



APÊNDICE DO ANEXO I - ESTUDO TÉCNICO PRELIMINAR

ESTUDO TÉCNICO PRELIMINAR – IN SGD-ME nº 94/2022

1 – Definição

Inciso I, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

1.1 - Diretrizes Gerais para Elaboração dos Estudos Preliminares

1.1.1. O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Formalização de Demanda - DFD, bem como demonstrar a viabilidade técnica e econômica da solução identificada, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação, em consonância com o art. 11 da Instrução Normativa SGD-ME nº 94/2022.

1.2 - Normativos que disciplinam os serviços a serem contratados

1.2.1. Lei nº 14.133/2021 - Lei de Licitações e Contratos Administrativos.

1.2.2. Instrução Normativa SGD-ME nº 94, de 23 de dezembro de 2022 - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo.

2 - Das Necessidade de negócio e tecnologia

Inciso I, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

2.1. O CRQ-IV/SP necessita contratar empresa especializada para a prestação de serviços por demanda, na modalidade de infraestrutura como serviço, de hospedagem, conectividade, segurança de rede, replicação e backup incluindo os serviços de garantia de funcionamento e suporte técnico, visando atender as necessidades conforme condições especificadas neste estudo técnico preliminar;

2.2. O CRQ-VI/SP deve impulsionar iniciativas de tecnologia que possam transformar processos e



melhorar a eficiência operacional;

- 2.3. A legislação determina que sejam utilizadas medidas técnicas e administrativas para proteger os dados de acessos não autorizados e situações acidentais de perda das informações;
- 2.4. Ataques cibernéticos têm como propósito interromper, desativar, destruir ou manipular os dados de uma rede corporativa. Em caso de ataques cibernéticos, a instituição poderá ficar exposta, já que os dados podem ser apagados ou criptografados;
- 2.5. Com a ameaça crescente de ataques ransomware, o cenário de segurança cibernética tem se tornado cada vez mais perigoso, com isso torna-se necessários políticas de armazenamento de dados seguros e que não possam ser alteradas. Além disso, o CRQ-IV/SP precisa estabelecer um plano de continuidade dos negócios baseados em tecnologia da informação através da implantação de procedimentos e estratégias eficientes que possibilite restabelecer a funcionalidade dos sistemas informatizados em caso de falhas técnicas;
- 2.6. O crescimento dos serviços de cloud Computing tem sido rápido e constante nos últimos anos impulsionados por fatores tecnológicos, econômicos e estratégicos. Os serviços de Cloud Computing (Computação em nuvem) é um modelo de fornecimentos de serviços de computação, tais como: servidores, armazenamento, banco de dados, redes, softwares, suporte técnico, backup etc. por meio da internet, com pagamentos efetuados conforma a utilização do recurso.
- 2.7. Como vantagens e benefícios da computação em nuvem podemos destacar:
- 2.7.1. Eliminação de gastos com hardware, licenças, energia, espaço físico e manutenção;
 - 2.7.2. Flexibilidade para aumentar ou reduzir os recursos usados conforme a demanda;
 - 2.7.3. Aumento da disponibilidade dos serviços em operação;
 - 2.7.4. Aumento da segurança da informação;
 - 2.7.5. Torna mais eficiente o processo de recuperação de desastre.
- 2.8. Tendo como objetivo a adoção de serviços baseados em Cloud Computing a médio prazo, esta contratação permitirá ao órgão iniciar um processo de transição dos serviços disponíveis on premise para ambiente nuvem;
- 2.9. O fornecedor dos serviços de computação em nuvem, objeto desta licitação, deverá possuir capacidade técnica para oferecer todos os serviços solicitados neste Estudo Técnico Preliminar. A Contratação de um único fornecedor que atenda a todos os requisitos e serviços solicitados consolidará a gestão em um único contrato permitindo padronização de processos, prazos, níveis



de serviço (SLAs) e responsabilidades. Através de um único contrato teremos mais eficiência operacional, governança, gestão e controle de custos;

- 2.10. Esta contratação está registrada no Plano de Contratações Anuais (PCA) – exercício 2025, elaborado pela Gerência de Tecnologia da Informação.

3.1 – Requisitos da contratação – Identificação das necessidades de negócio

- 3.1.1. Somente poderão participar deste processo licitatório pessoas jurídicas cujo ramo de atividade seja compatível com o objeto da licitação e que apresentem todos os documentos de habilitação exigidos;
- 3.1.3. Não será permitida a participação de cooperativas, conforme fundamentado pelas diretrizes da IN SEGES/MPDG n.º 05/2017 que dispõe, em seu art. 10, que a contratação de cooperativas por autarquias somente poderá ocorrer quando o serviço evidenciar possibilidade de ser executado com autonomia pelos cooperados e quando a gestão operacional do serviço for executada de forma compartilhada ou em rodízio;
- 3.1.4. A contratada deverá atender as exigências de habilitação jurídica e de regularidade fiscal, social e trabalhista, conforme disciplinado pela Lei 14.133/2021, além de outras exigências de habilitação, qualificação técnica e qualificação econômico-financeira;
- 3.1.5. Não deverá haver cobranças adicionais por tráfego de dados, consumo de banda ou de número de transações ou requisições, sejam de envio (upload) ou de recebimento (download);
- 3.1.6. A solução, objeto desta contratação, deverá ser totalmente compatível e baseada na plataforma de backup e replicação Veeam Backup & Replication versão Enterprise Plus Edition Perpetual, já em utilização pelo CRQ-IV/SP;
- 3.1.7. A solução deve incluir recursos de backup e replicação integrados em uma única solução, incluindo replicação e reversão da replicação de e para a infraestrutura virtualizada;
- 3.1.8. Deverá ser capaz de executar backups sem interromper o funcionamento das máquinas virtuais e sem gerar uma diminuição no desempenho, facilitando as tarefas de backup e as migrações como um todo;
- 3.1.9. Deve ser capaz de entender as máquinas virtuais como objetos no ambiente virtual e suportar a proteção das configurações destes, independentemente dos dados das máquinas;
- 3.1.10. Deverá ter tecnologia de deduplicação para obter uma economia de espaço de armazenamento para backups;



- 3.1.11. Deverá ser capaz de oferecer 100% de confiabilidade na inicialização correta de todas as suas máquinas virtuais protegidas e no funcionamento do serviço/função dessas máquinas virtuais (servidor DNS, controlador de domínio, servidor de correio, servidor SQL, Oracle etc.) no momento da recuperação, sendo capaz de realizar testes de recuperabilidade automaticamente a partir das máquinas copiadas;
- 3.1.12. Para a solução de backup imutável a Contratada deverá oferecer uma arquitetura tecnológica que permita a proteção de dados e que garanta a segurança e integridade das informações, evitando que sejam excluídas, modificadas ou corrompidas;
- 3.1.13. Para a solução de Disaster Recovery (DR) a Contratada deverá oferecer um conjunto de tecnologias e práticas que visa restaurar a funcionalidade e o acesso aos servidores que estejam associados nesta solução. A replicação das máquinas virtuais do CRQ-IV/SP para o ambiente de DR deverá ser realizada através da ferramenta de Veeam Backup & Replicação Enterprise Plus Edition através do fornecimento, caso seja necessário, das licenças;
- 3.1.14. Deverá oferecer suporte às últimas versões disponíveis dos hipervisores mais populares no mercado: VmWare vSphere e Microsoft Hyper-V em todas as versões compatíveis com o respectivo fabricante;
- 3.1.15. Não deve exigir hardware específico para obter a desduplicação e a compactação de informações fora dos requisitos padrão de qualquer software (appliance desduplicadora);
- 3.1.16. Deverá permitir a realização de backups de máquinas virtuais com sistemas operacionais Windows Server 2012 e/ou superior e as diversas versões de Linux disponíveis no mercado;
- 3.1.17. A solução contratada deverá possuir alta disponibilidade possibilitando a execução dos Jobs de backup e restauração na modalidade 24 x 7.
- 3.1.18. A Contratada deverá prestar suporte técnico a Contratante durante o processo de implantação do serviço objeto desta contratação;
- 3.1.19. A Contratada deverá entregar a documentação técnica como também oferecer suporte técnico caso algum servidor fique inoperante e seja necessário ativá-lo no ambiente da Contratada através do serviço de Disaster Recovery. Para que as operações do órgão não fiquem indisponível por muito tempo, a Contratada deverá disponibilizar o servidor em até 02 horas a partir do comunicado que o órgão fizer à Contratada.
- 3.1.20. A Contratada deverá hospedar as informações da Contratante em datacenter com certificado TIER 3 ou superior;



- 3.1.21. Ao final do contrato a Contratada deverá excluir todas as informações armazenadas em sua infraestrutura de datacenter, emitir um documento à CONTRATANTE atestando que tal procedimento foi realizado;
- 3.1.22. Para os serviços de backup do MS Office 365, backup tradicional e imutável das VMs bem como a replicação das VMs para o ambiente de Disaster Recovery (DR) da CONTRATADA, será utilizado a ferramenta Veeam Backup & Replication versão Enterprise Plus Edition Perpetual já de propriedade do CRQ-IV/SP. O fornecimento das licenças complementares necessárias para o perfeito funcionamento dos serviços ficará sob responsabilidade da CONTRATADA;
- 3.1.23. Caso seja necessário a ligação dos servidores que estejam replicados para o ambiente da CONTRATADA em ambiente de desastre (DR) a CONTRATADA deverá disponibilizar um link de comunicação lógica do tipo VPN, comunicando-se com o datacenter do CRQ-IV/SP. A CONTRATADA deverá oferecer o suporte técnico necessário a equipe do CRQ-IV/SP com o objetivo de estabelecer esta ligação lógica;
- 3.1.24. Para os servidores virtuais que estarão armazenados em ambiente desastre (DR), caso seja necessário torná-los operante na infraestrutura da CONTRATADA, ela deverá garantir um período mínimo de 7 dias sem a cobrança adicional nos preços contratados. A cobrança do serviço com base nos custos de Servidores Virtuais e Recursos Computacionais em ambiente de produção somente ocorrerá após o sétimo dia.

3.2 – Comprovação da capacidade técnica

- 3.2.1. A comprovação de capacidade técnica tem por objetivo assegurar que as empresas participantes estejam realmente preparadas para executar o objeto contratado. Com isso, faz-se necessário a apresentação de documentos que comprove sua capacidade técnica.
- 3.2.2. Ao exigir comprovação de capacidade técnica, a Administração Pública se resguarda para que apenas empresas com experiência comprovada executem o contrato, minimizando riscos de erros, atrasos ou má execução;
- 3.2.3. Além disso, empresas tecnicamente habilitadas oferecem mais segurança ao gestor público, que poderá comprovar que “escolheu” um fornecedor capaz de cumprir o contrato, evitando responsabilizações futuras;
- 3.2.4. Sem a exigência de apresentação da capacidade técnica, empresas sem experiências real



podem vencer a licitação apenas por oferecer menor preço, o que pode resultar em falhas e prejuízos para o órgão licitante. E por fim, tornar o processo mais justo nivelando a concorrência.

3.2.5 Para este processo licitatório, a LICITANTE deverá apresentar:

- i. Comprovação de capacidade operacional para execução de fornecimento similar de complexidade tecnológica e operacional equivalente ou superior ao objeto desta contratação, ou ao item pertinente, por meio da apresentação de certidão(ões) ou atestado(s), fornecido(s) por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso;
- ii. Para fins da comprovação de que trata o item anterior, o(s) atestado(s) ou certidão(ões) deverá(ão) dizer respeito a contrato(s) executado(s) com a(s) seguinte(s) característica(s) mínima(s):
 - I. aptidão para comercialização e implementação de ambiente de datacenter.
- iii. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor;
- iv. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade do(s) atestado(s), apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do contratante e local em que foi executado o objeto contratado, dentre outros documentos;

4 – Definição e justificativa da natureza continuada dos serviços:

- 4.1. O objeto da contratação tem a natureza de serviço comum de caráter continuado, pois pode ser objetivamente especificado por meio de padrões usuais no mercado e características comuns pré-estabelecidas, além de ser fundamental para a execução das atividades finalísticas do CRQ-IV/SP de forma contínua, devendo ser contratado por meio de processo licitatório na modalidade pregão em sua forma eletrônica.
- 4.2. Os serviços serão prestados visando garantir a disponibilidade e o armazenamento seguro das informações controladas pelo CRQ-IV/SP.
- 4.3. A contratação se caracteriza por ser um serviço continuado. O contrato terá vigência de 36 (trinta e seis) meses, podendo ser prorrogado caso a CONTRATANTE tenha interesse.



- 4.4. Esses serviços possuem natureza permanente e ininterrupta, não sendo operacionalmente viável, submetê-los a alterações contratuais frequentes, o que traria riscos significativos à continuidade dos serviços, à segurança da informação e ao atendimento aos usuários. A adoção de uma vigência mais longa permite não só maior estabilidade operacional, mas também ganho de escala, economia contratual e coerência com os ciclos tecnológicos e estratégicos da instituição.
- 4.5. A presente contratação tem por objeto a prestação contínua de serviços de Infraestrutura como Serviço (IaaS), com o objetivo de garantir a disponibilidade permanente de uma infraestrutura de tecnologia da informação escalável, segura e com alta disponibilidade, destinada ao suporte de sistemas corporativos estratégicos do Conselho Regional de Química da 4ª Região.
- 4.6. Tais sistemas são considerados estruturantes por sustentarem funções essenciais da gestão administrativa, financeira e operacional, sendo indispensáveis à continuidade dos serviços prestados e à governança institucional. Diante da essencialidade dos sistemas envolvidos e dos benefícios técnicos e econômicos, conforme previsão do art. 114 da Lei nº 14.133/2021, verifica-se a possibilidade de vigência para contratação de até 15 (quinze) anos.
- 4.7. O CRQ-IV/SP reserva-se no direito de rescindir o contrato a qualquer momento, mediante comunicado antecipado de 30 (trinta) dias.

5 – Estimativas das quantidades:

- 5.1. Os serviços e seus quantitativos relacionados na tabela abaixo foram estimados considerando a infraestrutura de TIC existente no CRQ-IV/SP. Está previsto escalabilidade dos recursos visando garantir que os sistemas e recursos tecnológicos possam crescer conforme o aumento e/ou mudança na demanda.

