas na CONTRATANTE.

1.5.4 SERVIÇO DE ADMINISTRAÇÃO E SUPORTE À INFRAESTRUTURA DE PRODUÇÃO

1.5.4.1 Ao contratar o serviço, por intermédio de emissão de Ordem de Serviço, a CONTRATANTE irá demandar, no mínimo, 36 (trinta e seis) meses de execução.

1.5.4.2 O dimensionamento da equipe necessária à execução das tarefas é de responsabilidade da CONTRATADA, que deverá, durante toda a execução do Contrato, atender os níveis de serviços e todos os perfis profissionais exigidos neste Elemento Técnico e seus anexos;

1.5.4.3 Os serviços contemplam a administração e suporte a infraestrutura de produção, compreendendo, no mínimo, as seguintes atividades:

1.5.4.3.1 Instalar, atualizar, configurar, customizar e suportar todos os servidores físicos e virtuais, sistemas operacionais, sistemas de armazenamento e sistemas de virtualização em todos os ambientes da CONTRATANTE (nuvem pública e privada);

1.5.4.3.2 Montar procedimentos de correção de falhas que serão adotados pela equipe

de monitoramento;

1.5.4.3.3 Prestar suporte à equipe do NOC da CONTRATANTE em caso de falhas nos ativos de rede;

1.5.4.3.4 Acompanhar chamados técnicos nos fabricantes das soluções instaladas;

1.5.4.3.5 Prover suporte técnico durante a instalação e configuração dos softwares em uso na CONTRATANTE;

1.5.4.3.6 Configurar o ambiente de virtualização: switches virtuais, servidores de virtualização, alta-disponibilidade, pool de recursos e quaisquer outras funcionalidades disponíveis no ambiente de virtualização;

1.5.4.3.7 Elaborar projetos de melhorias do ambiente de virtualização

1.5.4.3.8 Acompanhar o uso de recursos físicos pelo ambiente de virtualização, agindo proativamente, antes do esgotamento de recursos físicos;

1.5.4.3.9 Realizar mudanças de configuração, novas configurações, novas implantações e todas as atividades necessárias, nos ambientes suportados, de modo a atender plenamente os serviços de TI da CONTRATANTE;

1.5.4.3.10 Diagnosticar e resolver problemas de desempenho nos ambientes suportados;

1.5.4.3.11 Projetar, implantar e validar políticas de alta-disponibilidade de dados;

1.5.4.3.12 Alertar a CONTRATANTE, de forma proativa, sobre qualquer problema, anormalidade, falta de recursos ou comportamento não previsto que possam causar impactos nos serviços de TI

1.5.5 SERVIÇO DE ADMINISTRAÇÃO E SUPORTE À INFRAESTRUTURA DE REDES LAN E WAN

1.5.5.1 Ao contratar o serviço, por intermédio de emissão de Ordem de Serviço, a CONTRATANTE irá demandar, no mínimo, 36 (trinta e seis) meses de execução.

1.5.5.2 O dimensionamento da equipe necessária à execução das tarefas é de responsabilidade da contratada, que deverá, durante toda a execução do Contrato, atender os níveis de serviços e todos os perfis profissionais exigidos neste Elemento Técnico e seus anexos;

1.5.5.3 Os serviços contemplam a administração e suporte a infraestrutura de redes LAN e WAN, compreendendo, no mínimo, as seguintes atividades:

1.5.5.3.1 Instalar, atualizar, configurar, customizar e suportar todos os switches, roteadores e demais ativos de rede em uso, e que venham a ser adquiridos pela CONTRATANTE;

1.5.5.3.2 Administrar e suportar todos os serviços de redes, tais como, DNS, DHCP, switches virtuais, serviços de autenticação e demais serviços de suporte à conectividade dos usuários e clientes;

1.5.5.3.3 Prestar suporte à equipe do NOC da CONTRATANTE em caso de falhas nos

serviços e ativos de rede;

1.5.5.3.4 Acompanhar chamados técnicos nos fabricantes das soluções instaladas;

1.5.5.3.5 Configurar o ambiente de conectividade virtual: switches virtuais, alta-disponibilidade e quaisquer outras funcionalidades de conectividade disponíveis no ambiente de virtualização;

1.5.5.3.6 Realizar mudanças de configuração, novas configurações, novas implantações e todas as atividades necessárias nos ativos de rede da CONTRATANTE para suportar corretamente os serviços de TI;

1.5.5.3.7 Diagnosticar e resolver problemas de desempenho nos ativos de rede;

1.5.5.3.8 Organizar racks, cabos, servidores, ferramentas e toda demais infraestrutura do Datacenter;

1.5.5.3.9 Executar a movimentação de ativos de rede do Datacenter;

1.5.5.3.10 Elaborar e implantar projetos de estrutura física e lógica das redes LAN e WAN, com ou sem fio, garantindo desempenho, disponibilidade e segurança;

1.5.5.3.11 Projetar, implantar e validar políticas de alta-disponibilidade de dados;

1.5.5.3.12 Administrar todas as funcionalidades dos ativos e serviços de rede utilizados na CONTRATANTE;

1.5.5.3.13 Alertar a CONTRATANTE, de forma proativa, sobre qualquer problema, anormalidade, falta de recursos ou comportamento não previsto que possam causar impactos nos serviços de TI

1.5.6 SERVIÇO DE ADMINISTRAÇÃO E SUPORTE ÀS FERRAMENTAS DE MENSAGERIA E COLABORAÇÃO

1.5.6.1 Ao contratar o serviço, por intermédio de emissão de Ordem de Serviço, a CONTRATANTE irá demandar, no mínimo, 36 (trinta e seis) meses de execução.

1.5.6.2 O dimensionamento da equipe necessária à execução das tarefas é de responsabilidade da contratada, que deverá, durante toda a execução do Contrato, atender os níveis de serviços e todos os perfis profissionais exigidos neste Elemento Técnico e seus anexos;

1.5.6.3 Os serviços contemplam a administração e suporte às ferramentas de mensageria e colaboração, compreendendo, no mínimo, as seguintes atividades:

1.5.6.3.1 Os serviços de mensageria compreendem correio eletrônico, videoconferência e ferramenta de comunicação instantânea.

1.5.6.3.2 Instalar, atualizar, configurar, customizar e suportar todos os servidores de mensageria em uso na CONTRATANTE;

1.5.6.3.3 Gerenciar as políticas de acesso às contas de e-mail e serviços de

mensageria;

1.5.6.3.4 Avaliar o correto funcionamento da rotina de backup e restore do serviço de correio eletrônico;

1.5.6.3.5 Manter a integração do serviço de correio eletrônico com as demais ferramentas computacionais utilizadas pela Agência;

1.5.6.3.6 Administrar e manter os serviços de mensageria e colaboração;

1.5.6.3.7 Gerenciar os usuários, permissões, arquivos e políticas de backup dos sistemas de mensageria e colaboração;

1.5.6.3.8 Alertar a CONTRATANTE, de forma proativa, sobre qualquer problema, anormalidade, falta de recursos ou comportamento não previsto que possam causar impactos nos serviços de TI.

1.5.7 SERVIÇO DE ADMINISTRAÇÃO E SUPORTE ÀS FERRAMENTAS DE SEGURANÇA DA INFORMAÇÃO

1.5.7.1 Ao contratar o serviço, por intermédio de emissão de Ordem de Serviço, a CONTRATANTE irá demandar, no mínimo, 36 (trinta e seis) meses de execução.

1.5.7.2 O dimensionamento da equipe necessária à execução das tarefas é de responsabilidade da contratada, que deverá, durante toda a execução do Contrato, atender os níveis de serviços e todos os perfis profissionais exigidos neste Elemento Técnico e seus anexos;

1.5.7.3 Os serviços contemplam administração e suporte às ferramentas de segurança da informação, compreendendo, no mínimo, as seguintes atividades:

1.5.7.3.1 Definir, gerenciar, implementar, implantar, documentar e revisar a política de segurança da informação;

1.5.7.3.2 Instalar, atualizar, configurar, administrar e suportar todos os servidores, appliances e softwares que compõe os serviços de segurança da CONTRATANTE.

1.5.7.3.3 Manter todas as soluções de segurança atualizadas;

1.5.7.3.4 Consolidar os relatórios de vírus, ataques, vulnerabilidades, intrusões, regras de acesso e outros referentes a segurança para apresentação à CONTRATANTE, incluindo medidas tomadas e sugestões de ações preventivas;

1.5.7.3.5 Gerenciar projetos de implantação, substituição e atualização de soluções destinadas à segurança;

1.5.7.3.6 Apoiar a elaboração e manutenção do plano de contingência;

1.5.7.3.7 Apoiar a elaboração e manutenção do plano de gerenciamento de risco;

1.5.7.3.8 Adotar controles e métodos presentes nas normas ISO família 27000;

1.5.7.3.9 Auxiliar na homologação das soluções destinadas à segurança da informação;

1.5.7.3.10 Tratar incidentes de segurança;

1.5.7.3.11 Executar testes para implantação de serviços, políticas e regras de segurança;

1.5.7.3.12 Atuar de forma proativa para minimizar impacto dos riscos de segurança da Informação;

1.5.7.3.13 Alertar a CONTRATANTE, de forma proativa, sobre qualquer problema, anormalidade, falta de recursos ou comportamento não previsto que possam causar impactos nos serviços de TI.

1.5.8 SERVIÇO DE ADMINISTRAÇÃO E SUPORTE ÀS FERRAMENTAS DE BACKUP E RESTAURAÇÃO DE DADOS

1.5.8.1 Ao contratar o serviço, por intermédio de emissão de Ordem de Serviço, a CONTRATANTE irá demandar, no mínimo, 36 (trinta e seis) meses de execução.

1.5.8.2 O dimensionamento da equipe necessária à execução das tarefas é de responsabilidade da contratada, que deverá, durante toda a execução do Contrato, atender os níveis de serviços e todos os perfis profissionais exigidos neste Elemento Técnico e seus anexos;

1.5.8.3 Os serviços contemplam administração e suporte às ferramentas de backup e restauração de dados, compreendendo, no mínimo, as seguintes atividades:

1.5.8.3.1 Definir, gerenciar, implementar, implantar, documentar e revisar a política de backup e restauração de dados.

1.5.8.3.2 Instalar, atualizar, configurar, administrar e suportar todos os servidores, appliances e softwares que compõe os serviços de backup e restauração de dados na CONTRATANTE.

1.5.8.3.3 Manter todas as soluções de backup e restauração de dados atualizadas;

1.5.8.3.4 Elaborar relatórios dos backups e restaurações para apresentação à CONTRATANTE, constando os resultados de cada operação realizada e quais dados e serviços estão protegidos;

1.5.8.3.5 Manter as operações de backup e restore das informações, seguindo os procedimentos definidos na Política de Backup;

1.5.8.3.6 Suportar a proposição de ações e procedimentos para a melhoria contínua dos aspectos de backup e restauração de dados;

1.5.8.3.7 Alertar a CONTRATANTE, de forma proativa, sobre qualquer problema, anormalidade, falta de recursos ou comportamento não previsto que possam causar impactos nos serviços de TI.

1.5.9 NÍVEIS DE SERVIÇO PARA MONITORAMENTO E SUPORTE TÉCNICO PARA LAN/WAN E INFRAESTRUTURA NUVEM PRIVADA/HÍBRIDA

1.5.9.1 CONDIÇÕES GERAIS

1.5.9.1.1 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.

1.5.9.1.2 A apuração da disponibilidade dos serviços será feita a partir de relatórios emitidos pelo serviço de monitoramento.

1.5.9.1.3 A apuração dos indicadores relativos ao tempo para solução ou atendimento de demandas será calculada, para todos os serviços, sempre com base na data e hora de registro inicial da demanda. No cálculo desses indicadores, serão desconsiderados os períodos em que as demandas estiveram suspensas ou não estiveram sob a responsabilidade da contratada.