Serviço	Servidores Virtuais e Recursos Computacionais (Ambiente de Produção)		
Recurso	Unidade	Qtde. Mínima	Qtde. Máxima
Processador	vCPU	0	20
Memória	GB	0	150

Serviço	Servidores e Recursos Computacionais (Ambiente de Desastre - DR)		
Recurso	Unidade	Qtde. Mínima	Qtde. Máxima
Processador	vCPU	22	40



Memória	GB	132	180
Armazenamento SSD	GB	6.500 (6.5TB)	13.000 (13TB)
Armazenamento HDD	GB	0	3.000 (3TB)
Instancia Protegida	Instancia	06	10

Serviço	Armazenamento		
Recurso	Unidade	Qtde Mínima	Qtde. Máxima
Tipo SSD	GB	0	15.000 (11TB)
Tipo HDD	GB	0	25.000 (25 TB)
Object Storage	GB	17.000 (17TB)	25.000 (25 TB)

Serviço	Conectividade		
Recurso	Unidade	Qtde. Mínima	Qtde. Máxima
L2L	Gbps	0	1
Internet	Mbps	0	500
IPv4	Unidade	0	10
IPv6	Unidade	0	10

Serviço	Solução de Proteção dos Dados		
Recurso	Unidade	Qtde. Mínima	Qtde. Máxima
Firewall	Instancia	1	2

Serviço	Solução de Backups		
Recurso	Unidade	Qtde Mínima	Qtde. Máxima
Licença de Backup	Instancia	1	15
Backup Office 365	Caixa	170	200
Repositório de Backup	GB	18.500 (18TB)	25.000 (25 TB)

Serviço	Detecção e Resposta de EndPoint		
Recurso	Unidade	Qtde Mínima	Qtde. Máxima
EndPoint	Instancia	0	30

Serviço	Recuperação de Desastres		
Recurso	Unidade	Qtde. Mínima	Qtde. Máxima
Padrão	Instancia	0	10
Avançado	Instancia	0	10
Armazenamento SSD	GB	0	20.000 (20 TB)
Armazenamento HDD	GB	0	20.000 (20 TB)



Serviço	Softwares e Licenciamentos			
Recurso	Unidade	Qtde. Mínima	Qtde. Máxima	
Windows Server 2022 ou superior	vCPU	0	30	
Windows Remote Desktop	Dispositivo	0	150	
Red Hat Enterprise	Instância	0	2	
Microsoft SQL Server Standard	vCPU	0	2	
Microsoft SQL Server Enterprise	vCPU	0	1	

Serviço	Operação, Suporte e Gerenciamento			
Recurso	Unidade	Qtde. Mínima	Qtde. Máxima	
Suporte Ambiente Microsoft	Hora	0	50	
Suporte Ambiente Red Hat	Hora	0	10	
Suporte Banco de Dados	Hora	0	50	
Suporte Firewall	Hora	0	50	

Serviço	Servidor Rack			
Recurso	Unidade	Qtde. Mínima	Qtde. Máxima	
Servidor 2U	Servidor	0	2	

Serviço	Appliance de Monitoramento			
Recurso	Unidade	Qtde. Mínima	Qtde. Máxima	
Appliance	Servidor	0	1	

Serviço	Collocation			
Recurso	Unidade	Qtde. Mínima	Qtde. Máxima	
Rack Unit	Rack Unit	0	6	

OBSERVAÇÃO:

5.2. O CRQ-IV/SP, inicialmente, contratará apenas os serviços:

5.2.1. Servidores Virtuais e Recursos Computacionais (Ambiente de Desastres);

5.2.2. Armazenamento;

5.2.3. Solução de Proteção de Dados;

5.2.4. Solução de Backup.



5.3. Para todos os serviços objeto desta licitação, o CRQ-IV/SP poderá contratar todos ou parcialmente os recursos, respeitando as regras de quantidades mínimas e máximas.

5.4. Os demais serviços que constam neste Estudo Técnico Preliminar poderão ser contratados a médio e longo prazo, considerando a necessidade de disponibilizar novos recursos computacionais em decorrência da mudança na demanda ou novos serviços que porventura necessite de mais recursos.

6 – Descrição da Solução:

Inciso I, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

6.1. CARACTERÍSTICAS DA SOLUÇÃO DE CLOUD COMPUTING

6.1.1. Todos os equipamentos, software, infraestrutura e sustentação, necessários à implementação da solução proposta, são de inteira responsabilidade da Contratada, que deverá realizar de forma continuada tarefas e rotinas que garantam o pleno funcionamento de toda a infraestrutura, de forma integral e ininterrupta, ou seja, "24x7x365" (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano) nas dependências da Contratada, mantendo em pleno funcionamento todo objeto da contratação.

6.1.2. Todos os equipamentos de hardware e software utilizados para a prestação de serviços devem ser de propriedade da CONTRATADA que deverá ser responsável pela operação e manutenção dos equipamentos, não sendo permitida a revenda ou intermediação de serviços de terceiros.

6.1.3. A CONTRATADA deverá gerenciar, monitorar, sustentar e operar de forma proativa todos os recursos disponibilizados para a CONTRATANTE de forma a garantir o correto funcionamento de todas as funcionalidades especificadas neste Termo de Referência, a partir de seu Centro de Operações de Rede (NOC), em regime 24x7 (24 horas por dia, 7 dias por semana).

6.1.4. A solução de Computação em Nuvem ofertada deve permitir a criação de uma ou mais VPC's (Virtual Private Cloud), de forma que a CONTRATADA possa provisionar uma seção da nuvem da solução ofertada isolada logicamente, onde é possível executar recursos da solução em uma rede virtual definida pela CONTRATADA, permitindo o controle total sobre seu ambiente de redes virtuais, incluindo a seleção do seu próprio intervalo de endereços IP, a criação de sub-redes e a configuração de tabelas de rotas e gateways de rede, para acessar recursos e aplicações com segurança e facilidade. Além disso, a CONTRATADA poderá criar uma conexão



de Hardware Virtual Private Network (VPN) entre seu datacenter corporativo e a VPC e aproveitar a nuvem da solução ofertada como uma extensão do seu datacenter corporativo.

6.1.5. A solução deverá ser escalável, de forma a permitir aumentar os recursos na infraestrutura de Cloud Computing da CONTRATADA para absorver a demanda complementar oriunda de picos de acesso ou expansão natural dos usuários em ambiente Cloud Computing.

6.1.6. Os servidores virtuais deverão ser disponibilizados em ambiente de Cloud Computing, em ambiente seguro e separados logicamente de outros clientes, com as seguintes funcionalidades:

- i. Implementar características de escalabilidade horizontal (novos servidores) e vertical (aumento de recursos do mesmo servidor), flexibilidade de configuração de memória, processador e disco.
- ii. Implementar a movimentação automática de servidores virtuais para redistribuição de carga e recuperação de falhas do ambiente físico.

6.1.7. É de responsabilidade da CONTRATADA o monitoramento do hardware e seus componentes, bem como a manutenção deles, identificando necessidades de reposições, adaptações e melhorias, procedendo chamados aos fornecedores, acompanhando, garantindo a devida solução aos problemas que porventura ocorram, observando os tempos definidos no Nível de Serviço Exigido e fornecendo Console de Gestão para monitoramento em tempo real de todos os recursos computacionais.

6.1.8. O monitoramento deverá ser feito de forma continuada, não sobrecarregando os equipamentos ou consumindo recursos da solução de Cloud Computing provisionada aos clientes.

6.2 CARACTERÍSTICAS DA INFRAESTRUTURA FÍSICA

6.2.1. A solução proposta deverá hospedar os dados em datacenter localizado em território nacional;

6.2.2. Para fins de segurança da informação os dados poderão ser replicados entre datacenters com no mínimo 40km de distância entre eles. Em caso de desastre no datacenter principal o ambiente deverá estar disponível do datacenter réplica.

6.2.3. Os serviços de Cloud Computing a serem prestados deverão ser baseados em infraestrutura de Datacenter, que deverá manter compatibilidade com padrões internacionais, e deverão



manter compatibilidade durante toda vigência do contrato.

- 6.2.4. As instalações físicas e recursos de infraestrutura que suportarão o ambiente crítico de serviço atenderão, no mínimo, às características aqui definidas de estrutura física, instalações físicas, energia elétrica, climatização, proteção contra incêndio, segurança física, infraestrutura de acesso à internet do Datacenter e segurança lógica do Datacenter.
- 6.2.5. Os datacenters da CONTRATADA deverão possuir um ambiente com alta disponibilidade, atendendo aos seguintes requisitos mínimos:
- i. Possuir certificação padrão TIER III;
 - ii. Garantir a disponibilidade imediata de energia elétrica através do fornecimento de sistemas de nobreaks independentes e redundantes
 - iii. Redundância no fornecimento de link de internet de trânsito (uplink) através da utilização de no mínimo dois links IP's de trânsito diferentes e independentes. A comprovação deste item deverá ser feita através de sites públicos na internet como o <https://bgpview.io/> ou <https://bgp.he.net>.
 - iv. Redundância no anúncio de suas rotas através do protocolo BGP através da disponibilização de no mínimo dois roteadores distintos e independentes.
 - v. Redundância no fornecimento de portas de rede de acesso, através da disponibilidade de no mínimo dois switches distintos e independentes com portas Gigabit Ethernet ou superior com ao menos duas portas disponíveis em cada switch.
- 6.2.6. A fim de se comprovar o atendimento a estes requisitos mínimos, o CRQ-IV/SP se reserva no direito de realizar uma vistoria técnica presencial no ambiente da CONTRATADA, a qualquer momento durante a vigência deste contrato, mediante agendamento prévio.

6.3 CONSOLE DE GESTÃO DO AMBIENTE CLOUD COMPUTING

- 6.3.1. Permitir o gerenciamento da infraestrutura de Computação em Nuvem de forma independente de softwares de cliente (VNC, Remote Desktop, SSH etc.), por meio de API (Application Programming Interface), acessada via browser, de forma segura (HTTPS), utilizando-se de recursos de autenticação.
- 6.3.2. O acesso via interface web browser não poderá permitir a visualização ou edição de qualquer



componente persistente a infraestrutura física que compõe a solução.

- 6.3.3. Possibilitar o cadastramento dos colaboradores da CONTRATANTE, inclusive, por perfil de acesso para administrar, operar ou consultar o ambiente de produção da solução na infraestrutura de Computação em Nuvem disponibilizada pela CONTRATADA.
- 6.3.4. Permitir selecionar modelos preexistentes (templates) de máquinas virtuais e sistemas operacionais.
- 6.3.5. Permitir personalizar modelos (templates) que melhor se adaptem às necessidades da CONTRATANTE.
- 6.3.6. Permitir modificar os recursos da Infraestrutura de Computação em Nuvem e atualizá-los de uma forma controlada e previsível, aplicando-se, quando necessário, controles de versionamento, devendo ser permitido o rastreamento das alterações históricas efetuadas no ambiente.
- 6.3.7. Disponibilizar console via interface gráfica afim de permitir o agendamento, realização de backups e horários de funcionamento por recurso (servidor; banco de dados, fileserver), por ambiente (produção) ou por etiqueta (classificação das soluções/sistemas).
- 6.3.8. Deverá ser disponibilizado um painel de controle (software de gestão para alojamento web) com as opções mínimas de: gerenciamento FTP, gerenciamento de arquivos, gerenciamento de banco de dados, verificação de estatísticas, gerenciamento de domínios;
- 6.3.9. Conexão a 2 pontos de troca de tráfego distintos;
- 6.3.10. Deverá possuir gerenciador de arquivos web;
- 6.3.11 Deverá possuir painel de gerenciamento de DNS.

6.4 MONITORAMENTO DE RECURSOS

- 6.4.1. A Contratada deverá oferecer Console de Gestão de fácil utilização e que permita criar e gerenciar os recursos e/ou grupo de recursos relacionados ao serviço de Computação em Nuvem por meio de web browsers.
- 6.4.2. A solução ofertada deverá permitir o monitoramento das máquinas virtuais, provendo o monitoramento do ambiente de Computação em Nuvem (serviços e recursos), de forma automatizada e abrangendo servidores, sistemas operacionais e recursos de comunicação,



em tempo real (24x7x365), visando detectar problemas (incidentes), no que tange à sustentação operacional e não a aplicação do Contratante.

- 6.4.3. Prover o monitoramento constante em amostras com granularidade mínima de 1 hora (24X7X365) dos serviços e recursos, visando detectar os problemas mais frequentes, informando a CONTRATANTE a ocorrência destes.
- 6.4.4. Deverá ser realizada pela Contratada a monitoração da qualidade e nível de utilização da infraestrutura de acesso à Internet, disponibilizada pela solução ofertada pela Contratada, bem como as resoluções em caso de problemas.
- 6.4.5. Deverá permitir a visualização dos indicadores de desempenho, falhas do ambiente e características e requisitos operacionais dos recursos gerenciados por meio do painel de apresentação (dashboard) Online (tempo real).
- 6.4.6. A solução ofertada deverá prover alarmes para a Console de Gestão de eventos, mostrando quais recursos estiveram acima do threshold, permitindo gerar relatório a partir dos eventos observados.
- 6.4.7 Para cada servidor virtual, deverá ser possível o acompanhamento e monitoramento dos seguintes recursos: vCPU, RAM, Tráfego de Rede (In/Out) e Disco.

6.5 SERVIDORES VIRTUALIZADOS E RECURSOS COMPUTACIONAIS

- 6.5.1. Todos os servidores virtuais deverão ser disponibilizados em ambiente de Cloud Computing, em ambiente seguro e separados logicamente de outros clientes, com as seguintes funcionalidades:
- 6.5.2. Implementar características de escalabilidade vertical (aumento/diminuição de recursos do mesmo servidor), incluindo flexibilidade de configuração de memória, processador e disco;
- 6.5.3. Permitir a criação, pela CONTRATANTE, de pelo menos 1 (uma) imagem (snapshot) dos servidores virtuais sem custo adicional;
- 6.5.4. Assegurar a comunicação segura e encriptada entre os próprios servidores e os clientes que farão acesso aos mesmos, através de protocolo seguro HTTPS, ou seja, todos os servidores deverão ser disponibilizados com certificados digitais SSL instalados.
- 6.5.5. Os recursos computacionais adicionais, poderão ser utilizados para agregação ou distribuição



entre os servidores virtualizados existentes ou para a criação de novos servidores virtuais;

- 6.5.6 Deverá ser considerado um pool de recursos computacionais para suprir a demanda de todas as máquinas virtuais do ambiente atualmente em produção e no mínimo com as seguintes características Processador e Memória.