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

1.5.9.1.5 As glosas serão calculadas e aplicadas sobre o valor total mensal previsto para o serviço específico que não atingir a métrica exigida em contrato (ex. Serviço de administração e suporte à infraestrutura de produção)

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

1.5.9.1.7 Para a correta categorização dos chamados será empregada a tabela abaixo:

Criticidade 1	Serviço indisponível
Criticidade 2	Serviço operando parcialmente
Criticidade 3	Serviço com degradação da qualidade

1.5.9.2 Tabela de níveis de serviço

Indicadores de níveis de serviço/mês	**Unidade de medida**	**Meta exigida**	**Glosa aplicável**
Disponibilidade dos serviços básicos de rede (correio eletrônico, proxy, DNS, DHCP, SNA, entre outros).	%	>= 99,5	0,2% + (0,1% para cada 1% abaixo da meta exigida).
Disponibilidade dos servidores e aplicativos da CONTRATADA provisionados na IaaS ou nuvem privada/híbrida.	%	>= 99,5	0,2% + (0,1% para cada 1% abaixo da meta exigida).

Disponibilidade dos ativos de rede (switches, roteadores, entre outros).	%	>= 99,5	0,2% + (0,1% para cada 1% abaixo da meta exigida).
Início de tratamento de incidentes de criticidade 1.	minutos	<= 30	0,3% + (0,1% para cada 5 minutos acima do tempo exigido).
Início de tratamento de incidentes de criticidade 2.	minutos	<= 60	0,2% + (0,1% para cada 5 minutos acima do tempo exigido).
Início de tratamento de incidentes de criticidade 3.	minutos	<= 120	0,1% + (0,1% para cada 5 minutos acima do tempo exigido).
Resolução de incidentes de criticidade 1. (1)	Horas úteis	8	0,3% + (0,1% para cada 4 horas acima do tempo exigido).
Resolução de incidentes de criticidade 2. (1)	Horas úteis	16	0,2% + (0,1% para cada 8 horas acima do tempo exigido).
Resolução de incidentes de criticidade 3. (1)	Horas úteis	24	0,1% + (0,1% para cada 16 horas acima do tempo exigido).
Resolução de solicitação de serviço.	Prazo negociado (2)		0,1% + (0,1% para cada 4 dias acima do prazo negociado).

(1) Entende-se por resolução do incidente o retorno do serviço ou ativo de TI afetado à sua operação.

(2) Para cada solicitação de serviço será negociado o prazo de entrega de acordo com a complexidade da solicitação.

1.6 DETALHAMENTO DOS SERVIÇOS DO ITEM 6 - SERVIÇOS DE CONSULTORIA EM IAAS

1.6.1 CARACTERÍSTICAS GERAIS

1.6.1.1 Os serviços de consultoria em IaaS serão demandados para a realização de todas as atividades referentes a disponibilização de serviços na nuvem contratada;

1.6.1.2 Serão incluídos nesse serviço as seguintes atividades:

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

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

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

1.6.1.2.4 Consultoria sobre o uso dos recursos da nuvem privada;

1.6.1.2.5 Serviços de *tunning*, ajustes, correção de falhas, detecção de problemas na infraestrutura de nuvem pública;

1.6.1.2.6 Problemas de link e comunicação da nuvem pública com as dependências da contrata e/ou nuvem privada.

1.6.2 SOLICITAÇÃO DOS SERVIÇOS

1.6.2.1.1 As ações serão executadas a partir da emissão de Ordem de Serviço que deverá ser aceita em comum acordo entre CONTRATANTE e CONTRATADA;

1.6.2.1.2 A CONTRATANTEenviará a Ordem de Serviço à CONTRATANTE com descrição das atividades a serem realizadas e o prazo desejado para término das atividade;

1.6.2.1.3 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.;

1.6.2.1.4 Todos ajustes na Ordem de Serviço devem ser realizados no prazo citado acima;

1.6.2.1.5 A CONTRATADA poderá solicitar extensão no prazo de revisão e aceite da Ordem de Serviço que será avaliada pelo COTRATANTE;

1.6.2.1.6 Caberá ao unicamente CONTRATANTE aceitar ou não a extensão de prazo;

1.6.3 NÍVEIS DE SERVIÇO PARA SERVIÇOS DE CONSULTORIA EM IAAS

1.6.3.1 CONDIÇÕES GERAIS

1.6.3.1.1 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.

1.6.3.1.2 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.

1.6.3.1.3 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 foram de acordo com a qualidade exigida em contrato.

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

1.6.3.1.5 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.

1.6.3.2 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).

[1] Para cada Ordem de Serviço será negociado o prazo de entrega de acordo com a complexidade da solicitação.

1.7 DETALHAMENTO DOS SERVIÇOS DO ITEM 7 - DISPONIBILIZAÇÃO DE SOFTWARE DE GRC - GOVERNANÇA, RISCO E COMPLIANCE

1.7.1 Serviço de fornecimento de licença, suporte, manutenção e garantia técnica, visando automatização dos processos de GRC da CONTRATANTE;

1.7.2 A Solução deverá contemplar no mínimo as funcionalidades macros abaixo e deverão estar disponíveis para integração por meio de APIs:

1.7.2.1 Listar base de conhecimento;

1.7.2.2 Listar objetos;

1.7.2.3 Administrar objetos;

1.7.2.4 Listar componentes de negócio;

1.7.2.5 Administrar componentes de negócio;

1.7.2.6 Visualizar estrutura organizacional;

1.7.2.7 Administrar estrutura organizacional;

1.7.2.8 Administrar projetos de riscos;

1.7.2.9 Administrar projetos de conformidade;

1.7.2.10 Listar registros do módulo Ticket;

1.7.2.11 Administrar registros do módulo Ticket;

1.7.2.12 Listar registros do módulo de Atestação;

1.7.2.13 Administrar registros do módulo de Atestação;

1.7.2.14 Listar registros do módulo de Contratos;

1.7.2.15 Administrar registros do módulo de Contratos;

1.7.2.16 Listar registro do módulo de GCN;

1.7.2.17 Administrar registros do módulo de GCN;
1.7.2.18 Administrar registros do módulo de Scanners;
1.7.2.19 Executar consultas do módulo de Relatórios;
1.7.2.20 Executar gráficos do módulo de Relatórios;
1.7.2.21 Executar relatórios do módulo de Relatórios;
1.7.2.22 Administrar usuários;
1.7.2.23 Listar pessoas e grupos;
1.7.2.24 Listar privilégios de pessoas e grupos; e
1.7.2.25 Administrar pessoas e grupos.
1.7.2.26 Permitir a inclusão de informações que correspondam a Análise de Impacto de Negócios onde o usuário poderá definir o impacto financeiro, imagem, regulatórios e operacionais nos objetos/ativos de níveis organizacionais ;
1.7.2.27 Visualizar o relacionamento entre os objetos/ativos de níveis organizacionais e os elementos de análises de riscos e conformidades;
1.7.2.28 Permitir a criação e gerenciamento de objetos/ativos de níveis organizacionais que permitam a representação estratégia e tática da organização;
1.7.2.29 Permitir criar e customizar diferentes tipologias de objetos/ativos de níveis organizacionais;
1.7.2.30 Permitir a exportação, criação, atualização e importação de objetos/ativos de níveis organizacionais por meio de planilhas off-line;
1.7.2.31 Permitir a criação de campos informacionais para objetos/ativos de níveis organizacionais, contendo no mínimo os seguintes campos: nome, responsável, descrição, tipo e importância;
1.7.2.32 Permitir a criação de tabelas com informações da estrutura organizacional, incluindo as informações dos campos informacionais dos elementos de análise, diretórios de divisões lógicas e objetos/ativos de níveis organizacionais, possibilitando a seleção e customização das colunas a serem apresentadas;
1.7.2.33 As tabelas de informações da estrutura organizacional devem ser exportáveis para arquivos em forma de planilhas off-line e documentos texto;
1.7.2.34 Permitir a atualização das informações dos elementos de análise e dos objetos/ativos de níveis organizacionais de forma automática por meio de pesquisas, baseado nas respostas fornecidas e em regras preestabelecidas pelo usuário;
1.7.2.35 Permitir a criação de campos de informações para objetos/ativos de níveis organizacionais, podendo ser do tipo: anexo, texto, data, e-mail, lista de opção única, lista de opção múltipla, número e imagem.
1.7.2.36 Permitir estruturar análises de riscos, tratamento de incidentes e ocorrências com as seguintes funcionalidades mínimas:
1.7.2.37 Permitir a análise de riscos dos elementos cadastrados na estrutura

organizacional;

1.7.2.38 As análises de riscos devem ser realizadas a partir de listas de verificações de boas práticas que contenham requisitos com métricas de probabilidade e severidade, conforme definição da ABNT ISO Guia 73;

1.7.2.39 Permitir a criação de projetos para análise de riscos, possibilitando a seleção do escopo da análise e dos analistas responsáveis;

1.7.2.40 A coleta de informações para a análise de riscos deve ser realizada por meio de questionários web na interface do software ou por exportação e importação de planilhas off-line ou através de dispositivos móveis;

1.7.2.41 Permitir que as análises de riscos tenham suas coletas de informações realizadas por meio da análise de questionários, respostas com o uso de pesquisas web e análises automatizadas;

1.7.2.42 As respostas das entrevistas de requisitos de boas práticas devem ser processadas automaticamente pelo software, podendo posteriormente serem consultadas em detalhes;

1.7.2.43 O acompanhamento dos indicadores das análises de riscos deve ser realizados nativamente na interface gráfica do software;

1.7.2.44 Permitir o anexo de arquivos de evidência e a inserção de comentários no questionário web;

1.7.2.45 Permitir o envio por e-mail do recibo e resumo da entrevista posterior suas respostas;

1.7.2.46 Permitir a criação e edição de listas de verificação de boas práticas baseado em um processo estruturado com total controle de versionamento;

1.7.2.47 Proporcionar meios para avaliação de riscos baseado em um processo que considere os resultados consolidados e os indicadores obtidos, bem como oferecer um simulador para ajudar na decisão de tratamento ou aceitação dos riscos identificados;

1.7.2.48 Permitir a criação de ações de tratamento dos riscos em seção específica para gestão de tratamentos, possibilitando o acompanhamento das ações;

1.7.2.49 Permitir a geração de tabelas e mapas com informações de risco consolidadas dos elementos de análise, dos diretórios de divisão lógicas e dos Objetos/ativos de níveis organizacionais;

1.7.2.50 Permitir a geração de relatórios na interface do software, bem como a customização e criação de novos modelos de relatórios;

1.7.2.51 Permitir que os relatórios gerados sejam exportados para formatos PDF e RTF;

1.7.2.52 Permitir o agendamento para envio de relatórios definindo os destinatários e a frequência de envio;

1.7.2.53 Permitir a determinação de um período de tempo para que as análises de riscos e de conformidades realizadas se tornem obsoletas;

1.7.2.54 Possuir nativamente métricas de classificação quantitativa e qualitativa para os riscos analisados;

1.7.2.55 Permitir o gerenciamento e monitoramento de registros de tratamento, de incidentes/ocorrências e de ações/mudanças;

1.7.2.56 Permitir a criação de registros de incidentes/ocorrências e de ações/mudanças manualmente na interface do software, possibilitando o monitoramento e acompanhamento das atividades;

1.7.2.57 Permitir a criação de campos customizados para os registros, bem como sua customização, apresentando nativamente os campos de título, descrição, responsável, prazo e localização;

1.7.2.58 Permitir a criação de diferentes tipos de registros, possibilitando a criação de campos específicos para cada tipo, bem como layouts específicos, com respectivo controle de acesso;

1.7.2.59 Permitir a criação de regras automatizadas para controle dinâmico das informações cadastradas nos registros;

1.7.2.60 Permitir que os registros criados sejam apresentados em formato de lista na interface do software, permitindo a exportação para planilha;

1.7.2.61 Permitir que registros sejam atualizados, fechados, cancelados e reabertos;

1.7.2.62 Permitir que documentos sejam anexados aos registros cadastrados na sua interface;

1.7.2.63 Permitir o relacionamento entre registros por meio de sua interface;

1.7.2.64 Permitir o gerenciamento dos registros por meio de dispositivos móveis, possibilitando a criação, edição, atualização, fechamento e cancelamento de registros;

1.7.2.65 Notificações de modificações dos registros devem ser enviadas nativamente para os responsáveis do registro, possibilitando a customização destas notificações;

1.7.2.66 Permitir a criação de tabelas e matrizes gráficas dos registros cadastrados, configurando as informações que serão apresentadas;

1.7.2.67 Permitir o acompanhamento e monitoramento de registros de tratamento gerados pelas análises de riscos e não conformidades;

1.7.2.68 Permitir a integração com scanners de vulnerabilidades por meio da importação de arquivos no formato XML (eXtensibleMarkupLanguage) e pela interface do sistema onde o usuário poderá informar as credenciais para integração direta com o scanner;

1.7.2.69 Permitir a visualização dos registros e ocorrências por meio de dispositivos móveis, bem como possibilitar a criação, edição, exclusão e finalização de registros e ocorrências.