6.6 ARMAZENAMENTO

- 6.6.1. O armazenamento disponível para as máquinas virtuais deverá considerar o armazenamento dos dados de forma persistente.
- 6.6.2. Permitir o gerenciamento de discos virtuais pela CONTRATANTE através do portal WEB, desde sua criação, exclusão, expansão e anexo as máquinas virtuais no ambiente (VPC).
- 6.6.3. O(s) volume(s) criado(s) anexado(s) às máquinas virtuais deverão ser reconhecidos(s) pelo sistema operacional como um dispositivo físico local.
- 6.6.4. A solução de armazenamento deverá permitir que a CONTRATANTE defina a política de uso dos discos virtuais das máquinas virtuais em seu ambiente (VPC).
- 6.6.5. O armazenamento disponível e não alocado deverá permitir as seguintes características:
- i. Expansão dos discos existentes das máquinas virtuais no ambiente (VPC)
 - ii. Inclusão de novos discos nas máquinas virtuais existentes no ambiente (VPC)
 - iii. Criação de novas máquinas virtuais no ambiente (VPC)
- 6.6.6. O armazenamento disponível deverá permitir que a CONTRATANTE defina através de políticas pré-existentes a seguinte carga de uso:
- i. ALTA PERFORMANCE (SSD)
 - ii. BAIXA PERFORMANCE (HDD)
- 6.6.7. OBJECT STORAGE
- i. Gerenciamento de quotas e permissões de acesso via interface WEB;
 - ii. Compatível com API S3;
- 6.6.8. Os dados deverão estar localizados em território nacional;
- 6.6.9. O tráfego de dados (Download e Upload) deve ser ilimitado;
- 6.6.10 Os dados deverão estar acessíveis imediatamente sem restrições de acesso.



6.7 CONECTIVIDADE

6.7.1. Link Ponto a Ponto

- i. A CONTRATADA deverá prover um link de dados ponto a ponto em fibra óptica garantindo a banda dedicada para upload e download entre o site da CONTRATANTE e o datacenter da CONTRATADA onde se encontram os equipamentos que compõem a solução de datacenter virtual. Este link será utilizado exclusivamente para os serviços de comunicação entre datacenters;
- ii. O volume de tráfego de dados ofertado deve ser ilimitado, tanto no sentido de download como upload, permitindo a transferência, via funcionalidades de backup e restauração, de volume ilimitado de dados.

6.7.2. IP's públicos

- i. A CONTRATADA deverá disponibilizar endereços IP fixos e públicos (válidos) para uso da CONTRATANTE de tal forma que lhe convir para uso em seu ambiente de produção.
- ii. A fim de garantir que o endereçamento IP utilizado pelo serviço de replicação de backup e recuperação de desastres não sofra constantes alterações e consequentes indisponibilidades, a CONTRATADA deverá possuir seu próprio bloco de endereçamento IP atribuído pelo órgão gestor dos serviços de numeração brasileira (NIC.br). A CONTRATADA deve comprovar que possui a devida alocação do bloco ofertado de seu ASN (Autonomous System Number) através de uma declaração do NIC.br.

6.7.3. Link de Internet VPC

- i. A CONTRATADA deverá prover na VPC (Virtual Private Cloud) um link de internet dedicado para uso e comunicação das instâncias virtuais para a internet.
- ii. O volume de tráfego de dados ofertado deve ser ilimitado, tanto no sentido de download como upload, permitindo a transferência, via funcionalidades de backup e restauração, de volume ilimitado de dados.

6.8 SOLUÇÃO DE PROTEÇÃO DE DADOS



6.8.1. Deverá ser fornecido solução de segurança do tipo Firewall com as seguintes características mínimas:

- i. A solução deverá suportar throughput (Taxa de Transferência) de, no mínimo, 15 Gbps com a funcionalidade de firewall habilitada;
- ii. A solução deve suportar Throughput (Taxa de Transferência) de, no mínimo, 0.9 Gbps com as seguintes funcionalidades habilitadas simultaneamente: Firewall, Controle de Aplicação e Prevenção de Ameaças (Anti-Malware, IPS, Application Control URL Filtering). Esta taxa deve referenciar-se a tráfego multiprotocolo em ambiente de produção, tráfego considerado de mundo real ou tráfego misto, ou seja, aquele que não faz referência apenas a um protocolo e/ou um tamanho de pacote para teste em condição ideal;
- iii. Suportar throughput (Taxa de Transferência) de, no mínimo, 1 Gbps de VPN IPsec;
- iv. Deverá suportar e incluir licenciamento para, no mínimo, 2.000 Túneis VPN Lan-to-Lan (ou Gateway-to-Gateway) com VPN IPsec;
- v. Deverá suportar e incluir licenciamento para, no mínimo, 32.000 usuários remotos (ou client-to-site) com VPN IPsec;
- vi. Deverá suportar e incluir licenciamento para, no mínimo, 500 usuários remotos (ou client-to-site) com VPN SSL;
- vii. Suporte a, no mínimo, 3.300.000 (três milhões e trezentos mil) conexões TCP simultâneas;
- viii. Suporte a, no mínimo, 140.000 (cento e quarenta mil) novas conexões TCP por segundo;
- ix. A solução deve possuir o licenciamento para, no mínimo, 10 sistemas virtuais lógicos (Contextos), independentes entre si e estar licenciado e/ou ter incluído sem custo adicional pelo menos 5 sistemas;
- x. A solução deve possuir, no mínimo, 2 (duas) interfaces no padrão 10 GbE;
- xi. A solução deve possuir, no mínimo, 8 (oito) interfaces no padrão 1GbE;

6.9 SOLUÇÃO DE BACKUP



- 6.9.1. A Contratada deverá disponibilizar serviços que permitam realizar backup e restore rápidos dos servidores virtuais com retenção em storage.
- 6.9.2. A solução deverá ser licenciada por máquina virtual hospedada no ambiente Cloud Computing;
- 6.9.3. As políticas de backup deverão ser configuradas conforme necessidades de tempo de retenção e periodicidade que o cliente desejar.
- 6.9.4. A fim de manter a integridade das informações e dos dados armazenados, a solução de Cloud Computing deverá garantir o backup das instâncias baseado nas características técnicas mínimas de uma solução de Backup conforme listadas abaixo:
- 6.9.5. Os Backups poderão ser completos do tipo imagem dos volumes, sendo executados de forma automática (agendada) ou através de comandos manuais. Os backups das bases de dados de aplicações de execução contínua deverão ser realizados sem interrupção dos serviços (backup on line), e deverá ser utilizada uma rede de alta velocidade evitando que o tráfego de backup afete a operação normal dos sistemas.
- 6.9.6. Para realização da funcionalidade Backup e Restore, a Contratada deverá disponibilizar solução completa, com todos os recursos necessários para executar as rotinas da CONTRATANTE, sendo que a solução de Backup deverá estar preparada para geração automática de imagens das máquinas virtuais /Snapshots, gravados em ambiente de armazenamento em nuvem da Contratada, que devem ser acessíveis aos recursos de Computação em Nuvem disponibilizados para a CONTRATANTE.
- 6.9.7. As políticas de backup poderão ser ajustadas para uma maior quantidade de backups diários e/ou retenção no repositório de armazenamento a ser disponibilizado para as cópias de segurança das instâncias contratadas respeitando a capacidade máxima contratada sem considerar eventuais ganhos com compressão e deduplicação.
- 6.9.8. Não serão permitidas soluções de backup de dados baseados em cópias realizadas de forma manual, nem baseadas em scripts automatizados, devendo ser utilizado um software de uso específico e dedicado para backup.
- 6.9.9. Não serão permitidas soluções de backup de dados baseados em sistemas operacionais gratuitos ou de código aberto.



- 6.9.10. A solução proposta deverá dispor de software profissional para gerência e execução de backup e restauração de dados em nuvem, com garantia de atualizações e expansões durante o período do contrato sem ônus financeiro para a CONTRATANTE.
- 6.9.11. Deverá ter a capacidade de testar a consistência do backup e replicação (Sistema Operacional, aplicação, máquina virtual), emitindo relatório de auditoria para garantir a capacidade de recuperação, sempre que solicitado.
- 6.9.12. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de serviços de diretório Microsoft Active Directory, possam recuperar objetos individuais como usuários, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.
- 6.9.13. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de banco de dados Microsoft SQL Server, possam recuperar objetos individuais, tais como bases, tabelas, registros, entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.
- 6.9.14. Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de “rastreamento de blocos modificados” (CBT – changed block tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação).
- 6.9.15. Deverá oferecer a possibilidade de armazenar backups de forma criptografada, bem como garantir o trânsito de informações sob esse esquema a partir do arquivo de backup, sem exigir criptografia do sistema de armazenamento.
- 6.9.16. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar.
- 6.9.17. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.
- 6.9.18. Deverá permitir criar uma cópia da máquina virtual de produção para criação de ambiente de homologação, testes ou desenvolvimento, em qualquer estado anterior, para a resolução de problemas, provas de procedimentos ou capacitação.



- 6.9.19. Deverá permitir a recuperação de mais de uma máquina virtual e pontos de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais.
- 6.9.20. O software deverá possuir painel de gerenciamento de ambiente de backup (dashboard) com suporte a visualização de todas as rotinas de backup.
- 6.9.21. O software deverá permitir a execução de backup de arquivos abertos em Windows, mesmo que estejam sendo alterados durante a operação e backup, sem necessidade de suspender a utilização de aplicações pelos usuários nem a conexão da rede. A cópia do arquivo salvo deverá ser idêntica ao arquivo residente em disco, quando do início da operação de backup.
- 6.9.22. O sistema deve prover quantidade ilimitada de restaurações, conforme as solicitações da CONTRATANTE, durante a vigência deste Contrato.
- 6.9.23. O console central de administração dos backups das máquinas virtuais deve ser via WEB e acessível via navegador utilizando protocolos HTTPS integrado a solução de Console de gestão do ambiente Cloud Computing.
- 6.9.24. Solução de backup para caixas de correio do Office365, conforme características abaixo:
- i. O painel de administração do backup e restore das caixas de correio poderá ser separado da administração dos backups das máquinas virtuais, porém deverá ser da mesma fabricante.

6.10 DETECÇÃO E RESPOSTA DE ENDPOINT

6.10.1. Requisitos gerais da solução:

- i. Solução de proteção contra ameaças avançadas, com funcionalidades de detecção, bloqueio, investigação e resposta a incidentes, incluindo console Web ou console gráfica do próprio fabricante para administração da solução e centralização de eventos.
- ii. Fornecimento da console de gerência, incluindo implantação dos agentes, documentação da arquitetura da solução e repasse de conhecimento



- iii. A Solução de gerência deverá contemplar todos os softwares e respectivas licenças necessárias ou adicionais para a instalação, configuração e funcionamento da solução de proteção.
- iv. A solução de proteção deve ser oferecida na última versão disponibilizada pelo fabricante.
- v. Na data da proposta, nenhum dos softwares componentes da solução de proteção ofertados poderão estar listados pelo fabricante com data definida para fim de suporte (“end of support”) ou fim de vendas (“end of sale”).

6.10.2. Requisitos e funcionalidades técnicos da solução:

- i. A solução de proteção deve ser capaz de detectar e bloquear em tempo real ameaças conhecidas e desconhecidas (zeroday), ataques file-less, ameaças persistentes avançadas (APTs), ransomwares, exploits e outros comportamentos maliciosos, sem depender exclusivamente de base de assinaturas ou heurísticas.
- ii. A solução de proteção deverá possuir funcionalidades específicas para prevenção contra a ação de ransomwares com capacidade de restauração dos arquivos comprometidos.
- iii. A solução de proteção deve ter a funcionalidade específica de impedir as técnicas de manipulação e randomização de memória impossibilitando a exploração de vulnerabilidades em aplicações.
- iv. A solução de proteção deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades.
- v. Efetuar a análise baseada em técnicas de machine learning, inteligência artificial e threat intelligence, permitindo a proteção contra-ataques que explorem vulnerabilidades, mesmo que ainda não existam patches de correção.
- vi. Realizar análise de comportamento com base nas táticas, técnicas e procedimentos (TTPs) listados no framework MITRE ATT&CK.
- vii. A análise dos artefatos deve ocorrer em pré-execução, ou seja, antes de serem executados no sistema operacional, evitando que a máquina seja infectada.
- viii. Detectar e bloquear ameaças que utilizem técnicas de ofuscação e sequestro de DLL.



- ix. Detectar e bloquear técnicas de evasão, incluindo process injection e uso de executáveis legítimos do Windows para rodar scripts e ações maliciosas.
- x. Reconhecer padrões e bloquear comportamentos potencialmente maliciosos ou o possuir mecanismos automáticos preventivos ou corretivos que sejam capazes de inibir as ações maliciosas resultantes de pelo menos 5(cinco) das ações listadas abaixo:
 - I. Rodar a partir diretórios incomuns (ex: diretório de dados, temp e lixeira);
 - II. Executar elevações de privilégio inesperadas;
 - III. Tentar se passar por processos do Windows;
 - IV. Estabelecer conexões de rede suspeitas (call back ou command & control);
 - V. Uso suspeito do PSEXEC;
 - VI. Invocação maliciosa através do Rundll;
 - VII. Exploração ou modificação do arquivo hosts;
 - VIII. Tentativa de invocação de Remote Shell.
- xi. Identificar e bloquear alterações suspeitas em chaves de registro e tarefas agendadas na máquina.
- xii. Proteger contra macros maliciosas, bem como scripts e comandos Powershell maliciosos.
- xiii. Bloquear exploits e payloads suspeitos do Metasploit.
- xiv. As análises poderão ser complementadas utilizando recursos em nuvem da solução, sem custos adicionais, onde será permitido apenas o envio de metadados dos artefatos sob análise, sem submissão do artefato em si ou seu conteúdo à nuvem.
- xv. O agente da solução deve realizar suas análises e bloqueios nas estações mesmo quando estiver sem conectividade com os servidores da solução e sem acesso à Internet.
- xvi. O agente da solução deve possuir proteção contra desinstalação e/ou desativação dos seus componentes, serviços e processos de forma não autorizada.
- xvii. Deve ser possível realizar a configuração de proxy no agente ou obter as configurações de proxy definidas no próprio sistema operacional.



- xviii. Deve ser possível exibir ou inibir alertas ao usuário em caso de detecção de alguma ameaça, conforme definição do administrador.
- xix. Deve ser possível definir as seguintes ações de resposta quando uma ameaça ou comportamento malicioso for detectado:
 - I. Ignorar;
 - II. Registrar em log;
 - III. Alertar;
 - IV. Bloquear;
 - V. Remover ou quarentenar;
- xx. Isolar a máquina, de maneira que ela perca a comunicação com a rede ou se comunique apenas com os servidores da solução ou com servidores e serviços definidos na política de isolamento.
- xxi. O agente deve ter a capacidade de fazer o isolamento da máquina por si só, sem precisar de nenhuma integração com outros softwares ou dispositivos de rede para isso.
- xxii. Deve ser possível ao administrador efetuar a liberação da máquina do isolamento via console de gerência ou fornecer uma chave para realizar a liberação.
- xxiii. A solução deve possuir funcionalidade de EDR e análise forense, provendo uma visão completa do fluxo do ataque e informações detalhadas sobre os comportamentos detectados, de forma a auxiliar e agilizar as ações de remediação.
- xxiv. A console deve oferecer uma linha do tempo gráfica, contendo toda a sequência de eventos que ocorreram durante a execução do malware, sendo possível ainda expandir os detalhes de cada informação.
- xxv. Devem ser coletadas as atividades de todos os artefatos analisados, contendo informações sobre interação com outros processos, arquivos e chaves de registro acessadas/modificadas, conexões de rede realizadas, dentre outras. Deve ser possível gerar relatório dessas informações.
- xxvi. A solução deve correlacionar os eventos de detecção e bloqueio de malwares, permitindo a visualização de relatório com todas as fases do ataque.



- xxvii. Deve ser possível configurar regras de exclusão (whitelists) determinando quais arquivos, diretórios, processos ou aplicativos não devem ser analisados pela solução.
- xxviii. A solução deve ser capaz de remover de forma ágil e eficaz outras soluções de antivírus instaladas nos equipamentos do CONTRATANTE ou possuir mecanismos que possibilitem essa remoção.
- xxix. A Solução deve ter a capacidade de implementar, no mínimo, cinco das seguintes funcionalidades:
 - I. Reputação de Arquivos (Com ou sem acesso à internet no EndPoint);
 - II. IPS de Próxima Geração;
 - III. Proteção de Navegadores;
 - IV. Aprendizado de Máquinas;
 - V. Análise Comportamental;
 - VI. Mitigação da Exploração de Memória;
 - VII. Controle e isolamento de Aplicações;
 - VIII. Controle de Dispositivos;
 - IX. Emulação para Malware;
 - X. Proteção ao ambiente de Active Directory;
 - XI. Mitigação de Exploração de Vulnerabilidades em aplicações conhecidas.
- xxx. Deve ter a capacidade de implementar a funcionalidade de “Machine Learning” utilizando como fonte de aprendizado a rede de inteligência do fabricante, correlacionando no mínimo as seguintes técnicas de proteção com os vetores de ataques, identificando não somente os aspectos maliciosos.
- xxxi. De forma opcional ou não obrigatória a solução poderá ser capaz de distribuir iscas no ambiente com o objetivo de detectar e interromper tentativas de infiltração, através da implementação de pelo menos:
- xxxii. Criação de entradas falsas de cache, como Cache de DNS a fim de enganar um invasor e identificar ações maliciosas no ambiente;
- xxxiii. Deve possibilitar a criação de arquivos falsos nas máquinas dos usuários;
- xxxiv. Deve possibilitar a criação e distribuição de senhas falsas nos sistemas afim de identificar invasores no ambiente;



- xxxv. Criação de compartilhamentos de rede falsos em desktops;
- xxxvi. Deve ser capaz de enviar alertas quando as “Isclas” falsas são acionadas e/ou modificadas;
- xxxvii. Deve ter a capacidade de revelar tentativas de ataques dentro da rede interna;
- xxxviii. De forma opcional ou não obrigatória, a solução poderá ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo um dos conhecidos comportamentos de exploração de vulnerabilidades:
 - I. SEHOP - Structured Exception Handler Overwrite Protection.
 - II. Heap Spray (Exploits que iniciam através do HEAP);
 - III. Java Exploit Protection;
- xxxix. De forma opcional ou não obrigatória, a solução poderá ser capaz de:
 - I. A solução poderá ter a capacidade de bloquear exploits que trabalham em nível de “shell code”.
 - II. A solução poderá ter proteção contra técnicas de reconhecimento do domínio, sendo capaz de detectar um invasor que utilize técnicas de movimentação lateral ou roubo de credenciais válidas;
 - III. A solução poderá proteger contra intrusões por processo, usuário e terminal;
 - IV. A solução poderá ser capaz de identificar vulnerabilidades, erros de configurações e possíveis Backdoors presentes no Active Directory;
 - V. A solução poderá ser capaz de proteger alterações no Active Directory sem a necessidade de instalação de agentes ou componentes adicionais nas estações de trabalho;
 - VI. A solução poder ser capaz de detectar e proteger roubos de credenciais no ambiente que utilizem a técnica Pass-the-Hash e Pass-the-Ticket;
- xl. Instalação dos agentes:
 - I. A solução deve ser compatível com as versões de Sistema Operacionais:
 - II. Para computadores de usuários finais (estações: desktop, workstation e notebooks);



- III. Microsoft Windows 10 (32-64bit) e superior em todas as suas distribuições (home, starter, professional, ultimate e enterprise).
 - IV. Para servidores de rede físicos ou virtuais
 - V. Microsoft Windows Server 2016 (64bit) e superior.
 - VI. Ser suportado em sistemas operacionais linux, tais como Ubuntu, CentOS, Debian, Oracle Linux, Red Hat Enterprise, SUSE Linux Enterprise (32-64bit).
 - VII. O agente deve suportar sua instalação em Sistemas Operacionais virtualizados em ambiente Vmware.
-
- xli. O agente não deve impactar a performance das estações e servidores, gerando baixo consumo de CPU, memória, disco e rede.
 - xlvi. Deve ser possível a instalação e atualização dos agentes de forma manual ou remota, com suporte à distribuição do agente por ferramentas de terceiros, incluindo o System Center Configuration Manager (SCCM) da Microsoft.
 - xlvi. A instalação deve ser feita de forma silenciosa, sem interação com o usuário e sem necessidade de acesso à Internet.
 - xlvi. Deve ser possível permitir a desinstalação ou alteração da configuração do agente mediante requisição de senha ou token gerados pela console de gerência.
 - xlvi. Deve ser possível impedir alterações na configuração do agente por usuários ou processos não autorizados.
 - xlvi. Toda a solução deverá funcionar com agente único na estação de trabalho e servidores físicos e/ou virtuais a fim de diminuir o impacto ao usuário final;
 - xlvi. Para equipamentos que não podem se conectar à internet, devido a regras de negócio e/ou restrições impostas pelo próprio equipamento, a solução deve possibilitar a instalação de um componente on-premises, para que tais equipamentos possam ser gerenciados, atualizados e protegidos.
 - xlvi. Toda a solução deverá funcionar com agente nas estações de trabalho e servidores físicos e/ou virtuais a fim de diminuir o impacto ao usuário final. Será permitido agentes múltiplos para o atendimento deste requisito.

6.10.3. Console de Gerência:



- i. A solução deve oferecer console de gerência via protocolo web seguro ou console do próprio fabricante.
- ii. Caso a console seja Web, deve ser compatível com pelo menos dois dos seguintes navegadores: Microsoft Edge 41 ou superior; Google Chrome 70 ou superior; Mozilla Firefox 60 ou superior.
- iii. A console deve funcionar plenamente sem requerer a instalação de plug-ins, drivers, Java e flash player.
- iv. Permitir no mínimo 5(cinco) acessos simultâneos.
- v. A console e os agentes da solução devem possuir interface em português ou inglês.
- vi. Toda comunicação da solução deve ocorrer de forma criptografada usando protocolo seguro conforme padrão aceito pela indústria.
- vii. Permitir a configuração de perfis com permissões agrupadas que possam ser vinculados às contas de acesso à solução, para possibilitar a segregação de funções.
- viii. Suporte à criação de usuários, permitindo senhas de no mínimo 8 caracteres de 3 ou mais tipos, como: letras maiúsculas, letras minúsculas, dígitos numéricos e caracteres especiais.
- ix. A solução de console de gerência, deve ser possível configurar autenticação em múltiplos fatores.
- x. Permitir ao administrador criar diferentes políticas de segurança e aplicá-las a diferentes grupos de máquinas de acordo com seus atributos.
- xi. Registro em log de todas as ações de detecção e bloqueio de malware e comportamento malicioso.
- xii. Deve ser possível efetuar busca no log pelo IP de Origem, IP de destino, nome da máquina, nome do processo, arquivo e chave de registro.
- xiii. Deve ser possível efetuar o “drill down” das consultas realizadas a fim de avaliação mais detalhada das ocorrências.
- xiv. A partir dos eventos exibidos na console, deve ser possível tomar ações como quarentenar a máquina, adicionar o artefato a blacklist ou lista de exclusão (whitelist), dentre outras.
- xv. Permitir a geração de relatórios, consulta em log ou dashboard para visualizar no mínimo as informações abaixo:



- I. Eventos de ameaças;
 - II. Eventos de comportamentos suspeitos;
 - III. Malwares detectados e bloqueados;
 - IV. Computadores infectados.
- xvi. Deve ser possível exportar os relatórios para o formato CSV ou PDF.
- xvii. Permitir a configuração de alertas em tempo real de ameaças com envio de e-mail a usuários pré-definidos.
- xviii. A solução deve manter log de auditoria com registro das configurações realizadas por qualquer usuário ou administrador do sistema.
- xix. Permitir a visualização do inventário das máquinas que possuem o agente instalado, contendo no mínimo as seguintes informações:
- I. Nome da máquina;
 - II. Endereço IP;
 - III. Versão do sistema operacional (incluindo a versão do Service Pack);
 - IV. Versão do agente;
 - V. Política aplicada.
- xx. A partir do console de gerenciamento da solução, deve ser possível identificar o equipamento que está sofrendo ataques e comandar o agente de EndPoint para que aquele determinado equipamento seja movido para uma área de quarentena.

6.10.4. Monitoramento Assistido:

- i. Este serviço tem por objetivo operacionalizar as atividades de monitoração, detecção e resposta a incidentes de segurança, tratando os incidentes de forma coordenada, organizada e eficaz conforme necessidade do CONTRATANTE.
- ii. Deverá ser realizado de forma remota, externamente à CONTRATANTE, em dependências sob responsabilidade da CONTRATADA;
- iii. Deverá atuar na resposta à incidentes e ser realizado em língua portuguesa com monitoração em regime 12x5 (doze horas e cinco dias por semana);
- iv. Este serviço deverá ser prestado por equipe própria da CONTRATADA ou pela fabricante da solução;



- v. Este serviço deverá interagir com o CONTRATANTE via sistema de gestão e orquestração de incidentes de segurança da informação, sistemas disponibilizados pelo CONTRATANTE, ligação telefônica e correio eletrônico;
- vi. As solicitações e respostas de informações adicionais sobre os incidentes, como logs e evidências, devem ser anexadas ao tíquete registrado na ferramenta;
- vii. A CONTRATADA deverá garantir a prestação de serviço com disponibilidade mensal de 97% no regime de monitoração 12x5(doze horas e cinco dias por semana). Em casos de indisponibilidade, esta não deverá atingir períodos superiores a 4 horas consecutivas;
- viii. A CONTRATADA deverá apresentar plano de continuidade para a prestação deste serviço; será considerado incidente de segurança qualquer ação que vise comprometer a integridade, a confidencialidade das informações ou a disponibilidade dos serviços de tecnologia da informação do CONTRATANTE;
- ix. O serviço deverá atender os seguintes requisitos:
 - I. Monitorar ferramentas de segurança;
 - II. Monitorar o armazenamento dos logs de eventos e incidentes de segurança;
 - III. Monitorar sistema de gestão, orquestração e automação de incidentes de segurança da informação, controlando eventos, alertas, painéis e incidentes;
 - IV. Iniciar tratamento de incidentes em até 10 min;
 - V. Realizar triagem, classificação e categorização de eventos de segurança da informação;
 - VI. Realizar triagem, classificação e categorização de incidentes de segurança da informação, também identificando casos de falso positivo;
 - VII. Identificar incidentes de segurança da informação; Registrar, escalar e notificar incidentes de segurança da informação;
 - VIII. Registrar, escalar e notificar incidentes de segurança da informação;
 - IX. Realizar coleta de dados, informações e evidências para inclusão no registro do evento ou incidente;
 - X. Executar ações de mitigação, contenção, diagnóstico, resolução e outros procedimentos necessários para tratamento de incidentes de segurança da informação, solicitados pelo CONTRATANTE;



- XI. Interagir com a ETIR e demais equipes da CONTRATANTE, podendo realizar ações em conjunto;
- XII. Registrar e documentar ações e procedimentos realizados;
- XIII. Emitir relatório semanal estatístico das operações realizadas;
- XIV. Emitir relatórios conforme necessidade, periodicidade e padrões estabelecidos pela CONTRATANTE;
- XV. Apoiar na definição, documentação e manutenção de Política de Gerenciamento de Eventos, contendo diretrizes para geração, coleta, retenção e classificação de eventos e monitoramento de logs;
- XVI. Apoiar na definição, documentação e manutenção de estratégia de visibilidade de ameaças, devendo abordar: rotinas, periodicidade, métodos para identificação de novos casos de uso, utilização de fontes de visibilidade e inteligência de ameaças;
- XVII. Apoiar na definição, documentação e manutenção das normas, diretrizes e Política de Segurança da Informação e Comunicação da CONTRATANTE, visando refletir as definições instituídas por esses serviços de monitoramento;
- XVIII. Apoiar na Análise de Requisitos Regulatórios, Contratuais e Legais que se referem à segurança da informação e aplicáveis a CONTRATANTE;
- XIX. Apoiar na avaliação de Helth Check das soluções de segurança do CONTRATANTE, validando o mesmo e apresentando recomendações;
- XX. Apoiar na definição de ajustes e configuração de ferramentas de Segurança, apresentando recomendações a serem realizadas pela equipe técnica da CONTRATANTE.
- XXI. Apoiar na realização de Avaliação da Utilização de ferramentas de Segurança, observando: regras, alertas, painéis, fontes de dados, automatizações, integrações, relatórios e dimensionamento; apresentar recomendações e indicações de melhores práticas no que se refere à monitoração, análises, casos de uso de forma eficiente; e participar da implementação das recomendações quando necessário;
- XXII. Realizar Avaliação de Performance, com base nas métricas e indicadores definidos;



- XXIII. Gerar subsídios e recomendações para elaboração de conteúdo para divulgação de definições e orientações de segurança da informação e cibernética, a serem utilizados em ações de cultura e conscientização;
- XXIV. Apoiar na definição, documentação e manutenção de linha base (baseline) de comportamento para monitoração do ambiente de TI da CONTRATANTE, ajustando métricas e limiares de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção;
- XXV. Interagir com o sistema do CONTRATANTE para o processo de Gestão de Mudanças, Gestão de Incidentes de TI Gestão de requisições.