1.7.2.70 Permitir estruturar análises de conformidade com as seguintes funcionalidades

mínimas:

1.7.2.71 Permitir a análise de conformidade dos elementos cadastrados na estrutura organizacional, baseada em documentos regulatórios (leis, decretos, framework e políticas);

1.7.2.72 Permitir a criação de projetos de análise de conformidade, possibilitando a seleção de escopo de análise e dos analistas responsáveis;

1.7.2.73 Permitir a associação de revisores para as análises de conformidade;

1.7.2.74 A coleta de informações para a análise de conformidade deve ser realizada por meio de realizações de entrevistas web na interface do software ou por exportação e importação de planilhas off-line;

1.7.2.75 Permitir que pessoas recebam notificações por e-mail sobre ações de seu interesse, bem como responder e revisar entrevistas de análise de conformidade;

1.7.2.76 O acompanhamento dos indicadores dos projetos de conformidade deve ser realizado nativamente na interface gráfica do software;

1.7.2.77 Permitir o anexo de arquivos de evidência e a inserção de comentários na entrevista web de conformidade;

1.7.2.78 Permitir a criação e edição de documentos regulatórios, possibilitando a inclusão de políticas internas do Ministério dos Transportes;

1.7.2.79 Permitir que sejam definidas permissões para acesso aos documentos gerados através da sua interface;

1.7.2.80 O software deve possibilitar o gerenciamento das relações entre os requisitos dos documentos regulatórios estruturados, permitindo a geração de relatórios esses mapeamentos;

1.7.2.81 O software deve proporcionar meios adequados para avaliação de conformidades baseado em um processo que considere os resultados consolidados e os indicadores obtidos;

1.7.2.82 Permitir a geração de tabelas e mapas com informações de conformidade consolidadas dos elementos de análise, dos diretórios de divisão lógicas e dos Objetos/ativos de níveis organizacionais;

1.7.2.83 Permitir nativamente na interface do software a customização de pesquisas de riscos e conformidade, possibilitando a criação de regras para exibir ou ocultar itens, processar respostas automaticamente e alterar a obrigatoriedade de inclusão de documentos anexos ou comentários;

1.7.2.84 Permitir a geração de relatórios na interface do software, bem como a customização e criação de novos modelos de relatórios;

1.7.2.85 Permitir que os relatórios gerados sejam exportados para formatos PDF e RTF;

1.7.2.86 O agendamento de envio de relatórios para pessoas cadastradas no software deve ser configurado na interface do software, definindo os destinatários e a

frequência de envio.

1.7.2.87 Permitir estruturar processos para a gestão de contingência com as seguintes funcionalidades mínimas:

1.7.2.88 Permitir cadastrar na análise de impacto do negócio as estimativas da interrupção do processo ao longo do tempo para diferentes dimensões (impacto regulatório, financeiro, de imagem e operacional);

1.7.2.89 Permitir o cálculo automático da medida de impacto com base nas informações da análise de impacto do negócio;

1.7.2.90 Permitir configurar os parâmetros MTPD (MaximumTolerablePeriodofDisruption), RPO (Recovery Point Objective) e RTO (Recovery Time Objective) para os Objetos/ativos de níveis organizacionais;

1.7.2.91 Permitir que seja definida a data de validade das informações relacionadas a análise de impacto do negócio e o período de sensibilidade do processo a interrupções;

1.7.2.92 Permitir associar os recursos dos quais os Objetos/ativos de níveis organizacionais dependem para operação normal e em modo de contingência;

1.7.2.93 Permitir gerenciar os procedimentos de contingencia de objetos/ativos;

1.7.2.94 Permitir que sejam realizadas análises de impacto no negócio, definir estratégias para os procedimentos de continuidade do negócio e planos de continuidade;

1.7.2.95 Permitir visualização ordenada por escala de criticidade dos Objetos/ativos de níveis organizacionais;

1.7.2.96 Permitir que as informações da análise de impacto do negócio sejam revisadas e enviados automaticamente para aprovação por um ou mais revisores;

1.7.2.97 Permitir a configuração dos parâmetros da revisão dos dados da análise de impacto do negócio para os Objetos/ativos de níveis organizacionais, possibilitando alocar um ou mais revisores;

1.7.2.98 Enviar notificações automáticas por e-mail e/ou SMS aos revisores da análise de impacto do negócio indicando que há revisões a serem realizadas;

1.7.2.99 Enviar notificações automáticas por e-mail e/ou SMS aos responsáveis pelo processo de continuidade quando uma ou mais revisões forem aceitas ou rejeitadas pelos revisores;

1.7.2.100 Permitir calcular automaticamente e atualizar a medida de impacto quando os dados da análise de impacto e negócio forem aprovados pelos revisores;

1.7.2.101 Apresentar na interface do sistema aos revisores da análise de impacto do negócio as informações que estiverem pendentes de revisão e aprovação;

1.7.2.102 Permitir que os dados da análise de impacto do negócio sejam aprovados ou rejeitados pelos revisores. Quando os dados forem rejeitados, uma notificação deverá ser enviada por e-mail para a pessoa que solicitou a revisão e para o

responsável pelo componente estratégico ou tático;

1.7.2.103 Quando uma revisão da análise de impacto do negócio for rejeitada, o software não deve calcular a medida de impacto;

1.7.2.104 Deverá ser informada na interface do software que uma nova revisão deve ser iniciada para que a análise de impacto para aquele componente estratégico ou tático seja concluída;

1.7.2.105 Permitir que os gestores de continuidade determinem estratégias apropriadas aos Objetos/ativos de níveis organizacionais classificados como críticos;

1.7.2.106 Permitir a redefinição das estratégias de continuidade por parte dos gestores e registrar um histórico com a data em que estratégia foi definida, responsável pela redefinição da estratégia e qual a estratégia foi adotada;

1.7.2.107 O software não deve permitir a redefinição de estratégias de continuidade quando estas estiverem associadas a planos de continuidade já publicado;

1.7.2.108 Permitir que as estratégicas de continuidade sejam utilizadas para mais de um componente estratégico e tático;

1.7.2.109 O software deve conter justificativas para as estratégias de continuidade cadastradas no software;

1.7.2.110 O software deve apresentar em sua interface as estratégias de continuidade definidas por níveis estratégicos, responsáveis pela estratégia de continuidade, medida de impacto e planos associados;

1.7.2.111 Permitir a criação de procedimentos contendo conjuntos de instruções detalhadas a serem seguidas para execução da contingencia de objetos/ativos;

1.7.2.112 O software deve gerar automaticamente um identificador para cada procedimento criado no software seguido de 8 dígitos;

1.7.2.113 Permitir que os procedimentos sejam associados a um ou mais planos;

1.7.2.114 Permitir que os procedimentos publicados no software sejam editados e/ou excluídos. Os procedimentos excluídos e já associados a um plano de continuidade publicado deverão constar no plano mesmo após a sua exclusão;

1.7.2.115 O software deve disponibilizar os procedimentos excluídos não ficando mais disponíveis para associação a novos planos;

1.7.2.116 Permitir a criação de atributos do tipo texto, data, parágrafo, anexo entre outros para uso nos procedimentos de continuidade cadastrados no sistema;

1.7.2.117 Permitir que sejam definidos os tempos de execução para cada procedimento de continuidade;

1.7.2.118 Permitir que os procedimentos de continuidade cadastrados no software sejam exportados para planilhas off-line e documentos de texto;

1.7.2.119 Permitir que os procedimentos de continuidade publicados e disponíveis para uso sejam visualizados na interface do software;

1.7.2.120 O software deve versionar os procedimentos de continuidade a partir da sua

publicação e futuras alterações;

1.7.2.121 Permitir criar e gerenciar planos de contingencia de objetos/ativos;

1.7.2.122 Permitir que os planos de continuidade sejam associados a pelo menos um OBJETO ao qual se destina, podendo ser Objetos/ativos de níveis organizacionais ou elementos de análise;

1.7.2.123 Permitir a criação de planos possuindo no mínimo propriedades gerais, como responsável, objetivo, procedimentos a serem executados e tempo estimado para execução;

1.7.2.124 Permitir a associação de planos a um ou mais procedimentos já publicados e também um ou mais planos publicados;

1.7.2.125 Permitir que os planos tenham os recursos especificados que serão utilizados em modo de operação normal e em modo de contingência, e os detalhes sobre como cada um deles deve ser utilizado;

1.7.2.126 Permitir a inclusão de uma árvore de contatos no plano para definir as pessoas que deverão ser contatadas e quem deverá contatá-las quando o plano for ativado;

1.7.2.127 Permitir que os planos tenham imagens e outros tipos de arquivos anexados;

1.7.2.128 Permitir a criação de atributos como campos texto, data entre outros que possam ser aplicados ao plano de continuidade;

1.7.2.129 Permitir que os planos sejam validados na interface do software pelas equipes de contingência e gestores da continuidade.

1.7.2.130 Permitir a criação e acompanhamento de indicadores por meio de gráficos e o dashboards com as seguintes funcionalidades mínimas:

1.7.2.131 Permitir a criação de gráficos dos tipos pizza, linha, coluna e área, possibilitando a configuração de cores e rótulo;

1.7.2.132 Possibilitar nativamente a criação de gráficos de indicadores padrão de risco e conformidade, permitindo a utilização de filtros;

1.7.2.133 Permitir a criação de gráficos por meio da conexão e consultas SQL (Structured Query Language) à bancos de dados Microsoft SQL Server e Oracle externos ao sistema;

1.7.2.134 Permitir a criação de painéis de controle formados de gráficos na interface do software, possibilitando a configuração de permissão de visualização de cada painel.

1.7.3 A solução deverá ser composta por módulos, contemplando funcionalidades especificas para cada área de atuação na organização contendo, no mínimo, os seguintes módulos:

1.7.3.1 Conhecimento

1.7.3.1.1 Base de conhecimento de riscos, vulnerabilidades e conformidade;

1.7.3.1.2 Criação de bases de conhecimento de forma dinâmica a partir dos riscos identificados em projetos de riscos e vulnerabilidades encontradas;

1.7.3.1.3 Identificação de pontos de controle de conformidade nos documentos de referência, que poderão ser usados para elaboração de entrevistas de conformidade; e

1.7.3.1.4 Documentos de referência deverão ser importados e visualizados dentro do sistema, devendo possuir versionamento das bases de conhecimento.

1.7.3.2 Objeto

1.7.3.2.1 Cadastramento de ativos da organização;

1.7.3.2.2 Permitir a personalização de tipos de ativos e campos de propriedades;

1.7.3.2.3 Permitir o georreferenciamento dos ativos cadastrados;

1.7.3.2.4 Ativos devem ser organizados conforme a hierarquia desejada pelo gestor;

1.7.3.2.5 Ativos devem ser associados à bases de conhecimento e a componentes de negócio;

1.7.3.2.6 Possuir módulo de visualização gráfica das associações entre ativos e componentes de negócio, e níveis de risco;

1.7.3.2.7 Possuir Importação/exportação de ativos a partir de planilhas EXCEL e

1.7.3.2.8 Permitir ver o histórico de tudo que ocorreu com um ativo como, por exemplo: projetos associados, alterações realizadas nas propriedades, vulnerabilidades associadas etc.

1.7.3.3 Projeto de Risco

1.7.3.3.1 Gerenciar todas as fases previstas na ISO 31000;

1.7.3.3.2 Permitir a identificação de riscos por meio de checklist e/ou inclusão manual;

1.7.3.3.3 Permitir o envio de checklist para que os responsáveis do ativo possam responder on-line;

1.7.3.3.4 Permitir a inclusão de anexos como evidências de riscos ou conformidade com os controles do checklist;

1.7.3.3.5 Permitir ajustar os níveis de risco em tempo real, com atualização automática de indicadores;

1.7.3.3.6 Possuir visualização de riscos identificados que permitam a rápida identificação de causas, consequências e ativos associados (matriz de risco);

1.7.3.3.7 Permitir o envio de riscos para tratamento em qualquer fase do projeto;

1.7.3.3.8 Gerenciar todo o processo de tratamento e aceitação de riscos;

1.7.3.3.9 Gerar insumos que possam ser usados para alimentar as bases de conhecimento existentes ou criar novas; e

1.7.3.3.10 Possuir dashboards integrados com indicados pré-definidos.

1.7.3.4 Projeto de Conformidade

1.7.3.4.1 Gerenciar todo o ciclo de um projeto de conformidade conforme ISO 19600;

1.7.3.4.2 O projeto de conformidade deverá ser baseado em entrevistas, que possam ser personalizadas conforme o público alvo;

1.7.3.4.3 Controlar a situação de todas as entrevistas enviadas, permitindo identificar entrevistas que foram abertas, respondidas ou parcialmente respondidas;

1.7.3.4.4 Os entrevistados não precisaram ser usuários do sistema;

1.7.3.4.5 Os Indicadores de conformidade deverão ser gerados dinamicamente conforme os questionários são respondidos;

1.7.3.4.6 Gerenciar todas as atividades referentes ao tratamento das não conformidades identificadas no projeto.

1.7.3.5 GCN (Gestão de Continuidade de Negócios)

1.7.3.5.1 Possuir a Base de armazenamento estruturada de todos os planos de continuidade de negócios;

1.7.3.5.2 Permitir a associação dos planos de ação com outros planos e/ou ativos da organização;

1.7.3.5.3 Permitir a identificação de responsabilidades das atividades do plano de ação; e

1.7.3.5.4 Possuir uma matriz de contatos dinâmica, gerada a partir das associações com outros planos, ativos ou pessoas da organização.

1.7.3.6 Contratos

1.7.3.6.1 Permitir o gerenciamento dos contratos estabelecidos entre a organização e fornecedores;

1.7.3.6.2 Permitir adicionar as métricas utilizadas no contrato, incluindo valor unitário e quantidade contratada. Por exemplo: Horas, UST, PF e Valor Monetário;

1.7.3.6.3 Permitir adicionar aditivos, reduções e ordens de serviços;

1.7.3.6.4 Permitir acompanhar o histórico com uma visão cronológica dos acontecimentos e

1.7.3.6.5 Permitir a geração de relatório padrão: Ex.:Extrato do contrato.

1.7.3.7 Atestação

1.7.3.7.1 Oferecer de forma simples ao projeto de conformidade, a possibilidade de envio de comunicados, notas, informativos de forma rápida; e

1.7.3.7.2 Permitir enviar, reenviar e acompanhar o recebimento dos atestados.

1.7.3.8 Tickets

1.7.3.8.1 Permitir a Centralização dos chamados, tratamentos oriundos de projetos de

riscos e conformidade, e incidentes. O processo de acompanhamento de inclusão de atividades e comunicados a envolvidos, deverão ser realizados dentro desse módulo;

1.7.3.8.2 Permitir o relacionamento com objetos (ativos);

1.7.3.8.3 Permitir o relacionamento com outros tickets;

1.7.3.8.4 Permitir a inclusão de novos tipos de tickets, com a possibilidade de escolha do nome, descrição e cor e

1.7.3.8.5 Permitir importar e exportar registros via planilha excel.

1.7.3.9 Relatórios

1.7.3.9.1 O módulo de relatórios deverá permitir a construção de relatórios, gráficos e dashboards. Além do uso dos dados nativos da solução deverá permitir a conexão com outras bases para compor as informações de seus gráficos e relatórios;

1.7.3.9.2 Permitir o cadastro de consultas utilizando linguagem SQL;

1.7.3.9.3 Permitir a criação de gráficos a partir de uma consulta criada. Gráficos do tipo: Pizza, Linha, Coluna e Barra;

1.7.3.9.4 Permitir a criação de templates com possibilidade de inclusão e remoção de consultas e gráficos criados previamente dentro das funcionalidades Consulta e Gráfico respectivamente; e

1.7.3.9.5 Permitir o agendamento do relatório com possibilidade de envio por e-mail para um ou mais destinatários.;

1.7.3.10 Scanners

1.7.3.10.1 O módulo scanners deve possuir dois módulos, um para inventariar os equipamentos da rede e outro para identificar as vulnerabilidades de cada equipamento identificado da rede; e

1.7.3.10.2 As vulnerabilidades poderão ser utilizadas no tratamento utilizando o módulo de projeto de riscos.;

1.7.3.11 Mensageiro

1.7.3.11.1 Possibilitar: notificações gerais do sistema; mensagens de associações; envolvimentos, papéis, remoções, entrevistas, atestados, tickets e afins.

1.7.3.12 Painel

1.7.3.12.1 Centralizar todos os gráficos e indicadores fixos e os customizados que foram desenhados dentro do módulo de Relatórios. Permitir exibição em televisores, e painéis de monitoramento;

1.7.3.13 Administração

1.7.3.13.1 As configurações gerais, controle de acesso e usuários deverão ser gerenciados dentro do módulo administração. Suas alterações deverão ser realizadas apenas pelo administrador do sistema.;

1.7.3.14 API - Integrações

1.7.3.14.1 A solução deverá possuir funcionalidades de integração via API em todos os módulos do software.

1.8 DETALHAMENTO DOS SERVIÇOS DO ITEM 8 - SERVIÇOS DE CONSULTORIA EM GRC - GOVERNANÇA, RISCO E COMPLIANCE

1.8.1 ESCOPO DA CONTRATAÇÃO DO SERVIÇO

1.8.1.1 Serviços de Consultoria Técnica Especializada em GRC contemplando:

1.8.1.1.1 Atividades de análise e gestão de riscos em processos e ambientes,

1.8.1.1.2 Análise e gestão de conformidade em legislações, normativos e políticas,

1.8.1.1.3 Desenvolvimento de aplicações customizadas que possuam interações com o Software de GRC, dentre outras atividades que sejam realizadas no software de GRC ou que seja integrado a ele tem o objetivo de executar atividades sob a ótica das três temáticas em questão, Governança, Risco e Conformidade na organização, proporcionando um melhor direcionamento dos recursos através das recomendações que serão propostas, além de permitir a implementação do Software de GRC para auxiliar as diversas áreas da organização.

1.8.2 Execução do Serviço

1.8.2.1 A prestação de serviço deverá ocorrer por meio de demandas de acordo com as atividades previstas nesta proposta em cada Ordem de Serviço. Para cada demanda deverá identificado o escopo, o prazo de entrega, as limitações, os pré-requisitos obrigatórios e o esforço necessário para execução das atividades e geração dos produtos relacionados.

1.8.2.2 Os serviços de consultoria especializada e operação do software deverão ser mensurados em horas cujo valor unitário é de acordo com a complexidade (baixa, média e alta.

1.8.2.3 O software deverá automatizar processos de GRC, integrando diferentes áreas e atividades para permitir o gerenciamento centralizado desses processos, que normalmente são segregados. O software deverá oferecer uma estrutura para gerenciar as diversas áreas e atividades de um negócio, como gestão de riscos, continuidade de negócios, conformidade com leis e padrões, riscos corporativos, entre outros.

1.8.2.4 A solução deverá possuir nativamente uma base de conhecimento com o intuito de dar suporte aos projetos de GRC, contendo diversas boas práticas de segurança para avaliação de riscos, catálogos de ameaças e de vulnerabilidades identificadas por scanners, além de outros conteúdos metodológicos especializados para automatizar o processo de conformidade com normas e regulamentações relevantes para a organização. Além do conteúdo fornecido, também deverão estar disponíveis editores para a criação, edição e publicação de conteúdo próprio, o que garantirá a flexibilidade necessária para que o sistema se ajuste a uma ampla gama de projetos de GRC.

1.8.2.5 As ações que precisam ser monitoradas, como tarefas, processos, solicitações e questões relativas a diversos módulos deverão ser gerenciadas como eventos em um único módulo, reduzindo o tempo de resposta, centralizando informação e gerando métricas. Além disso, as consultas deverão permitir que os resultados e as métricas geradas através de avaliações de riscos e de conformidade sejam consolidados para diferentes objetos da organização, centralizando assim as informações essenciais para a gestão dos processos que essas informações suportam.

1.8.3 CATÁLOGO DE SERVIÇOS DE CONSULTORIA

1.8.3.1 O Serviço de consultoria será executado sob demanda (somente será pago mediante a conclusão da demanda por parte daCONTRATADA).

1.8.3.2 O catalogo abaixo é uma visão macro de possíveis serviços a serem executados, o catalogo é uma tabela “viva”, onde os serviços poderão ser mudados, excluídos ou inseridos novos.

1.8.3.3 O quantitativo será dimensionado juntamente com a equipe responsável de cada área solicitante da CONTRATANTE.

PROJETO	ATIVIDADES	COMPLEXIDADE
Gestão de Riscos Corporativo	Elaboração metodologia de gestão de riscos corporativo	**Alta**
	Revisão metodologia de gestão de riscos corporativo	**Baixa**
	Implantação, monitoramento e melhoria mensal - Gestão de Riscos Corporativo	**Baixa**
	Mapeamento de (1-5) processos, (1-5) sub processos e suas atividades	**Média**

	Mapeamento de (6-10) processos, (6-10) sub processos e suas atividades	**Média**
	Mapeamento de (11-15) processos, (11- 15) sub processos e suas atividades	**Média**
	Mapeamento de (16-20) processos, (16- 20) sub processos e suas atividades	**Média**
	Mapeamento de (21-25) processos, (21- 25) sub processos e suas atividades	**Média**
	Mapeamento de (26-30) processos, (26- 30) subprocessos e suas atividades	**Média**
	Mapeamento de (Acima de 30) processos, (Acima de 30) subprocessos e suas atividades	**Alta**
	Elaboração de fluxo do processo	**Média**
	Análise e mapeamento de riscos em processos críticos	**Alta**
	Monitoramento e controle de atividades e processos críticos	**Baixa**

Gestão de SIC	Elaboração do Modelo de Gestão de Segurança da Informação e Comunicações	**Alta**
	Revisão do Modelo de Gestão de Segurança da Informação e Comunicações	**Média**

POSIC	Elaboração de Diretrizes da POSIC	**Alta**
	Revisão de Diretrizes da POSIC	**Média**
	Elaboração das Normas de Segurança	**Alta**

	Revisão das Normas de Segurança	**Média**
	Elaboração de Procedimentos Operacionais	**Alta**
	Revisão de Procedimentos Operacionais	**Média**
	Elaboração de sumário executivo	**Média**
	Elaboração de dicionário de ternos	**Baixa**
	Análise de conformidade com os controles das normas de segurança	**Média**
	Automatização do processo de divulgação da POSIC no software de GRC	**Alta**
	Elaboração de Plano de campanha em SIC	**Alta**
	Palestras de divulgação e conscientização da POSIC	**Média**