6.10.5. Instalação da solução e repasse de conhecimento.

- i. A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deverá ser realizada pela Contratada ou pelo fabricante da solução presencialmente na Sede do CONTRATANTE, em dias úteis, no período das 8h00 às 12h00 e das 14h00 às 18h00.
- ii. A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deve ser executada por pessoal especializado, qualificado e com certificação na solução.
- iii. A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deverá ser concluída em 30 (trinta) dias corridos para a sede do CONTRATANTE, contados a partir da assinatura da Ordem de Serviço
- iv. A instalação compreenderá:
 - I. Implantação de todos os componentes em sua última versão estável.
 - II. Configuração completa da solução, incluindo o apoio na definição de políticas e melhores práticas de segurança.
 - III. Configuração de dashboards, relatórios e alertas, de maneira coordenada com o CONTRATANTE.
 - IV. Customização dos pacotes de instalação dos agentes e distribuição a todas as estações do CONTRATANTE.
 - V. Instrução da equipe técnica do CONTRATANTE para a integração da a solução com ferramenta SIEM ou envio para servidor de registro de logs (Syslog).



- VI. Documentação da topologia da solução, relatório das atividades e configurações realizadas.
- VII. Apresentação da solução configurada e implantada.
- VIII. Deverá ser realizado repasse de conhecimento da solução de gerência para 1 grupo de até 4 pessoas, oferecido por técnico certificado na solução.
- IX. No repasse de conhecimento deve ser utilizado material em português.
- X. Não é necessário que o repasse seja feito para um grupo fechado do CONTRATANTE e o mesmo pode ser realizado de forma remota.
- XI. O repasse de conhecimento deve conter parte teórica e prática, incluindo tópicos sobre a instalação, uso, configuração, resolução de problemas da solução, análise de relatórios, respostas a incidentes, introdução ao Framework MITRE ATT&CK e outros.
- XII. As datas dos repasses de conhecimento devem ser previamente combinadas com o CONTRATANTE.
- XIII. Todas as despesas do repasse de conhecimento devem correr por conta da Contratada.
- XIV. O CONTRATANTE se reserva o direito de solicitar novo repasse caso aquele oferecido venha a ser questionado com relação à qualidade ou à carga horária.
- XV. Deverá ser disponibilizado formulário de avaliação (online ou impresso) e a média das notas deverá ser superior a 80%. Caso a média das notas seja inferior a 80% a contratada deverá ministrar novo repasse.
- XVI. A fornecedora e/ou fabricante da solução poderá, a qualquer tempo, durante a vigência do contrato, sem ônus extra para o CONTRATANTE, oferecer participação em seminários, conferências, visitas técnicas, eventos educacionais e treinamentos não previstos nesta especificação técnica, desde que relacionados ao objeto contratado.

6.11 RECUPERAÇÃO DE DESASTRES



- 6.11.1. Deverá fornecer solução de recuperação de desastres, baseado em replicação automatizada entre os datacenters da CONTRATADA.
- 6.11.2. A solução deverá ser integrada a mesma solução de gerenciamento do ambiente de máquinas virtuais, não sendo permitido utilização de software externos.
- 6.11.3. Garantir a proteção e replicação automatizada de máquinas virtuais.
- 6.11.4. Permitir a criação de planos de recuperação personalizáveis.
- 6.11.5. Deverá possuir funcionalidade de testes de plano de recuperação sem impacto.
- 6.11.6. Permitir a recuperação orquestrada quando necessário.
- 6.11.7. Permitir a replicação e recuperação para outro ambiente de Cloud Computing.
- 6.11.8. Permitir a utilização do ambiente em nuvem como datacenter secundário ou como um ambiente de recuperação.
- 6.11.9. Fornecer o monitoramento e envio de alertas do estado de suas instâncias protegidas.
- 6.11.10. A solução deverá permitir a reconfiguração das interfaces de rede destino.
- 6.11.11. A solução deverá disponibilizar a réplica de armazenamento em um segundo datacenter isolado do armazenamento de origem.
- 6.11.12. O armazenamento disponível para as máquinas virtuais replicadas deverá considerar o armazenamento dos dados de forma persistente.
- 6.11.13. O armazenamento da réplica disponível deverá permitir que a CONTRATANTE defina através de políticas pré-existentes a seguinte carga de uso:
- i. ALTA PERFORMANCE (SSD)
 - ii. BAIXA PERFORMANCE (HDD)
- 6.11.14. Solução de Desastre Padrão
- i. A solução de desastres padrão deverá ser licenciada por máquina virtual.
 - ii. A solução de desastre padrão deverá ser entregue com uma política de replicação a cada 24 horas.
- 6.11.15. Solução de Desastres Avançado
- i. A solução de desastre avançada deverá ser licenciada por máquina virtual.
 - ii. A solução de desastre avançada deverá ser entregue com uma política de replicação para no mínimo 15 minutos de RPO (Recovery Point Object).



- iii. A solução de desastre avançada deverá ser entregue com a funcionalidade de retenção para os pontos no tempo, provendo no mínimo 7 dias de retenção.
- iv. Caso haja necessidade de ligar o servidor ora replicado no ambiente da CONTRATADA, deverá ser considerado o custo da estrutura de RECUPERAÇÃO DE DESASTRES. Após 7 dias de utilização o custo será o de SERVIDORES VIRTUAIS E RECURSOS COMPUTACIONAIS EM AMBIENTE DE PRODUÇÃO.

6.12 SOFTWARES E LICENCIAMENTO

- 6.12.1. Todos os licenciamentos necessários para a prestação dos serviços de Cloud Computing, conforme descrito neste Termo de Referência, serão responsabilidade da contratada.
- 6.12.2. Durante a vigência do contrato, a Contratada deverá fornecer os seguintes softwares licenciados:
 - i. Windows Server na sua versão mais recente;
 - ii. Red Hat Enterprise Linux na sua versão mais recente;
 - iii. Windows Remote Desktop na sua versão mais recente;
 - iv. Microsoft SQL Server Standard;
 - v. Caso haja a requisição de uso do licenciamento SQL Server Standard, deverá ser considerado o consumo mensal para no mínimo 4 vCPUs.
 - vi. Microsoft SQL Server Enterprise;
 - vii. Caso haja a requisição de uso do licenciamento SQL Server Enterprise, deverá ser considerado o consumo mensal para no mínimo 4 vCPUs.
- 6.12.3. Os softwares poderão ser atualizados pela contratada durante toda a vigência do contrato.
- 6.12.4. A solução deve permitir licenciamentos atuais de posse desta Administração, conforme os parâmetros de licenças determinados, não se limitando a estes.

6.13 OPERAÇÃO, SUPORTE E GERENCIAMENTO

- 6.13.1. A CONTRATADA deverá prover todo o suporte e gestão da solução ofertada.



- 6.13.2. É responsabilidade da CONTRATADA monitorar a solução 24 x 7 x 365 (vinte e quatro horas, sete dias por semana, 365 dias por ano) para garantia da disponibilidade dela.
- 6.13.3. A CONTRATADA será responsável por operar e gerenciar as tarefas de backup de acordo com as solicitações realizadas pelo time da CONTRATANTE, devendo adicionar, alterar ou remover tarefas e rotinas de backup, de acordo com as solicitações.
- 6.13.4. A CONTRATADA será responsável em verificar a execução das rotinas e tarefas de backup.
- 6.13.5. Em casos de falha, a CONTRATADA deverá notificar prontamente o time da CONTRATANTE, verificar a causa raiz da falha, e sendo possível a correção, corrigir e executar novamente a tarefa.
- 6.13.6. A CONTRATANTE terá direito a um número ilimitado de alterações mensais nas políticas e rotinas vigentes em seu cenário de backup sem qualquer custo adicional.
- 6.13.7. A CONTRATADA deverá enviar mensalmente relatório estatístico das rotinas de backup.
- 6.13.8. A CONTRATADA deverá fornecer suporte técnico na modalidade 8 x 5 (8 horas por dia e 5 dias por semana) em língua portuguesa, para sanar dúvidas quanto da solução, sua configuração ou quaisquer outros assuntos relacionados à solução, através de suporte telefônico, por e-mail e através de um sistema online de chamados.
- 6.13.9. Em casos de acionamento de desastre, restaurações de bancos ou que seja necessária a restauração baremetal de um ou mais servidores, a CONTRATADA deve disponibilizar time técnico devidamente qualificado e de forma presencial nas dependências da CONTRATADA para a realização ou acompanhamento das tarefas.
- 6.13.10. A equipe técnica deverá estar alocada em até no máximo 4 horas na CONTRATANTE, após a constatação efetiva do desastre.
- 6.13.11. Durante a execução deste serviço a CONTRATADA se obriga a manter profissional(ais) com todas as qualificações.
- 6.13.12. SUPORTE A AMBIENTE MICROSOFT
- i. Alguns serviços a serem executados incluem, mas não se limitam a:
 - I. Auxílio na migração de servidores Windows 2016 para Windows 2022;
 - II. Auxílio na migração de servidores Windows 2016 para Windows 2025;
 - III. Auxílio na atualização da estrutura de domínio para ambiente Windows 2022;
 - IV. Auxílio no troubleshooting de problemas de operação;
 - V. Auxílio no planejamento de Life-cycle de servidores;



VI. Auxílio na implantação de novos serviços e rotinas pertinentes ao domínio.

6.13.13. SUPORTE A AMBIENTE RED HAT

- i. Alguns serviços a serem executados incluem, mas não se limitam a:
 - I. Suporte na migração de servidores;
 - II. Suporte na atualização da estrutura;
 - III. Suporte no troubleshooting de problemas de operação;
 - IV. Suporte no planejamento de Life-cycle de servidores;
 - V. Suporte na implantação de novos serviços e rotinas pertinentes ao ambiente.

6.13.14. SUPORTE A BANCO DE DADOS

- i. Alguns serviços a serem executados incluem, mas não se limitam a:
 - I. Suporte no monitoramento
 - II. Suporte no troubleshooting de problemas de operação;
 - III. Suporte na implantação de novos serviços e rotinas pertinentes ao banco de dados.

6.13.15. SUPORTE A AMBIENTE DE FIREWALL

- i. O serviço deve ser prestado por profissional certificado pela solução NSE4, SNSA, JNCIP, PCNSA ou equivalentes (certificação ativa ou desativa) ou especialista em solução de segurança baseada em firewall.
- ii. Alguns serviços a serem executados incluem, mas não se limitam a:
 - I. Suporte na migração das regras do firewall existente para o firewall em nuvem;
 - II. Suporte no troubleshooting de problemas de operação;
 - III. Suporte na implantação de novos serviços e rotinas pertinentes ao ambiente.

6.14 SERVIDOR RACK

6.14.1. Gabinete

- i. Gabinete para instalação em rack de 19” através de sistema de trilhos deslizantes;
- ii. Altura mínima de 2U;
- iii. Deve possuir botão liga/desliga na parte frontal do equipamento;



- iv. Possuir display ou leds embutido no painel frontal do gabinete para exibição de alertas de funcionamento dos componentes internos, tais como falhas de memória RAM, fontes de alimentação, disco rígido e ventilador;
- v. Deve possuir suporte de no mínimo 24 baias para instalação de discos rígidos de 2.5 polegadas padrão SAS ou SATA;
- vi. Deverá ser entregue junto com o servidor, um kit de fixação para rack, do tipo retrátil, permitindo o deslizamento do servidor e a organização dos cabos de alimentação e dados a fim de facilitar sua manutenção;
- vii. Deve possuir sistema de ventilação redundante e hot-pluggable para que a CPU suporte a configuração máxima e dentro dos limites de temperatura adequados para o perfeito funcionamento do equipamento, e que permita a substituição mesmo com o equipamento em funcionamento.

6.14.2. Fonte de Alimentação

- i. Mínimo de 2 (duas) fontes, suportando o funcionamento do equipamento na configuração ofertada mesmo em caso de falha de uma das fontes;
- ii. Deverá ser fornecido com sua quantidade máxima de fontes;
- iii. As fontes deverão ser redundantes e hot-pluggable permitindo a substituição de qualquer uma das fontes em caso de falha sem parada ou comprometimento do funcionamento do equipamento;
- iv. A fonte deve ter potência mínima de 2000 watts;
- v. As fontes devem possuir tensão de entrada de 100-240VAC a 60Hz;
- vi. Deverá acompanhar cabo de alimentação para cada fonte de alimentação fornecida.

6.14.3. Processador

- i. Equipado com 2 (dois) processadores de 32 (trinta e dois) núcleos, com arquitetura x86;
- ii. Deverá implementar mecanismos de gerenciamento do consumo de energia;
- iii. Deve suportar conjunto de instruções estendido compatível com padrão AVX-512;
- iv. Consumo de até 270W;
- v. Tecnologia de no mínimo 10nm;
- vi. Frequência de clock interno de no mínimo 2.1 GHz;



- vii. Controladora de memória com suporte a DDR4 de no mínimo 4400 MHz, oferecendo no mínimo 6 canais de memória;
- viii. Link de comunicação do processador com o restante do sistema de 16 GT/s;
- ix. Memória cache de 60 MB – L3

6.14.4. Desempenho

- i. O processador ofertado deverá ter índice SPEC CPU2017 Floating Point Rate Results (Floating Base) auditado de no mínimo 610 pontos para 2 processadores. Os índices SPEC CPU2017 Floating Point Rate Results (Floating Point) utilizados como referência serão validados junto ao site da Internet <http://www.spec.org/Standard Performance Evaluation Corporation>. Não serão aceitas estimativas para modelos / famílias de processadores não auditados pelo SPEC, resultados obtidos com a utilização de servidores em cluster, bem como estimativas em resultados inferiores ao mínimo especificado;
- ii. Não será aceito modelo de servidor não auditado pelo Standard Performance Evaluation Corporation ou auditado antes de 2017.

6.14.5. Memória RAM

- i. Módulos de memória RAM tipo DDR5 RDIMM (Registered DIMM) e velocidade de, no mínimo, 4800 MT/s;
- ii. Deve possuir no mínimo 32 slots de memória DIMM;
- iii. Suportar expansão de memória RAM para até no mínimo 8 TB (Oito Terabytes)
- iv. Deverá possuir 2 TB de memória distribuídos em módulos de no mínimo 64GB;
- v. Só será aceita memórias do tipo LRDIMM ou RDIMM para a funcionalidade de memória RAM.

6.14.6. Circuitos Integrados (Chipset) e Placa Mãe

- i. O chipset deve ser da mesma marca do fabricante do processador;
- ii. Suportar, no mínimo, 4 (quatro) slots PCI Express 3.0, com a adição de módulos;
- iii. Placa mãe da mesma marca do fabricante do equipamento, desenvolvida especificamente para o modelo ofertado. Não serão aceitas placas de livre comercialização no mercado;
- iv. A Interface LOM deverá permitir substituição em campo, sem a necessidade de troca da placa mãe.



6.14.7. Controladora de Vídeo

- i. Deve ser do tipo on board (integrado na placa mãe);
- ii. Capacidade da memória cache de vídeo ou da placa de vídeo: mínimo de 16 MB (dezesesseis megabytes);
- iii. Resolução gráfica de 1280 x 1024 pixels ou superior.

6.14.8. PLACA GPU

- i. Deverá ser fornecido 1 (uma) placa de Processamento GPU para cada servidor com dimensões adequadas para gabinete servidor rack com altura denominada “full-height” (perfil alto), ocupando slot simples (single slot) ou slot duplo (dual slot);
- ii. Será de responsabilidade da CONTRATADA a substituição da fonte de alimentação do servidor para compatibilidade da placa de vídeo, caso haja a necessidade;
- iii. Consumo máximo de potência de 300W;
- iv. Memory bus interface de 5100 bits no mínimo;
- v. GPU Clock Base de 760MHz no mínimo;
- vi. Memória de Vídeo: 80GB ou mais, com largura de banda (Memory bandwidth) de, no mínimo, 1900GB/s
- vii. Bus Type: Compatível com especificação PCI Express 4.0 ou superior x16.
- viii. Suporte a vGPU 11.x (or later): Virtual Compute
- ix. Suporte a GPU Multi-Instância provendo até 7 instâncias GPU.
- x. Suporte à adição de placas de vídeo idênticas em um único domínio de processamento, garantindo no mínimo banda de 600 Gbytes por segundo.

6.14.9. Bios e Segurança

- i. BIOS desenvolvida pelo mesmo fabricante do equipamento não sendo aceitas soluções em regime de OEM ou customizadas;
- ii. A BIOS deve possuir o número de série do equipamento e campo editável que permita inserir identificação customizada podendo ser consultada por software de gerenciamento, como número de propriedade e de serviço;
- iii. A BIOS deve possuir opção de criação de senha de acesso, senha de administrador ao sistema de configuração do equipamento;
- iv. Deve ser atualizável por software;



- v. As atualizações de BIOS/UEFI devem possuir (assinatura) autenticação criptográfica segundo as especificações NIST SP800-147B e NIST SP800-155.
- vi. Deve possuir funcionalidade de recuperação de estado da BIOS/UEFI a uma versão anterior gravada em área de memória exclusiva e destinada a este fim, de modo a garantir recuperação em caso de eventuais falhas em atualizações ou incidentes de segurança.
- vii. Deverá ser fornecido com Módulo TPM 2.0;
- viii. Deverá ser fornecido tampa frontal;
- ix. Deverá emitir alerta de abertura do gabinete;
- x. Por solicitação da licitante o equipamento poderá ser fornecido de fábrica com senha única, individual e exclusiva afixada em uma etiqueta de difícil remoção;

6.14.10. Portas de Comunicação

- i. Todos os conectores das portas de entrada/saída devem ser identificados pelos nomes ou símbolos;
- ii. Deverá ser fornecido com 3 portas USB;
- iii. Possuir, no mínimo, 2 (duas) portas de vídeo padrão VGA (DB-15) ou Displayport, uma localizada na parte frontal do gabinete e outra na parte traseira do gabinete;
- iv. Possuir, capacidade de no mínimo, 01 (uma) porta serial (DB-9).
- v. Possuir porta USB frontal dedicada para gerência.

6.14.11. Portas de Rede

- i. Interface de rede 10 Gbps
- ii. Possuir 04 (quatro) interfaces de rede 10Gb SFP+;
- iii. Suportar taxa de transferência 10Gbps;
- iv. Suporte ao protocolo de virtualização VMQ
- v. Suporte ao protocolo VXLAN
- vi. Possuir tecnologia de processamento TCP/IP offload LSO, RSS e TSS

6.14.12. Controladora RAID

- i. Controladora RAID, compatível com discos rígido padrão SAS 12Gb/s e SATA 6Gb/s;
- ii. Memória cache de no mínimo, 2GB (dois gigabytes) sendo que esta quantidade total de memória cache poderá ser atendida através de uma ou no máximo duas placas instaladas no servidor;



- iii. Suportar e implementar RAID 0, 1, 5, 6, 10, 50 e 60;
- iv. Suportar a criação de RAID por API;
- v. Suportar expansão de capacidade de formatação on-line;
- vi. A controladora RAID deverá possuir quantidade de canais para atender a todos os discos do chassi ofertado.
- vii. Permita detecção e recuperação automática de falhas e reconstrução, também de forma automática, dos volumes de RAID sem impacto para as aplicações e sem necessidade de reiniciar o equipamento;
- viii. Deverá permitir a operação em modo RAID e pass-through em discos distintos. Ou fornecer controladora RAID e controladora pass-through.
- ix. Suporte a recursos de hot swap para as unidades de disco rígido;
- x. Suportar implementação de disco Global Hot-spare;
- xi. Suportar migração de nível de RAID;
- xii. Suportar Self-Monitoring Analysis and Reporting Technology (SMART).

6.14.13. Armazenamento

- i. Armazenamento bruto (raw) composto por, no mínimo, 4 (quatro) unidades do dispositivo de armazenamento de dados do tipo SSD de, no mínimo, 7.68 TB cada.
- ii. Deve ser do tipo hot plug e hot swap, que permita sua substituição sem necessidade de desligar o equipamento, garantindo a continuidade das operações sem impacto para as aplicações;

6.14.14. Dispositivo para instalação do sistema operacional:

- i. Deve possuir dispositivos internos do tipo M.2, redundantes (espelhado), para inicialização de S.O com capacidade mínima de 480GB. Caso a solução ofertada não possua estes dispositivos, devem ser fornecidos dois discos do tipo SSD de, no mínimo, 480GB ligados em RAID1 através da controladora de discos / M.2 especificada; Estes discos deverão ser dedicados para a instalação do sistema operacional ou de virtualização;
- ii. Deve ser fornecida uma controladora de RAID exclusiva e dedicada para estes discos suportando configuração mínima de RAID 1 (mirroring).
- iii. Estes discos deverão ser dedicado para a instalação do sistema operacional, ou de virtualização e ou hiperconvergência.



- iv. Não será aceita soluções baseadas em cartão SD ou similar

6.14.15. Sistema Operacional

- i. Acompanhar mídia de inicialização e configuração do equipamento contendo todos os drivers de dispositivos de forma a permitir a fácil instalação do equipamento;
- ii. O fabricante deve disponibilizar no seu respectivo web site, download gratuito de todos os Drivers dos dispositivos, BIOS e Firmwares para o equipamento ofertado;
- iii. Apresentar declaração do fabricante informando que todos os componentes do objeto são novos (sem uso, reforma ou recondicionamento) e que não estão fora de linha de fabricação;
- iv. O modelo do equipamento ofertado deverá suportar o sistema operacional Windows Server 2019. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Microsoft no link: <http://www.windowsservercatalog.com>;
- v. O modelo do equipamento ofertado deverá suportar o sistema operacional Red Hat Enterprise Linux 9 ou posterior. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Red Hat no link: <https://hardware.redhat.com/hwcert/index.cgi>;
- vi. O modelo do equipamento ofertado deverá suportar o sistema de virtualização VMware ESXi 8.0 ou posterior. Esse item deverá ser comprovado através do Compatibility Guide da VMware no link: <http://www.vmware.com/resources/compatibility>.

6.14.16. SOFTWARE

- i. Deverá vir acompanhado de todos os drivers de todos os dispositivos opcionais e que compõe o hardware.

6.14.17. Certificados

- i. Deverá ser entregue no dia do pregão a certificação comprovando que o equipamento está em conformidade com a norma IEC 60950, Energy Star e Inmetro
- ii. O equipamento ofertado deve estar de acordo com as diretivas ROHS.

6.14.18. Gerenciamento e Inventário

- i. O equipamento deve possuir solução de gerenciamento do próprio fabricante através de recursos de hardware e software com capacidade de prover as seguintes funcionalidades:



- ii. Possuir software de gerência, com capacidade de gerenciamento remoto de um único equipamento (1:1) e vários equipamentos (1:N);
- iii. O equipamento deve possuir interface de rede dedicada para gerenciamento que suporte nativamente a atribuição de endereçamento IP dinâmico;
- iv. Permitir o monitoramento remoto, de todo o hardware das condições de funcionamento dos equipamentos e seus componentes, tais como: processadores, memória RAM, controladora RAID, discos, fontes de alimentação, NICs e ventiladores;
- v. Suportar os protocolos de criptografia SSL para acesso Web e SSH para acesso CLI;
- vi. Emitir alertas de anormalidade de hardware através do software de gerência e suportar o encaminhamento via e-mail e trap SNMP;
- vii. Suportar autenticação local e através de integração com MS Active Directory/LDAP;
- viii. Deverá suportar autenticação de 2 fatores.
- ix. Permitir o controle remoto da console do servidor do tipo virtual KVM out-of-band, ou seja, independente de sistema operacional ou software agente;
- x. Permitir a captura de vídeo ou tela de situações de falhas críticas de sistemas operacionais e inicialização do sistema (boot), possibilitando uma depuração mais aprimorada;
- xi. As funcionalidades de gerenciamento e monitoramento de hardware devem ser providas por recursos do próprio equipamento e independente de agentes ou sistema operacional;
- xii. Caso a console virtual deverá ser acessível via interface HTML5 ou caso necessite de algum tipo de plugin licenciado, por exemplo JAVA deverá ser fornecido o licenciamento por pelo menos 5 anos
- xiii. Suportar os protocolos de gerenciamento, IPMI e SNMP v1, v2c, v3, WMI, SSH, WS MAN e REDFISH;
- xiv. Permitir customizar alertas e automatizar a execução de tarefas baseadas em script;
- xv. Deverá possuir integração com VMware vCenter e Microsoft System Center.
- xvi. Interface de gerência baseado em HTML5.
- xvii. Permitir configurar os seguintes parâmetros de hardware, (WWN, BIOS, RAID, NIC, MAC, Virtual Mac address, iSCSI Name, Vlan e perfil de QOS), através de templates pré-definidos;



- xviii. Permitir a instalação, update e configuração remota de sistemas operacionais, drivers e firmwares, através de solução de deployment compatível com a solução ofertada;
- xix. Permitir a criação de perfis (baselines) de configuração para detectar desvios relacionados ao firmware dos componentes de hardware;
- xx. Possuir informações de garantia e apresentar via relatório e ou scorecard, listando o tipo de garantia e data limite, em caso de limite informar via email de forma automatizada para que seja possível ação da contratante;
- xxi. Permitir a detecção de pré-falhas dos componentes de hardware.
- xxii. Realizar a abertura automática de chamados sem intervenção humana, diretamente ao fabricante dos equipamentos em caso de falha de componentes de hardware;
- xxiii. Permitir ligar, desligar e reiniciar os servidores remotamente e independente de sistema operacional;
- xxiv. Deve possuir recurso remoto que permita o completo desligamento e reinicialização (Hard-Reset) remoto do equipamento através da interface de gerência ou através de solução alternativa (Hardware/Software);
- xxv. Permitir a emulação de mídias virtuais de inicialização (boot) através de CD/DVD remoto, compartilhamentos de rede NFS/CIFS e dispositivos de armazenamento USB remotos;
- xxvi. Permitir acesso do tipo Console Virtual, do mesmo fabricante dos servidores ofertados, que permita gerenciar, monitorar e configurar parâmetros físicos dos servidores de forma remota e centralizada;
- xxvii. O software de gerenciamento deve realizar descoberta automática dos servidores, permitindo inventariar os mesmos e seus componentes;
- xxviii. Suportar o monitoramento remoto (1:1 e 1:N) do consumo de energia elétrico e temperatura dos servidores, através de exibição gráfica, e permitir gerenciar parâmetros de consumo de CPU, memória, IO e Motherboard, com geração de alertas;
- xxix. Possuir configuração de alerta de consumo de energia para grupos de dispositivos;
- xxx. Possuir controles de energia baseados no tempo (diariamente, semanalmente e ou faixa de datas);
- xxxi. Permitir configurar dispositivos individuais, grupos físicos e grupos lógicos;



- xxxii. Permitir comparação de dispositivos relacionado ao seu consumo, criando reports com equipamentos ociosos em consumo e os de maior consumo;
- xxxiii. A interface de gerência do servidor deve permitir a criação de grupos de modo a permitir o gerenciamento de outros servidores a partir de um único IP sem a necessidade de softwares adicionais.
- xxxiv. Deve possuir funcionalidade que permita que os discos locais do servidor sejam apagados de forma definitiva através de tecnologia de regravação de dados ou similar. Esta funcionalidade deve possibilitar que sejam definitivamente apagados quaisquer disco dentro do servidor, suportando, no mínimo discos físicos (HDDs), discos criptografados (SEDs) e dispositivos de memória não volátil (SSDs e NVMe).
- xxxv. Deve possibilitar o download automático de atualizações de firmwares, BIOS e drivers diretamente do site do fabricante ou repositório local.
- xxxvi. As atualizações de firmwares, BIOS e drivers devem ser possuir tecnologia de verificação de integridade do fabricante, de modo a garantir a autenticidade dela.
- xxxvii. Deverá ser fornecido software que realize a descoberta de ativos no datacenter como servidores, switch, storage do mesmo fabricante e de outros fabricantes usando o protocolo SNMP, assim como o gerenciamento básico (ativo ou desligado) de dispositivos e inventário de hardware para até 1500 dispositivos.
- xxxviii. A solução de gerenciamento de servidores deve permitir o gerenciamento através de aplicação de gerenciamento via dispositivos moveis (smartphones e tablets) compatível com sistemas IOS e ou Android. O APP deverá estar disponível para download na Google Play Store e Apple APP Store.
- xxxix. Deverá possuir relatórios de status de garantia via interface de gerência.