Gestão de Riscos	Elaboração do Modelo de Gestão de Riscos	**Alta**
	Revisão do Modelo de Gestão de Riscos	**Média**
	Elaboração do inventário de ativos (Manual)	**Baixa**
	Elaboração do inventário de ativos (Automatizado)	**Alta**
	Elaboração de Relatório de Inventário de ativos	**Baixa**

	Análise de Riscos de Ativos do tipo Tecnologia (ativos de rede, servidores, banco de dados, segurança e etc..)	**Média**
	Análise de Riscos de Ativos do tipo Processos	**Média**
	Análise de Riscos de Ativos do tipo Pessoas (Gestores, Técnicos e Usuários)	**Baixa**
	Análise de Riscos de Ativos do tipo Ambiente (escritório, PABX e Datacenter)	**Baixa**
	Elaboração de Plano de Avaliação e Tratamento de Riscos	**Média**
	Elaboração de Painel Indicadores de Riscos	**Baixa**
	Treinamento sobre operacionalização da GR (12 participantes)	**Média**

Gestão de Incidentes	Elaboração do Modelo de Gestão de Incidentes - ETIR	**Alta**
	Revisão do Modelo de Gestão de Incidentes - ETIR	**Média**
	Automatização do processo no software de GRC	**Média**
	Elaboração de Manual de operacional	**Baixa**
	Elaboração de Plano de Comunicação de Incidentes	**Média**
	Revisão de Plano de Comunicação de	**Baixa**

	Incidentes	
	Treinamento sobre operacionalização da ETIR (12 participantes)	**Média**
	Integração do software de GRC com outras tecnologias	**Baixa**
	Monitoramento e resposta a incidentes de segurança (24x7)	**Alta**
	Monitoramento e resposta a incidentes de segurança (16x7)	**Média**
	Monitoramento e resposta a incidentes de segurança (8x7)	**Média**
	Monitoramento e resposta a incidentes de segurança (8x5)	**Baixa**

GCN	Elaboração da Política de Continuidade de Negócios	**Alta**
	Revisão da Política de Continuidade de Negócios	**Média**
	Elaboração do Modelo de Gestão de Continuidade de Negócios	**Alta**
	Revisão do Modelo de Gestão de Continuidade de Negócios	**Média**
	Elaboração da Estratégia de Continuidade de Negócios	**Alta**

	Revisão da Estratégia de Continuidade de Negócios	**Média**

BIA	Elaboração do Relatório de Impacto de Negócios (BIA)	**Alta**
	Elaboração de plano de recuperação de desastres	**Alta**
	Revisão de plano de recuperação de desastres	**Média**
	Elaboração de plano de gerenciamento de incidentes	**Alta**
	Revisão de plano de gerenciamento de incidentes	**Média**
	Elaboração do plano de administração de crises	**Alta**
	Revisão do plano de administração de crises	**Média**
	Elaboração de plano de continuidade operacional	**Alta**
	Revisão de plano de continuidade operacional	**Média**
	Realização de teste em plano de contingência	**Baixa**
	Treinamento em temas relacionados a GRC (16 participantes) (GCN)	**Média**

Gestão de	Análise de conformidade (baseado em leis, normativos internos, acórdãos, normas da	**Alta**

Conformidade	ABNT, ISOs, Frameworks ou Fluxo de Trabalho)	
	Elaboração de documentos de referência	**Média**
	Inserção de documentos de referência	**Baixa**
	Elaboração de Relatório de conformidade	**Média**

Auditoria	Auditoria de contratos (SLA's)	**Alta**
	Elaboração de Relatório de Auditoria e Recomendações de Melhoria	**Média**

Plano Diretor de TIC e /ou SIC	Elaboração de Plano Diretor de TIC e/ou SIC	**Alta**
	Revisão de Plano Diretor de TIC e/ou SIC	**Média**
	Automatização do processo de controle e monitoramento dos Planos Diretores no software de GRC	**Alta**
	Elaboração de relatório de monitoramento dos planos diretores	**Média**
	Elaboração de Painel de Indicadores no software de GRC	**Baixa**
	Treinamento na solução de controle e monitoramento dos Planos Diretores no Software de GRC (10 participantes)	**Média**

Apoio Técnico Especializado	Análise de vulnerabilidades em tecnologias	**Alta**
	Parecer técnico especializado	**Alta**
	Teste de Invasão (Pentest)	**Alta**
	Análise de riscos em sistemas críticos (baseado em OWASP, ISOs, ABNT e boas práticas)	**Alta**
	Análise e mapeamento de riscos em processos críticos	**Alta**

1.8.4 NÍVEIS DE SERVIÇO PARA SERVIÇOS DE CONSULTORIA EM GRC - GOVERNANÇA, RISCO E COMPLIANCE

1.8.4.1 CONDIÇÕES GERAIS

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

1.8.4.1.2 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.

1.8.4.1.3 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.

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

1.8.4.1.5 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.

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).

(1) Para cada Ordem de Serviço será negociado o prazo de entrega de acordo com a complexidade da solicitação.

1.9 DETALHAMENTO DOS SERVIÇOS DO ITEM 9 - DISPONIBILIZAÇÃO DE SOFTWARE DE GERENCIAMENTO DE CHAVES CRIPTOGRÁFICAS

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

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

1.9.2.1 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

1.9.2.2 Possuir funcionalidade de auditoria e log e integra com diretórios de usuário (LDAP e AD) para controles de autorização e uso de chaves.

1.9.2.3 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.

1.9.2.4 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.

1.9.2.5 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 InteroperabilityProtocol (KMIP).

1.9.2.6 Gerenciar centralmente chaves simétricas e assimétricas, dados secretos e certificados X.509 junto com políticas associadas.

1.9.2.7 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.

1.9.2.8 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.

1.9.2.9 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.

1.9.2.10 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.

1.9.2.11 Criptografar em nível de coluna transparente e eficiente

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

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

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

1.9.2.15 Implantar em ambientes de nuvem locais, virtuais e públicos

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

1.9.2.17 Possuir Rotação de chave integrada e re-digitação de dados

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

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

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

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

1.9.2.22 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;

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

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

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

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

1.9.2.27 Suportar Cloud e Infraestruturas Virtuais;

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

1.9.2.29 Suportar integração e Gerenciamento de Conteúdo Alfresco Open ECM, Open Text (EMC), InfoArchiveStealthContentStore, ServiceNow, Mainframe EncryptionPKware, Big Data Dataguise, DataStax, Hadoop, MongoDB, MariaDB, HANA SAP, Cassandra, Couchbase, Hortonworks, CloudEra, Analytics IBM Qradar, HPE ArcSight, Splunk, Análise de Segurança RSA, Acima de Segurança;

1.9.2.30 Suportar Servidores de Aplicativos IBM WebSphere, Oracle Weblogic, Microsoft IIS, Apache Tomcat, Soluções de Backup RedHatJBoss, CommvaultSimpana, Symantec NetBackup (via NetApp), CloudStorageNutanix, Amazon Web Services S3, DropBox, Google CloudStorage, Google Drive, NetAppCloud ONTAP, NetAppAltaVault, IBM ICDES, Controlador de Armazenamento Panzura;

1.9.2.31 Criptografar arquivos e discos PKware, IBM, Dell, AWS, Microsoft, LUKS, ViaSat;

1.9.2.32 Gerenciar de Identidades CentrifyPrivilege Service, Lieberman Software ;

1.9.2.33 Suportar Armazenamento físico NetApp NSE, Dell Compellent (SC e XC), MSL HPE / ESL Tape Libraries, HPE 3Par StoreServ, HPE XP7, Hitachi, SP, Hitachi HUS, Hitachi RAID700, IBM XIV SED, Quantum Scalar Series (i6000, i500 & i40 / 80), Viasat, Brocade FS8-18, HuaweiOceanstor, TintriVMStore, Cisco UCS, SpringPathHyperFlex, NexentaStor 4.5;

1.10 DETALHAMENTO DOS SERVIÇOS DO ITEM 10 - DISPONIBILIZAÇÃO DE SOLUÇÃO DE SEGURANÇA CONTRA AMEAÇAS DIGITAIS

1.10.1 SERVIÇO DE SEGURANÇA PARA SERVIDORES VIRTUAIS:

1.10.1.1. 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;

1.10.1.2. Características de Licenciamento da Solução:

1.10.1.2.1. Estar dimensionada para 150 servidores virtuais.

1.10.1.3. Funcionalidades e Requisitos Mínimos:

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

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

1.10.1.3.2. Permitir a integração com todas as versões do VMwarevCenter a partir da Versão 4.0, de modo a importar e sincronizar os objetos (hosts VMware e Guests VM) para a console de gerenciamento da solução;

1.10.1.3.3. Permitir, no caso de versões anteriores a VMware 6.0, integração com as seguintes API'sVMware:

1.10.1.3.3.1. VMsafe API;

1.10.1.3.3.2. vShieldEndpoint API.

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

1.10.1.3.4.1. Firewall;

1.10.1.3.4.2. Inspeção de Pacotes;

1.10.1.3.4.3. Monitoramento de Integridade;

1.10.1.3.4.4. Inspeção de Log's;

1.10.1.3.4.5. Anti-malware e Reputação Web;

1.10.1.3.4.6. Controle de Aplicação;

1.10.1.3.5. Suportar a aplicação das funcionalidades de segurança acima, inclusive para ambientes com versão 6.0 do vCenter/ vSphere, com integração com as novas API's da VMware (NSX);

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

1.10.1.3.6.1. Windows Server 2003, 2008 e 2012 (todas as versões);

1.10.1.3.6.2. Sistemas Operacionais Linux, no mínimo para as distribuições: RedHat, Suse, CentOs e Debian.

1.10.1.3.7. Possuir a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais a partir de uma console única e centralizada do mesmo fabricante;

1.10.1.3.8. Executar rastreamento nas máquinas virtuais e fornecer lista de todas as recomendações de segurança para os softwares que estiverem instalados nessas máquinas virtuais, bem como do sistema operacional;

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

1.10.1.4. Funcionalidades de Firewall:

1.10.1.4.1. Operar como firewall de host stateful bidirecional, monitorando as comunicações nos servidores protegidos;

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

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

1.10.1.4.4. 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);

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

1.10.1.4.6. Permitir realizar pseudostateful em tráfego UDP;

1.10.1.4.7. Permitir limitar o número de conexões entrantes e de saída de um determinado IP de origem;

1.10.1.4.8. Permitir a criação de novas regras utilizando templates padrão;

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

1.10.1.5. Funcionalidades de Inspeção de Pacotes:

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

1.10.1.5.2. 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;

1.10.1.5.3. Permitir execução de varreduras sob demanda ou agendada;

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

1.10.1.5.5. 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;

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

1.10.1.5.6.1. Windows 2003, 2008 e 2012;

1.10.1.5.6.2. Linux RedHat, Suse, CentOS e Debian;

1.10.1.5.6.3. 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.