6.15 APPLIANCE DE MONITORAMENTO

- 6.15.1. Solução de monitoramento utilizando dispositivo de hardware dedicado a função de monitoramento de infraestrutura, não sendo aceito soluções montadas sob a plataforma PC/x86 nem dispositivos montados usando soluções Open Source.
- 6.15.2. Deve permitir instalação em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.



- 6.15.3. Deve possuir, no máximo, 1 RU (Rack Unit) de altura.
- 6.15.4. Deve possuir 2 fontes de alimentação AC bivolt interna, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).
- 6.15.5. Processador interno com quatro cores, Intel x86 ou equivalente, para permitir execução de aplicações internas tipo Dockers ou Kubernetes
- 6.15.6. Deve possuir 16 portas seriais com suporte a expansão até 96 portas seriais com conectores seriais RJ-45 em uma unidade “RU”, sem a utilização de switches externos
- 6.15.7. Deve possuir para up-link ou aceso, no mínimo, 2 (duas) portas Gigabit Ethernet (10/100/1000BT) com interface RJ-45 e 2 (duas) portas SFP+ 10GB.
- 6.15.8. Deve permitir alimentação de energia em corrente contínua (DC).
- 6.15.9. Deve possuir portas tipo USB para conectar modem celular, serial, ethernet, Wi-Fi, armazenamento e modem analógico e ou ethernet via conversor USB-Ethernet.
- 6.15.10. Deve permitir o acesso opcional via rede móvel LTE 5G/4G, devendo ser fornecido com chip de dados ativo;
- 6.15.11. Permitir acesso pelos protocolos HTTPS, SSHv2; opcional HTTP, Telnet and SSHv1.
- 6.15.12. Permitir a configuração via interface Gráfica ou linha de comando e Linux.
- 6.15.13. Deve suportar no mínimo 32GB de armazenamento interno
- 6.15.14. Deve suportar as funções de servidor DHCP e executar roteamento e funções de firewall.
- 6.15.15. Deve suportar plataforma para Automação para end device via Python Scripts, Puppet, Chef, Docker e Ansible
- 6.15.16. Deve suportar automação via diferentes meios, incluindo, shell Script, Cloud, RESTFUL, ANSIBLE, Chef, Docker, KVM Hypervisor, Puppet, Python, RedHat Ansible, Ruby, Node.js JavaScript
- 6.15.17. Permitir Agrupamento de equipamentos via software em grupos associando múltiplas unidades e permitir o gerenciamento através do login em uma das unidades apenas.
- 6.15.18. Envio de alertas e eventos deve permitir envio de mensagens via log de sistema, E-mail e na própria console.
- 6.15.19. Deve suportar a customização do nível de acesso de usuários.
- 6.15.20. Deve suportar a descoberta automática de novos dispositivos.
- 6.15.21. Deve permitir configurar suporte a NTP, zonas de horários mundiais ou sincronização através de torre de celular.



- 6.15.22. Deve permitir a restrição do acesso à interface de linha de comando (CLI) através de senha e dupla autenticação usando protocolos RSA e DUO.
- 6.15.23. Deve permitir NAT e possuir funções de Firewall integrado com o sistema operacional.
- 6.15.24. Deve suportar tunelamento através de SSL VPN, IPSec e Wireguard VPN.
- 6.15.25. Deve suportar mecanismos de AAA (Authentication, Authorization e Accounting), com suporte aos protocolos RADIUS e TACACS+, LDAP e Kerberos
- 6.15.26. Deve suportar o protocolo IPv6;
- 6.15.27. Deve permitir a configuração de endereços IPv6 para gerenciamento;
- 6.15.28. Deve permitir consultas de DNS com resolução de nomes em endereços IPv6;
- 6.15.29. Deve suportar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH e HTTP sobre IPv6;
- 6.15.30. Deve suportar mecanismo de Dual Stack (IPv4 e IPv6), para permitir implantação de IPv4 para IPv6\ Suportar IPv4 / IPv6.

6.16 COLLOCATION

- 6.16.1. A CONTRATADA deverá prover no mínimo 2 Datacenters em território nacional;
- 6.16.2. O serviço deverá prover infraestrutura de sustentação operacional e atender características técnicas construtivas para a prestação do Serviço Collocation compostas pelas especificações e normas técnicas indicadas nos itens a seguir:
 - i. Possuir certificação padrão TIER III;
 - ii. A CONTRATADA deverá possibilitar ao CONTRATANTE o acesso irrestrito ao DATA CENTER a qualquer hora do dia ou da noite do Collocation;
 - iii. O Data Center deverá estar localizado em um raio de até 300 Km (trezentos quilômetros) da sede do CRQ-IV/SP, visando otimizar o tempo de acesso aos equipamentos, quando necessário, através do suporte presencial dos seus profissionais.
 - iv. Disponibilização de racks padrão 19 polegadas com (no mínimo 600 mm) de largura, no mínimo profundidade 1000 mm, no mínimo altura 42U (2100 mm) com porta frontal com chave, incluindo todos os acessórios de fixação dos equipamentos e organização de cabeamento.



- v. Disponibilização do serviço de Rack Unit em rack compartilhado com outros clientes;
- 6.16.3. A CONTRATANTE terá o acesso monitorado e acompanhado por um técnico da CONTRATADA OU DO DATA CENTER 100%;
- 6.16.4. Piso elevado com resistência mínima para acomodar a carga dos racks mesmo que estes estejam completamente ocupados por equipamentos;
- 6.16.5. Deverá ser disponibilizado fora da área dos equipamentos Sala de Uso Técnico para acesso seguro através de notebooks portados por especialistas do CONTRATANTE para conexão com o DATA CENTER hospedado, mediante autorização prévia;
- 6.16.6. Deverá ser disponibilizado no endereço de Serviço Collocation Sala de Desembalagem de equipamentos recebidos por envio do CONTRATANTE, com responsabilidade de descarte sustentável de materiais e invólucros não utilizados;
- 6.16.7. Deverá ter sistema de detecção de incêndio de alta sensibilidade e dispositivo de pré-alarme e alarme, no ambiente do DATA CENTER, incluindo a área embaixo do piso elevado, os quadros elétricos de distribuição e ar-condicionado, com sistema integrado de alarme monitorado por computador e acompanhado em regime 24 x 7 x 365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano);
- 6.16.8. Em eventual necessidade de solicitação ou realocação para uso de rack ou cage privativo, ou seja, rack totalmente dedicado e exclusivo aos equipamentos da CONTRATANTE, deverá ser contratado uma quantidade mínima conforme regras abaixo:
- i. Rack Privativo, mínimo de 40 rack units;
 - ii. Cage Privativo, mínimo 320 rack units.

6.17 PRIVACIDADE E DISPONIBILIDADE

- 6.17.1. O prazo para disponibilização dos serviços para a CONTRATANTE deverá ser de até 30 dias após a assinatura do contrato
- 6.17.2. A qualquer momento durante a execução deste contrato, todos os dados e informações da CONTRATADA poderão ser solicitados pela CONTRATADA para a CONTRATANTE e deverão ser disponibilizados em até 48 horas após esta solicitação. Os dados deverão ser disponibilizados em formato de padrão de mercado, sem qualquer tipo de criptografia ou



formato proprietário da CONTRATADA, de forma que permita serem lidos, acessados e modificados pela CONTRATANTE.

- 6.17.3. Após o término do contrato, todos os dados e informações da CONTRATADA devem ser disponibilizados em formato de padrão de mercado, sem qualquer tipo de criptografia ou formato proprietário da CONTRATADA, de forma que permita serem lidos, acessados ou modificados pela CONTRATANTE. Os dados deverão ser disponibilizados em um local a ser disponibilizado pela CONTRATANTE em um prazo de até 48 horas após a solicitação formal.

6.18 TREINAMENTO

- 6.18.1. A CONTRATADA deverá fornecer treinamento via web ou presencial para a equipe técnica da CONTRATANTE, habilitando-a a realizar Diagnóstico e Manutenção dos equipamentos fornecidos;
- 6.18.2. O treinamento capacitará equipe técnica a realizar diagnósticos, abrir chamados diretamente em ferramenta do fabricante, solicitar peça e se necessário realizar a troca do componente;
- 6.18.3. Esse escopo será tratado como um recurso opcional e/ou complementar, ao nível de suporte dos equipamentos visando incrementar o atendimento referente ao suporte técnico do fabricante. Tal certificação/habilitação não torna a CONTRATANTE responsável técnica pelos atendimentos dos referidos equipamentos. Esta responsabilidade permanece do fabricante;
- 6.18.4. O treinamento deve propiciar aos técnicos da CONTRATANTE a autorização de abertura dos equipamentos para diagnóstico e acréscimo de periféricos / dispositivos homologados sem perda da garantia, bem como solicitação de peças para reposição e abertura de chamados com o fabricante.

6.19 REGULAMENTO DA PROVA DE CONCEITO (PoC)

- 6.19.1. Por se tratar de uma contratação de serviço em um ambiente de terceiros, não há como fazer a habilitação do licitante vencedor apenas através da análise de documentos ou da



conferência física em equipamentos, pois eles estarão instalados no datacenter da empresa vencedora.

- 6.19.2. A prova de conceito tem a finalidade de validar e conferir se todas as exigências técnicas serão devidamente cumpridas antes da efetivação do contrato com a empresa vencedora;
- 6.19.3. Após a fase de classificação das propostas e habilitação, será realizada a Prova de Conceito (PoC) com a equipe técnica do licitante provisoriamente vencedor, visando à comprovação da capacidade técnica e metodológica para a execução dos serviços;
- 6.19.4. O diferimento da realização da Prova de Conceito justifica-se sob a ótica dos princípios da eficiência, economicidade e racionalidade administrativa, considerando que a execução da PoC demanda custos financeiros, logísticos e de alocação de pessoal. Tal medida visa evitar o dispêndio de recursos com propostas que eventualmente não atendam aos requisitos mínimos de habilitação, promovendo, assim, maior otimização do processo licitatório;
- 6.19.5. Todas as atividades relativas à Prova de Conceito serão realizadas dentro do horário comercial das 09h às 17h;
- 6.19.6. O CRQ-IV/SP disponibilizará um ambiente virtual para realização da Prova de Conceito, que permita a interação em tempo real para apresentação da solução.
- 6.19.7. A Prova de Conceito será composta pela homologação das funcionalidades, características e demais evidências acerca da Solução Computacional de Nuvem ofertada, segundo o Roteiro apresentado neste documento.
- 6.19.8. O prazo máximo para a conclusão de todas as etapas previstas no Roteiro da Prova de Conceito será de 10 (dez) dias úteis após iniciada a atividade.
- 6.19.9. A LICITANTE deverá executar todas as atividades previstas no Roteiro da Prova de Conceito, devendo apresentar os produtos gerados para a verificação da conformidade quanto aos requisitos descritos neste Estudo Técnico Preliminar.
- 6.19.10. A partir da convocação do pregoeiro, a LICITANTE terá até 05 (cinco) dias úteis para iniciar a Prova de Conceito. Nesse prazo, dúvidas a respeito ao Roteiro poderão ser sanadas.
- 6.19.11. A Prova de Conceito (PoC) poderá ser acompanhada por representantes dos demais licitantes.
- 6.19.12. Os licitantes interessados em participar da PoC deverão manifestar seu interesse formalmente ao Pregoeiro. A exigência de manifestação formal de interesse por parte dos



licitantes para participação é necessária para garantir a adequada organização e preparação do ambiente na qual será realizada a apresentação técnica e disponibilização de recursos e alocação de pessoal de apoio, otimizando o processo e evitando atrasos no cronograma da licitação.

- 6.19.13. A Prova de conceito será avaliada quanto ao cumprimento dos requisitos do Roteiro e aderência ao Termo de Referência, por uma equipe de técnicos a ser nomeada pelo CONTRATANTE.
- 6.19.14. Apenas os membros da Equipe Técnica de avaliação poderão fazer perguntas ou solicitar esclarecimentos ao representante do licitante enquanto o mesmo estiver demonstrando o requisito;
- 6.19.15. Não serão permitidos quaisquer questionamentos durante a demonstração, para que se possa garantir o cumprimento dos prazos estipulados da apresentação.
- 6.19.16. Após o término da Prova de Conceito, o CRQ-IV/SP por meio de sua equipe técnica designada emitirá um parecer quanto a aprovação ou reprovação, sendo que, nesse último caso, deverá especificar as funcionalidades não foram atendidas, ouvindo também eventuais apontamentos por parte das demais licitantes, que poderão se manifestar em Ata a ser gerada ao final da apresentação, na qual serão registradas as ocorrências relevantes e assinada pela Equipe o Técnica e pelos licitantes presentes.
- 6.19.17. Encerrado a Prova de Conceito, a Equipe Técnica designada informará ao Pregoeiro o resultado, que dará continuidade ao certame.
- 6.19.18. Caso a empresa vencedora não consiga comprovar o atendimento à todas as exigências da prova de conceito, sua proposta será considerada como desclassificada, sendo chamado o próximo licitante com a menor oferta durante a fase de lances para executar a mesma prova de conceito.
- 6.19.19. Só será considerada como habilitada a empresa que comprovar o atendimento à todas as exigências da prova de conceito.