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

1.10.1.5.8. Possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

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

1.10.1.5.10. 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;

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

1.10.1.5.12. Implementar a inspeção de tráfego incoming SSL;

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

1.10.1.5.14. 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;

1.10.1.5.15. 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;

1.10.1.5.16. 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;

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

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

1.10.1.6. Funcionalidades de Monitoramento de Integridade:

1.10.1.6.1. Possuir a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

1.10.1.6.2. Possuir a capacidade de detectar mudanças no estado de portas em sistemas operacionais Linux;

1.10.1.6.3. Possuir a capacidade de monitorar o status de serviços e processos do sistema operacional;

1.10.1.6.4. Possuir a capacidade de monitorar mudanças efetuadas no registro do Windows;

1.10.1.6.5. 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;

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

1.10.1.6.7. Permitir execução de varreduras sob demanda ou agendada;

1.10.1.6.8. Rastrear arquivos por criação, última modificação, último acesso, permissões, owner, grupo, tamanho, SHA1, SHA256 e Flags;

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

1.10.1.6.10. Registrar em relatório todas as modificações que ocorram nos objetos monitorados;

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

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

1.10.1.7. Funcionalidades de Inspeção de Log's:

1.10.1.7.1. 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;

1.10.1.7.2. 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;

1.10.1.7.3. Permitir execução de varreduras sob demanda ou agendada;

1.10.1.7.4. Permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

1.10.1.7.5. Permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

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

1.10.1.7.7. Permitir modificar as regras por severidade de ocorrência de eventos;

1.10.1.8. Funcionalidades de Anti-malware e Reputação Web:

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

1.10.1.8.2. Permitir execução de varreduras sob demanda ou agendada;

1.10.1.8.3. Possibilitar a criação de listas de exclusão para processos, diretórios ou arquivos do SO;

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

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

1.10.1.8.6. Permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema.

1.10.1.9. Funcionalidades de Controle de Aplicação:

1.10.1.9.1. A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;

1.10.1.9.2. O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256

1.10.1.9.3. O agrupamento dos eventos deverá ser realizado pelo menos por Hash é por máquina;

1.10.1.9.4. A console deverá exibir eventos de no mínimo 30 dias;

1.10.1.9.5. A solução deverá possuir funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente;

1.10.1.10. Funcionalidades de Gerenciamento:

1.10.1.10.1. Permitir o envio de notificações via SMTP;

1.10.1.10.2. Permitir o envio de registros de logs a um servidor remoto;

1.10.1.10.3. Implementar gravação de eventos de auditoria envolvendo todos os eventos e ações realizadas na console de gerenciamento;

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

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

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

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

1.10.1.10.8. Permitir opções de permissionamento, no mínimo, para modos de visualização e edição de políticas;

1.10.1.10.9. 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;

1.10.1.10.10. Possuir dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;

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

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

1.10.1.10.13. Permitir o envio de eventos da console via SNMP;

1.10.1.10.14. Permitir o rollback de atualização de regras pela console de gerenciamento;

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

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

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

1.10.2. SERVIÇO DE PROTEÇÃO DE ENDPOINTS:

1.10.2.1. Os softwares (solução) necessários à prestação dos serviços deverão ser instalados, de modo a avaliar e proteger contra códigos maliciosos as estações de trabalho do ambiente da CONTRATANTE.

1.10.2.2. Características Licenciamento:

1.10.2.2.1. Estar dimensionada para no mínimo 1.200 estações de trabalho.

1.10.2.3. Funcionalidades e Requisitos Específicos:

1.10.2.3.1. Realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais: Windows 7 (x86/x64); Windows 8 e 8.1 (x86/x64) e Windows 10 (x86/x64);

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

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

1.10.2.3.4. Possuir regras específicas para detecção de ransonware;

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

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

1.10.2.3.6.1. Processos em execução em memória principal (RAM);

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

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

1.10.2.3.6.4. Arquivos recebidos por meio de programas de comunicação instantânea (msnmessenger, yahoomessenger, googletalk, icq, dentre outros).

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

1.10.2.3.8. 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;

1.10.2.3.9. 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;

1.10.2.3.10. 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;

1.10.2.3.11. Permitir proteção dedicada contra URL's maliciosas voltadas a clientes utilizando Microsoft Skype for Business e Microsoft Lync Server.

1.10.2.3.12. 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;

1.10.2.3.13. Permitir o rollback das atualizações das listas de definições de vírus e engines;

1.10.2.3.14. Permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações;

1.10.2.3.15. Permitir proteção dedicada contra códigos maliciosos voltadas a clientes Microsoft Skype for Business e Microsoft Lync Server.

1.10.2.3.16. 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.

1.10.2.4. Funcionalidades de Controle de Dispositivos:

1.10.2.4.1. Possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

1.10.2.4.2. Possuir o controle de acesso a drives de mídias de armazenamento como CD-ROM e DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

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

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

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

1.10.2.5. Funcionalidades de Host IPS e Host Firewall:

1.10.2.5.1. 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);

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

1.10.2.5.3. Efetuar varredura de segurança automática ou sob demanda que aponte vulnerabilidades de sistemas operacionais e aplicações e atribua automaticamente as regras de Host IPS para proteger a estação de trabalho ou notebook contra a possível exploração da vulnerabilidade;

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

1.10.2.5.5. Prover proteção contra as vulnerabilidades de aplicações terceiras, por meio de regras de host ips, tais como oraclejava, abobe pdfreader, adobe flash player, realnetworks real player, Microsoft office, appleitunes, applequick time, apple safari, googlechrome, mozillafirefox, opera browser, ms internet explorer, entre outras;

1.10.2.5.6. Permitir a emissão de alertas via SMTP e SNMP;

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

1.10.2.5.8. Permitir criação de regras de firewall por origem de ip ou mac ou porta e destino de ip ou mac ou porta;

1.10.2.5.9. Permitir a criação de contextos para a aplicação para criação de regras de firewall;

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

1.10.2.6. Funcionalidades de Controle de Aplicação:

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

1.10.2.6.2. Permitir a criação de políticas de segurança personalizadas;

1.10.2.6.3. Permitir o controle do intervalo de envio dos logs e para envio de atualização de cada política;

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

1.10.2.6.5. Permitir as seguintes ações: Permissão de execução; Bloqueio de execução e Bloqueio de novas instalações;

1.10.2.6.6. 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;

1.10.2.6.7. Possuir categorias de aplicações e permitir a utilização de múltiplas regras de controle de aplicações;

1.10.2.6.8. Possuir atualização das categorias de maneira automatizada.

1.10.2.7. Funcionalidades de Proteção contra Vazamento de Informações:

1.10.2.7.1. Possuir a capacidade de realizar a proteção contra vazamento de informação nos seguintes sistemas operacionais: Windows 7 (x86/x64);Windows 8 e 8.1 (x86/x64) e Windows 10 (x86/x64);

1.10.2.7.2. 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;

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

1.10.2.7.4. Permitir a configuração de quantas camadas de compressão serão verificadas;

1.10.2.7.5. Permitir a criação de modelos personalizados para identificação de informações;

1.10.2.7.6. 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.

1.10.2.7.7. Permitir proteção dedicada contra vazamento de informações voltadas a clientes Microsoft Skype for Business e Microsoft Lync Server.

1.10.2.7.8. 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.

1.10.2.8. Funcionalidades de Criptografia:

1.10.2.8.1. 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);

1.10.2.8.2. 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;

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

1.10.2.8.4. Possuir a capacidade de exceções para criptografia automática;

1.10.2.8.5. Possuir compatibilidade de autenticação por múltiplos fatores;

1.10.2.8.6. Permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

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

1.10.2.8.8. Possuir mecanismos para wipe (limpeza) remoto;

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

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

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

1.10.2.8.12. Permitir, em nível de política, a indicação de pastas a serem criptografadas;

1.10.2.8.13. Possibilitar que cada política tenha uma chave de criptografia única;

1.10.2.8.14. Permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;

1.10.2.8.15. Possibilitar a desativação de dispositivos de gravação de mídias óticas e de dispositivos de armazenamento USB;

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

1.10.2.9. Módulo de proteção para smartphones e tablets

1.10.2.9.1. O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais:

1.10.2.9.2. IOS, Android, Windows Phone;

1.10.2.9.3. As funcionalidades estarão disponíveis de acordo com cada plataforma

1.10.2.9.4. Deve permitir o provisionamento de configurações de:

1.10.2.9.5. Wi-fi, Exchange Activesync, vpn, proxy http global e certificados;

1.10.2.9.6. Deve possuir proteção de anti-malware para Android;

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

1.10.2.9.8. Deve possuir capacidade de detecção de spam proveniente de SMS;

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

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

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

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

1.10.2.9.13. Deve permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;

1.10.2.9.14. Deve permitir o bloqueio de aplicativos de acordo com sua faixa etária indicativa;

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

1.10.2.9.16. Tempo de expiração;

1.10.2.9.17. Bloqueio automático da tela;

1.10.2.9.18. Bloqueio por tentativas inválidas;

1.10.2.9.19. Controle de acesso à seguinte lista funções e status de ativação de funções dos dispositivos móveis:

1.10.2.9.20. Bluetooth

1.10.2.9.21. Câmera

1.10.2.9.22. Cartões de memória

1.10.2.9.23. Wlan/wifi

1.10.2.9.24. GPS

1.10.2.9.25. Microsoft Activesync

1.10.2.9.26. MMS/SMS

1.10.2.9.27. Alto-falante

1.10.2.9.28. Armazenamento USB

1.10.2.9.29. 3g

1.10.2.9.30. Modo de desenvolvedor

1.10.2.9.31. Ancoragem (tethering)

1.10.3 Serviço de disponibilização de firewall

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

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

1.10.3.3 Performance

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

1.10.3.3.2. Suporte a, no mínimo, 8M conexões simultâneas

1.10.3.3.3. Suporte a, no mínimo, 300K novas conexões por segundo

1.10.3.3.4. Throughput de, no mínimo, 20 Gbps de VPN IPSec

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

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

1.10.3.3.7. Throughput de, no mínimo, 5 Gbps de VPN SSL

1.10.3.3.8. Suporte a, no mínimo, 500 clientes de VPN SSL simultâneos

1.10.3.3.9. Suportar no mínimo 5,2 Gbps de throughput de IPS

1.10.3.3.10. Suportar no mínimo 6,8 Gbps de throughput de Inspeção SSL

1.10.3.3.11. Throughput de, no mínimo, 4,7 Gbps com as seguintes funcionalidade 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;

1.10.3.3.12. Possuir ao menos 8 interfaces GE SFP

1.10.3.3.13. Possuir ao menos 8 interfaces GE RJ45

1.10.3.3.14. Possuir ao menos 2 interfaces 10GE SFP+

1.10.3.3.15. Disco SSD de, no mínimo, 480 GBytes para armazenamento de informações locais

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

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

1.10.3.3.18. Possuir ao menos 2 interfaces GE RJ45 dedicadas à gerenciamento

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

1.10.3.4 Características Gerais

1.10.3.4.1. 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;

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

1.10.3.4.3. 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;

1.10.3.4.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

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

1.10.3.4.6. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de protecção da rede;

1.10.3.4.7. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;

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

1.10.3.4.9. Os dispositivos de proteção de rede devem possuir suporte a Policybasedrouting ou policybasedforwarding;

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

1.10.3.4.11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

1.10.3.4.12. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

1.10.3.4.13. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

1.10.3.4.14. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

1.10.3.4.15. Deve suportar NAT dinâmico (Many-to-1);

1.10.3.4.16. Deve suportar NAT dinâmico (Many-to-Many);

1.10.3.4.17. Deve suportar NAT estático (1-to-1);

1.10.3.4.18. Deve suportar NAT estático (Many-to-Many);

1.10.3.4.19. Deve suportar NAT estático bidirecional 1-to-1;

1.10.3.4.20. Deve suportar Tradução de porta (PAT);

1.10.3.4.21. Deve suportar NAT de Origem;

1.10.3.4.22. Deve suportar NAT de Destino;

1.10.3.4.23. Deve suportar NAT de Origem e NAT de Destino simultaneamente;

1.10.3.4.24. Deve poder combinar NAT de origem e NAT de destino na mesma politica

1.10.3.4.25. Deve implementar Network PrefixTranslation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

1.10.3.4.26. Deve suportar NAT64 e NAT46;

1.10.3.4.27. Deve implementar o protocolo ECMP;

1.10.3.4.28. Deve implementar balanceamento de link por hash do IP de origem;

1.10.3.4.29. Deve implementar balanceamento de link por hash do IP de origem e destino;

1.10.3.4.30. 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;

1.10.3.4.31. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

1.10.3.4.32. 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;

1.10.3.4.33. Enviar log para sistemas de monitoração externos, simultaneamente;

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

1.10.3.4.35. Proteção anti-spoofing;

1.10.3.4.36. Implementar otimização do tráfego entre dois equipamentos;

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

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

1.10.3.4.39. Suportar OSPF gracefulrestart;

1.10.3.4.40. 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);

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

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

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

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

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

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

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

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

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

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

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

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

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

1.10.3.4.54. 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;

1.10.3.4.55. 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;

1.10.3.4.56. 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);

1.10.3.5 Controle por Política de Firewall

1.10.3.5.1. Deverá suportar controles por zona de segurança;

1.10.3.5.2. Controles de políticas por porta e protocolo;

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

1.10.3.5.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

1.10.3.5.5. Firewall deve ser capaz de aplicar a inspeção UTM (ApplicationControl e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;

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

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

1.10.3.5.8. "

1.10.3.5.9. Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common EventFormat (CEF);

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

1.10.3.5.11. Deve suportar o protocolo padrão da indústria VXLAN;

1.10.3.6 Controle de Aplicações

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

1.10.3.6.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

1.10.3.6.3. 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;

1.10.3.6.4. 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;

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

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

1.10.3.6.7. 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;

1.10.3.6.8. 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;

1.10.3.6.9. 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;

1.10.3.6.10. Identificar o uso de táticas evasivas via comunicações criptografadas;

1.10.3.6.11. Atualizar a base de assinaturas de aplicações automaticamente;

1.10.3.6.12. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos;

1.10.3.6.13. 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;

1.10.3.6.14. 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;

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

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

1.10.3.6.17. 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;

1.10.3.6.18. 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;

1.10.3.6.19. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

1.10.3.6.20. Deve alertar o usuário quando uma aplicação for bloqueada;

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

1.10.3.6.22. Deve possibilitar a diferenciação de tráfegos de InstantMessaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

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

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

1.10.3.6.25. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, BrowseBased, Network Protocol, etc);

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

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

1.10.3.7 Prevenção de Ameaças

1.10.3.7.1. 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;

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

1.10.3.7.3. 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;

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

1.10.3.7.5. 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;

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

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

1.10.3.7.8. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

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

1.10.3.7.10. Deve permitir o bloqueio de vulnerabilidades;

1.10.3.7.11. Deve permitir o bloqueio de exploits conhecidos;

1.10.3.7.12. Deve incluir proteção contra ataques de negação de serviços;

1.10.3.7.13. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de padrões de estado de conexões;

1.10.3.7.14. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;

1.10.3.7.15. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;

1.10.3.7.16. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise heurística;

1.10.3.7.17. Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;

1.10.3.7.18. Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;

1.10.3.7.19. Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;

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

1.10.3.7.21. Detectar e bloquear a origem de portscans;

1.10.3.7.22. Bloquear ataques efetuados por worms conhecidos;

1.10.3.7.23. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

1.10.3.7.24. Possuir assinaturas para bloqueio de ataques de buffer overflow;

1.10.3.7.25. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

1.10.3.7.26. 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;

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

1.10.3.7.28. Identificar e bloquear comunicação com botnets;

1.10.3.7.29. 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;

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

1.10.3.7.31. 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;

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

1.10.3.7.33. Os eventos devem identificar o país de onde partiu a ameaça;

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

1.10.3.7.35. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

1.10.3.7.36. 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;

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

1.10.3.8 Filtro de URL

1.10.3.8.1. 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);

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

1.10.3.8.3. 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;

1.10.3.8.4. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

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

1.10.3.8.6. Possuir pelo menos 60 categorias de URLs;

1.10.3.8.7. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

1.10.3.8.8. Permitir a customização de página de bloqueio;

1.10.3.8.9. 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);

1.10.3.8.10. Além do Explicit Web Proxy, suportar proxy Web transparente;

1.10.3.9 Identificação de Usuários

1.10.3.9.1. 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;

1.10.3.9.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

1.10.3.9.3. 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;

1.10.3.9.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas 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;

1.10.3.9.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

1.10.3.9.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;

1.10.3.9.7. Deve permitir o controle, sem instalação de cliente de software, 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);

1.10.3.9.8. 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;

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

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

1.10.3.9.11. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;

1.10.3.10 QoS e TrafficShaping

1.10.3.10.1. 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;

1.10.3.10.2. Suportar a criação de políticas de QoS e TrafficShaping por endereço de origem;

1.10.3.10.3. Suportar a criação de políticas de QoS e TrafficShaping por endereço de destino;

1.10.3.10.4. Suportar a criação de políticas de QoS e TrafficShaping por usuário e grupo;

1.10.3.10.5. Suportar a criação de políticas de QoS e TrafficShaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

1.10.3.10.6. Suportar a criação de políticas de QoS e TrafficShaping por porta;

1.10.3.10.7. O QoS deve possibilitar a definição de tráfego com banda garantida;

1.10.3.10.8. O QoS deve possibilitar a definição de tráfego com banda máxima;

1.10.3.10.9. O QoS deve possibilitar a definição de fila de prioridade;

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

1.10.3.10.11. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

1.10.3.10.12. Disponibilizar estatísticas em tempo real para classes de QoS ou TrafficShaping;

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

1.10.3.11 Filtro de Dados

1.10.3.10.14. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

1.10.3.10.15. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.10.3.10.16. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.10.3.10.17. 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;

1.10.3.12 Geo Localização

1.10.3.12.1. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;

1.10.3.12.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

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

1.10.3.13 VPN

1.10.3.13.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.10.3.13.2. Suportar IPSec VPN;

1.10.3.13.3. Suportar SSL VPN;

1.10.3.13.4. A VPN IPSEc deve suportar 3DES;

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

1.10.3.13.6. A VPN IPSEcdevesuportar Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;

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

1.10.3.13.8. A VPN IPSEc deve suportar AES 128, 192 e 256 (AdvancedEncryption Standard);

1.10.3.13.9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

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

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

1.10.3.13.12. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

1.10.3.13.13. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

1.10.3.13.14. 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;

1.10.3.13.15. Atribuição de DNS nos clientes remotos de VPN;

1.10.3.13.16. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

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

1.10.3.13.18. Suportar leitura e verificação de CRL (certificaterevocationlist);

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

1.10.3.13.20. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Antes do usuário autenticar na estação;

1.10.3.13.21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Após autenticação do usuário na estação;

1.10.3.13.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Sob demanda do usuário;

1.10.3.13.23. Deverá manter uma conexão segura com o portal durante a sessão;

1.10.3.13.24. 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);

1.10.3.14 Relatórios

1.10.3.14.1. Deve suportar receber logs de ao menos 10K dispositivos

1.10.3.14.2. Possuir capacidade de receber ao menos 1 GBytes de logs diários

1.10.3.14.3. Possuir ao menos 500 GB de capacidade de espaço em disco

1.10.3.14.4. Possuir ao menos 4 interfaces vNIC

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

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

1.10.3.14.7. Deve ser appliance do tipo virtual, compatível com VMWare ESX/ESXI 4.0 ou superior

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

1.10.3.14.9. 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)

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

1.10.3.14.11. Suportar SNMP versão 2 e versão 3 na solução de relatórios

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

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

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

1.10.3.14.15. Autenticação integrada a servidor Radius

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

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

1.10.3.14.18. Autenticação integrada ao Microsoft Active Directory

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

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

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

1.10.3.14.22. Possuir mecanismo para que logs antigos sejam removidos automaticamente

1.10.3.14.23. Permitir a importação e exportação de relatórios

1.10.3.14.24. Deve possuir a capacidade de criar relatórios nos formatos HTML

1.10.3.14.25. Deve possuir a capacidade de criar relatórios nos formatos PDF

1.10.3.14.26. Deve possuir a capacidade de criar relatórios nos formatos XML

1.10.3.14.27. Deve possuir a capacidade de criar relatórios nos formatos CSV

1.10.3.14.28. Deve ser possível exportar os logs em CSV

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

1.10.3.14.30. 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.

1.10.3.14.31. A solução deve possuir relatórios pré definidos

1.10.3.14.32. Possuir envio automático de logs para um servidor FTP externo a solução

1.10.3.14.33. Possibilitar a duplicação de relatórios existentes e edita-los logo após

1.10.3.14.34. Possuir a capacidade de personalização de capas para os relatórios

1.10.3.14.35. 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

1.10.3.14.36. 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.

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

1.10.3.14.38. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em realtime;

1.10.3.14.39. Dever ser possível fazer download dos arquivos de logs recebidos

1.10.3.14.40. Deve possuir agendamento para gerar e enviar automaticamente relatórios

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

1.10.3.14.42. Permitir o envio de maneira automática de relatórios por email

1.10.3.14.43. Deve permitir a escolha do email a ser enviado para cada relatório escolhido

1.10.3.14.44. Permitir programar a geração de relatórios, conforme calendário definido pelo administrador

1.10.3.14.45. Deve ser possível visualizar através de gráficos em tempo real o consumo de disco e taxa de geração de logs dos dispositivos gerenciados

1.10.3.14.46. Deve ser possível definir filtros nos relatórios

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

1.10.3.14.48. Permitir que relatórios criado sejam no idioma Português

1.10.3.14.49. Gerar alertas automáticos via Email, SNMP e Syslog baseados em eventos como ocorrência como log, severidade de log, entre outros

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

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

1.10.3.14.52. 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

1.10.3.14.53. 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.

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

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

1.10.3.14.56. A solução deve servir como um servidor de syslog e aceitar logs de diferentes fabricantes

1.10.3.14.57. Deve possuir a informação da quantidade de logs armazenado e estatística de tempo de retenção restante

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

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

1.10.3.14.60. Deve permitir ver em tempo real os log recebidos

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

1.10.3.14.62. 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.

1.10.3.14.63. Deve possuir relatório de PCI DSS Compliance

1.10.3.14.64. Deve possuir relatório de utilização de aplicações SAAS

1.10.3.14.65. Deve possuir relatório detalhado de prevenção de perda de dados (DLP)

1.10.3.14.66. Deve possuir relatório de VPN

1.10.3.14.67. Deve possuir relatório de Sistemas de prevenção de intrusão (IPS)

1.10.3.14.68. Deve possuir relatório de reputação do cliente

1.10.3.14.69. Deve possuir relatório de análise de segurança do usuário

1.10.3.14.70. Deve pussuir relatório de avaliação da ameaça cibernética

1.10.3.14.71. Deve possuir relatório de WiFi PCI Compliance

1.10.3.14.72. Deve possuir relatório a informação de AP´s e SSID´s autorizados, tambem clientes WiFi

1.10.3.14.73. Deve possuir relatório de equipamentos terminais de solução de segurança gerenciada

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

1.10.3.14.75. Deve possuir relatório de análise aplicações web, se há uma plataforma de segurança web

1.10.3.15 Gerência

1.10.3.15.1. Deve permitir gerenciar ao menos 20 dispositivos

1.10.3.15.2. Possuir ao menos 4 interfaces Vnic

1.10.3.15.3. Suportar mapeamento de ao menos 200 GB de espaço em disco

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

1.10.3.15.5. Caso a solução seja virtualizada, deverá ser compatível com ambiente VMwareESXi 5.5 e 6.0;

1.10.3.15.6. Caso a solução seja virtualizada, deverá ser compatível com ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2

1.10.3.15.7. Caso a solução seja virtualizada, deverá ser compatível com ambiente Citrix XenServer 6.0+

1.10.3.15.8. Caso a solução seja virtualizada, deverá ser compatível com ambiente Open SourceXen 4.1+

1.10.3.15.9. Caso a solução seja virtualizada, deverá ser compatível com ambiente KVM

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

1.10.3.15.11. Não deve possuir limite na quantidade de múltiplas vCPU caso entregue como appliance virtual;

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

1.10.3.15.13. 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;

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

1.10.3.15.15. Permitir acesso concorrente de administradores;

1.10.3.15.16. Possuir interface baseada em linha de comando para

administração da solução de gerência

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

1.10.3.15.18. Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;

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

1.10.3.15.20. Gerar alertas automáticos via Email

1.10.3.15.21. Gerar alertas automáticos via SNMP

1.10.3.15.22. Gerar alertas automáticos via Syslog

1.10.3.15.23. 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.

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

1.10.3.15.25. Deve ser permitido ao administrador transferir os backups para um servidor SCP

1.10.3.15.26. Deve ser permitido ao administrador transferir os backups para um servidor SFTP

1.10.3.15.27. As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante

1.10.3.15.28. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS

1.10.3.15.29. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa TACACS

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

1.10.3.15.31. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa RADIUS

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

1.10.3.15.33. Deve suportar sincronização do relógio interno via protocolo NTP.

1.10.3.15.34. Deve registrar as ações efetuadas por quaisquer usuários

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

1.10.3.15.36. Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência

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

1.10.3.15.38. 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.

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

1.10.3.15.40.

1.10.3.15.41. Deve suportar XML API

1.10.3.15.42. Deve suportar JSON API

1.10.3.16 Funcionalidades de Gerência de UTM/NGFW

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

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

1.0.3.16.3. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;

1.0.3.16.4. Permitir localizar quais regras um objeto está sendo utilizado;

1.0.3.16.5. Deve atribuir sequencialmente um número a cada regra de firewall;

1.0.3.16.6. Deve atribuir sequencialmente um número a cada regra de DOS;

1.0.3.16.7. Permitir criação de regras que fiquem ativas em horário definido;

1.0.3.16.8. Permitir backup das configurações e rollback de configuração para a última configuração salva;

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

1.0.3.16.10. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;

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

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

1.0.3.16.13. 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.

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

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

1.0.3.16.16. 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

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

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

1.0.3.16.19. 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.

1.0.3.16.20. Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos

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

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

1.0.3.16.23. Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência

1.0.3.16.24. Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada

1.0.3.16.25. Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos

1.0.3.16.26. Deve permitir criar regras de NAT64 e NAT46 de forma centralizada

1.0.3.16.27. Permitir criar regras antiDoS de forma centralizada

1.0.3.16.28. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada

1.0.3.16.29. 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

1.11 DETALHAMENTO DOS SERVIÇOS DO ITEM 10 - LINKS DE COMUNICAÇÃO

1.11.1 A CONTRATADA deverá disponibilizar 2 (dois) links dedicados de acesso à Internet de acordo com as especificações abaixo (para cara link):

1.11.1.1 Cada link deve ser disponibilizado por diferentes operadoras;

1.11.1.2 Garantia de conexão 24 horas por dia e 7 dias por semana;

1.11.1.3 Garantia total da banda contratada com redundância;

1.11.1.4 Link Simétrico, mesma velocidade de download e upload;

1.11.1.5 64 endereços IP fixos;

1.11.1.6 Velocidade do Link de conexão com a Internet de no mínimo 100Mbps

1.11.1.7 A Contratada se responsabilizará pelo fornecimento e instalação dos materiais e equipamentos necessários à prestação do serviço;

1.11.1.8 Após a implantação do link, solicitações de instalação, retirada e alteração de

1.11.1.9 características físicas já existentes, incluindo as configurações em equipamentos decomunicação de dados decorrentes dessas mudanças, dar-se-ão através de solicitaçõesformais por parte do Contratante, sendo que estas solicitações deverão ser executadaspela Contratada em, no máximo, 30 (trinta) dias.

1.11.1.10 A contratada se responsabilizará por eventuais adaptações nas instalações físicas nas dependências do contratante, assim como a infraestrutura externa, para a implantação dos serviços contratados (passagem de cabos, lançamento de fibras ópticas, adaptação de tomadas etc).;

1.11.2 SUPORTE DE SERVIÇOS:

1.11.2.1 Quando da ocorrência de falha no link a contratada deverá efetuar a verificação de todo oenlace (modems e link).

1.11.2.2 Deverão ser efetuados testes de verificação de qualidade de transmissão, pelo contratado dosserviços, sempre que houver solicitação da CONTRATANTE, sem custos adicionais.

1.11.2.3 A contratada deverá manter uma central de serviços para atendimento técnico com um númerotelefônico, com chamadas franqueadas, para o registro de chamados no período de 24 horas por dia, sete dias por semana, todos os dias do ano.

1.11.2.4 Somente serão aceitas solicitações técnicas oriundas da Área de TI da CONTRATANTE.

1.11.2.5 Manutenção do link com defeito. Os serviços de assistência técnica serão realizados emqualquer horário, sete dias por semana.

ANEXO II

PROPOSTA PADRONIZADA

Ao XXXXXXXXXXX de XXXXXX do XXXXXX

A empresa _____ (razão social), inscrita no CNPJ sob o número _____, inscrição estadual número _____, sediada no endereço _____ (citar endereço completo), para fins de participação no presente processo Seleção de Fornecedores n.º _____, vem pela presente apresentar - em anexo - sua proposta de preços, de acordo com as exigências do Ato Convocatório supracitado.

ITEM	Descrição	Detalhamento	UNIDADE	QTDE.	PREÇO UNITÁRIO
1	Infraestrutura como serviço - IaaS	Instância Virtual 01	Instância/Mensal	2	
		Instância Virtual 02	Instância/Mensal	1	
		Tráfego de saída da nuvem pública	Gigabyte/ mês	5	
2	Serviço de mensageria e colaboração em nuvem	Disponibilização de caixas postais e colaboração	Usuário / mês	1.200	
		Serviços de migração	Horas	400	
3	Storage como serviço	-	TB/mês	2	
4	Infraestrutura para nuvem privada/híbrida	-	Mensal	36	
5	Monitoramento e suporte técnico para LAN/WAN e	Serviço de monitoramento	Mensal	36	
		Serviço de Supervisão	Mensal	36	

	infraestrutura nuvem privada/híbrida	Serviço de administração e suporte à infraestrutura de produção	Mensal	36	
		Serviço de administração e suporte à infraestrutura de redes LAN e WAN	Mensal	36	
		Serviço de administração e suporte às ferramentas de mensageria e colaboração	Mensal	36	
		Serviço de administração e suporte às ferramentas de segurança da informação	Mensal	36	
		Serviço de administração e suporte às ferramentas de backup e restauração de dados	Mensal	36	
		-	Horas	1.200	
6	Serviços de consultoria em IaaS		Mensal	36	
7	Disponibilização de software de GRC - Governança, Risco e Compliance	Complexidade baixa	Horas	2.000	

8	Serviços de consultoria em GRC - Governança, Risco e Compliance	Complexidade média	Horas	2.500	
		Complexidade alta	Horas	1.500	
			Mensal	36	
9	Disponibilização de software de Gerenciamento de Chaves criptográficas	Disponibilização de Next Generation Firewall em Alta Disponibilidade	Mensal	36	
10	Disponibilização de solução de segurança contra ameaças digitais	Disponibilização de antivírus para caixas postais	Usuário/Mês	1.200	
		Disponibilização de antivírus para servidores Windows e Linux	Servidor/Mês	150	
		Disponibilização de antivírus para estações de trabalho Windows	Estação/Mês	1.200	
11	Links de comunicação		mensal	36	

1) Prazo de validade da proposta é de 90 (noventa) dias corridos, contados a partir da sua assinatura.
2) Declaramos estar cientes de todas as cláusulas do instrumento convocatório, bem como de seus anexos.
3) Apresentamos, conforme exigido no Ato Convocatório, os dados bancários para pagamento mediante depósito bancário em conta corrente, constando:
- Nome e número do Banco:

- Agência:

- Número da conta concorrente:
4) Declaramos que nos preços cotados estão incluídas todas as despesas, tais como tributos, seguros, transporte, pagamento de mão de obra, treinamento, frete até o destino, seguros, garantia e todos os demais encargos e/ou descontos porventura existentes.
Local/data

_____
(Assinatura do responsável pela empresa)
Nome/Cargo

ANEXO III – CHECK LIST

CHECK LIST - PARA CONTRATAÇÃO DE EMPRESA ESPECIALIZADA DE TIC	
Descrição	**Nr. Pág**
Proposta	
Proposta de preço (conforme modelo em anexo)	
Documentos para Habilitação:	
Habilitação Jurídica:	
Procuração	
Identidade	
Contrato Social	
Regularidade Fiscal:	
Prova de Inscrição e Situação CNPJ (site RFB)	
Inscrição no cadastro de contribuintes estadual (SEF)	
Certidão Conjunta Negativa de Débito - Trib. Federais e Dívida Ativa União / INSS	
Certidão Negativa de Débito com a Fazenda Distrital	
Certidão Regularidade FGTS – CRF	
Qualificação Econômica-financeira:	
Demonstração de Resultado e Balanço Patrimonial - O balanço será avaliado por meio de obtenção dos índices de Liquidez Geral (LG), de Solvência Geral (SG) e de Liquidez Corrente (LC), maiores que um (>1)	
Índice Balanço Econômico-financeiro	
Certidão de Falência e Concordata	
SICAF	
Certidão Negativa de Débitos Trabalhista (TST)	
Cadastro nacional de empresas inidôneas e suspensas - CEIS	
Cadastro nacional de empresas punidas - CNEP	
Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça – CNJ	
Cadastro Nacional de Empresas Inabilitadas e Inidôneas – TCU	
Qualificação Técnica:	
Atestados Capacidade Técnica:	
Declarações	

Considerando o histórico supracitado a cotação de preço, deve ser baseada na planilha de itens disponíveis no item 3 do 5º Termo Aditivo (96071640) e de forma que as especificações técnicas disponíveis no Elemento Técnico nº 2/2018 (28345241) devem compreender os itens conforme itens apresentados na planilha abaixo:

Item	Descrição	Detalhamento do Item	UNIDADE	QT	Valor Unitário	Valor Total mensal	Valor Total Anual
1	Infraestrutura IaaS	1-instância virtual 03	instancia	6	R$	R$	R$
		2-instância virtual 04	instancia	4	R$	R$	R$
		3-instância virtual 05	instancia	4	R$	R$	R$
		4-instância virtual 06	instancia	6	R$	R$	R$
		5-instância virtual 07	instancia	6	R$	R$	R$
		6-instância virtual 08	instancia	4	R$	R$	R$
		7-tráfego de saída da nuvem privada	Gb/mês	2	R$	R$	R$
2	Serviço de mensageria e colaboração em nuvem	disponibilidade de caixa postais e colaboração	usuário/mês	1800	R$	R$	R$
3	Storage como serviço		Tb/mês	30	R$	R$	R$
4	Infraestrutura par nuvem privada / hibrida		mês	1	R$	R$	R$
10	Disponibilização de solução de segurança	Next Generation		2	R$	R$	R$
		Antivírus para caixa de e-mail		1800	R$	R$	R$
		Antivírus para servidor		43	R$	R$	R$
		Antivírus para estação Windows		2400	R$	R$	R$
11	link de comunicação		unidade	6,5	R$	R$	R$
Valor mensal estimado mensal do Termo Aditivo: R$ xxxxxxxxx (_____). **Valor total estimado anual do Termo Aditivo: R$ xxxxxxxxx (_____).**							

- Configuração de cada instancia Virtual:

Item	Descrição	Serviço	Componentes	Sistema Operacional
1	Infraestrutura IaaS	1-instância virtual 03	2 vCPU(s) 8 GB de RAM	Microsoft Windows Server
		2-instância virtual 04	4 vCPU(s) 16 GB de RAM	Microsoft Windows Server
		3-instância virtual 05	8 vCPU(s) 32 GB de RAM	Microsoft Windows Server
		4-instância virtual 06	2 vCPU(s) 8 GB de RAM	Linux
		5-instância virtual 07	4 vCPU(s) 16 GB de RAM	Linux
		6-instância virtual 08	8 vCPU(s) 32 GB de RAM	Linux

Ante o exposto, encaminha-se os autos para Núcleo de Compras Diversas.