6.20 ROTEIRO DA PROVA DE CONCEITO

- 6.20.1 O roteiro para testes desta prova de conceito deverá ocorrer conforme as tarefas a seguir, sendo executadas pela licitante vencedora e acompanhadas pelo CRQ-IV/SP.



- i. Deverá demonstrar a capacidade de conexão lógica entre a infraestrutura de TI do CRQ-IV/SP e o datacenter da licitante vencedora;
- ii. Deverá executar uma operação de backup de uma máquina virtual (VM) do ambiente computacional do CRQ-IV/SP para o datacenter da CONTRATADA utilizando a plataforma de backup e replicação Veeam Backup & Replication versão Enterprise Plus Edition Perpetual;
- iii. Deverá executar uma operação de restore da máquina virtual (VM) para o local de origem.
- iv. Deverá realizar uma operação de Restore granular da máquina virtual (VM) demonstrando que é possível restaurar arquivos, pastas ou itens específicos;
- v. Deverá realizar uma operação de replicação de uma máquina virtual, através de ferramenta de backup e replicação Veeam Backup Enterprise Edition e VPN (Rede Privada Virtual), da infraestrutura computacional do CRQ-IV/SP para a infraestrutura de datacenter da CONTRATADA para que possamos validar o serviço de Disaster Recovery (DR).
- vi. Deverá realizar uma operação de backup de, no mínimo, 5 (cinco) caixas de correio eletrônico do Microsoft Office 365 para a infraestrutura de datacenter da CONTRATADA;
- vii. Nesta Prova de Conceito, a Contratada deverá apresentar a interface Web de gestão dos servidores replicados pelo serviço de DR.

6.21 INDICADORES DE NÍVEIS MÍNIMOS DE SERVIÇO (SLA) E MEDIÇÃO:

Indicador	Meta	Medição	Penalidade por descumprimento
Disponibilidade dos serviços (uptime)	≥ 98,0	Mensal	Desconto de 5 % por ponto percentual abaixo da meta
Tempo de Resposta de Suporte	1h (crítico) 4h (alto) 12h (médio) 24h (baixo)	Por solicitação	Multa de 2% por atraso
Tempo de Resolução de Incidentes	≤ 4h (crítico) ≤ 12h (alto) ≤ 24h (médio)	Por incidente	Multa de 10% por atraso



7 – Análise comparativa de soluções:

Inciso II, do artigo II da Instrução Normativa SGD-ME nº 94/2022

7.1 – ANÁLISE COMPARATIVA DE SOLUÇÕES AMBIENTE ON PREMISES E COMPUTAÇÃO EM NUVEM

A comparação entre computação em nuvem e on premises envolve uma série de considerações, incluindo desempenho, custo, segurança, escalabilidade e complexidade de gerenciamento. Abaixo vamos destacar os principais pontos de comparação entre os dois:

7.1.1. Desempenho:

- i. On Premises: Geralmente oferecem desempenho previsível e consistente, pois os recursos são dedicados exclusivamente à carga de trabalho.
- ii. Computação em Nuvem: O desempenho pode variar dependendo da demanda do provedor de nuvem e do compartilhamento de recursos. No entanto, muitos provedores de nuvem oferecem opções de instâncias de alta performance para atender às necessidades exigentes de algumas cargas de trabalho.

7.1.2. Custos:

- i. On Premises: Exigem investimento inicial significativo em hardware, além de custos contínuos de manutenção, energia elétrica, refrigeração e espaço físico.
- ii. Computação em Nuvem: Normalmente opera sob um modelo de pagamento conforme o uso, o que pode ser mais econômico para empresas que têm cargas de trabalho variáveis ou precisam escalar rapidamente.

7.1.3. Segurança:

- i. On Premises: Oferecem controle direto sobre a segurança, mas exigem a implementação e manutenção de medidas de segurança física e lógica.
- ii. Computação em Nuvem: Muitos provedores de nuvem possuem certificações de segurança e oferecem uma variedade de recursos de segurança, incluindo firewalls, criptografia e gerenciamento de identidade. No entanto, a segurança dos dados na nuvem depende da confiança no provedor de serviços e da implementação correta de medidas de segurança por parte do usuário.

7.1.4. Escalabilidade:



- i. On Premises: A escalabilidade pode ser limitada pela capacidade de hardware disponível e pelo tempo necessário para adquirir e configurar novos servidores.
- ii. Computação em Nuvem: Oferece escalabilidade quase instantânea, permitindo aumentar ou diminuir os recursos conforme necessário, pagando apenas pelo que é usado.

7.1.5. Complexidade de Gerenciamento:

- i. On Premises: Exigem gerenciamento direto de hardware, atualizações de software e configuração de rede, o que pode ser complexo e exigir habilidades especializadas.
- ii. Computação em Nuvem: Geralmente oferece ferramentas de gerenciamento centralizado que simplificam muitas tarefas administrativas, mas ainda requerem conhecimento técnico para configurar e otimizar adequadamente.

7.1.6. Confiabilidade e Disponibilidade:

- i. On Premises: A disponibilidade depende da redundância e da qualidade do hardware e infraestrutura de rede.
- ii. Computação em Nuvem: Muitos provedores de nuvem oferecem SLAs (Acordos de Nível de Serviço) que garantem alta disponibilidade e podem oferecer recursos de redundância geográfica para aumentar a confiabilidade.

7.1.7. Flexibilidade:

- i. On Premises: Oferecem total controle sobre o hardware e o software, permitindo customização completa de acordo com as necessidades da empresa.
- ii. Computação em Nuvem: Oferece uma ampla gama de serviços e recursos, permitindo que as empresas escolham entre várias opções de configuração e migrem entre elas conforme necessário.
- iii. Em resumo, a escolha entre nuvem e servidores físicos depende das necessidades específicas de cada empresa, incluindo requisitos de desempenho, custo, segurança e flexibilidade. Muitas empresas optam por uma abordagem híbrida, combinando servidores físicos para cargas de trabalho específicas com a utilização de serviços de nuvem para flexibilidade e escalabilidade.

7.1.8. On Premises - Vantagens

- i. Controle total: Os servidores físicos oferecem controle total sobre hardware e software, permitindo ajustes precisos de configuração.
- ii. Desempenho previsível: Com recursos dedicados, os servidores físicos geralmente oferecem desempenho mais previsível e consistente.



- iii. Segurança: Alguns argumentam que os servidores físicos oferecem maior controle e segurança sobre os dados, pois estão diretamente sob o controle da organização.
- iv. Custos previsíveis a longo prazo: Enquanto os custos iniciais de investimento podem ser mais altos, a manutenção de servidores físicos pode ser mais previsível ao longo do tempo, sem taxas mensais.

7.1.9. On Premises - Desvantagens

- i. Custos iniciais elevados: Aquisição de hardware, instalação e configuração podem resultar em custos iniciais significativos.
- ii. Manutenção e atualização: As empresas são responsáveis pela manutenção, atualização e substituição de hardware e software, o que pode exigir tempo e recursos significativos.
- iii. Escalabilidade limitada: A capacidade de escalabilidade é limitada pela capacidade física do hardware existente, o que pode resultar em problemas de capacidade em momentos de crescimento rápido ou inesperado.
- iv. Riscos de tempo de inatividade: Falhas de hardware podem resultar em tempo de inatividade significativo, especialmente se não houver medidas de redundância adequadas.

7.1.10. Computação em Nuvem – Vantagens

- i. Escalabilidade: Os serviços em nuvem oferecem escalabilidade instantânea, permitindo que as empresas aumentem ou diminuam os recursos conforme necessário.
- ii. Redução de custos iniciais: As soluções em nuvem geralmente envolvem custos operacionais mensais ou anuais, em vez de grandes investimentos iniciais em hardware.
- iii. Manutenção simplificada: A manutenção de hardware e software é de responsabilidade do provedor de nuvem, liberando a equipe de TI interna para se concentrar em outras áreas.
- iv. Disponibilidade e redundância: Muitos provedores de nuvem oferecem redundância geográfica e recursos de alta disponibilidade, reduzindo significativamente o risco de tempo de inatividade.

7.1.11. Computação em Nuvem – Desvantagens

- i. Dependência de conexão com a internet: Acesso aos recursos em nuvem depende de uma conexão estável com a internet. Interrupções na conectividade podem resultar em indisponibilidade temporária.
- ii. Segurança percebida: Alguns podem ter preocupações sobre a segurança dos dados na nuvem, embora os provedores de nuvem geralmente implementem medidas rigorosas de segurança.
- iii. Custos variáveis: Enquanto os custos iniciais podem ser menores, os custos operacionais contínuos podem variar dependendo do uso e da demanda.
- iv. Personalização limitada: Em alguns casos, a personalização de configurações de hardware ou software pode ser limitada em comparação com servidores físicos.

7.1.12. Quadro comparativo: Computação em Nuvem x On-Premises

Critério	Nuvem	On-Premises
Custo Inicial	Baixo (pagamento sob demanda)	Alto (compra de hardware e licenciamentos)



Critério	Nuvem	On-Premises
Manutenção	Feita pelo provedor	Necessita gestão da equipe interna
Escalabilidade	Ilimitada e automática	Limitada a capacidade adquirida
Segurança	Atualizações automáticas e compliance	Dependência da equipe interna
Acessibilidade	Qualquer lugar e hora	Normalmente limitado à rede local
Recuperação de Dados	Backup e replicação em ambiente seguro	Backup e replicação em ambiente local.

7.1.13. Conclusão

O crescimento dos serviços de Cloud Computing tem sido rápido e constante nos últimos anos. E tudo indica que continuará assim. Esse crescimento é impulsionado por fatores tecnológicos, econômicos e estratégicos. Com base nessas considerações, concluímos que a contratação dos serviços de Cloud Computing é uma alternativa totalmente eficiente para garantir disponibilidade dos serviços de TIC deste Conselho.

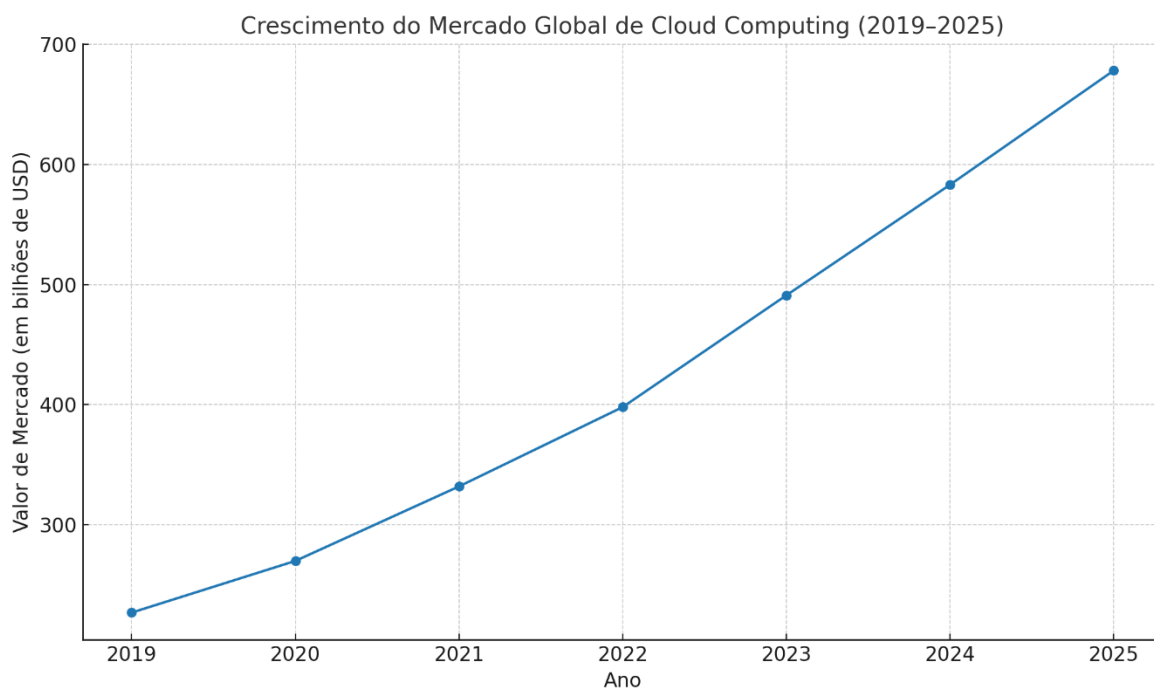




Gráfico baseado em IA

7.2 – Necessidades similares em outros órgãos ou entidade da Administração Pública e as soluções adotadas.

Inciso II, letra “a” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

As entidades da administração pública estão adotando **serviços de computação em nuvem** de forma crescente para melhorar a eficiência, reduzir custos, garantir escalabilidade e aumentar a segurança de seus serviços.

7.3 – As alternativas de mercado:

Inciso II, letra “b” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Há diversos provedores de serviços de computação em nuvem em território nacional.

7.4 – A existência de softwares disponíveis conforme descrito na Portaria STI/MP Nº 46, de 28/09/2016

Inciso II, letra “c” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

7.5 – As políticas, os modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico – ePing, Modelo de Acessibilidade em Governo Eletrônico – eMag, Padrões Web em Governo Eletrônico – ePwg, padrões de Design System de governo, Infraestrutura de Chaves Públicas Brasileira – ICP Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil, quando aplicáveis

Inciso II, letra “d” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

7.6 – As necessidades de adequação do ambiente do órgão para viabilizar a execução contratual

Inciso II, letra “e” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

O CRQ-IV/SP precisará adequar a estrutura de segurança da informação para que o serviço, objeto desta licitação, possa ser executado. Regras de firewall serão implementadas.

7.7 – Os diferentes modelos de prestação de serviços;

Inciso II, letra “f” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

7.8 – Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

Inciso II, letra “g” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022



Não se aplica.

7.9 – A possibilidade de aquisição na forma de bens ou contratação como serviço;
Inciso II, letra “h” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

O objeto desta contratação será como serviço.

7.10 – A ampliação ou substituição da solução implantada;
Inciso II, letra “i” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

7.11 – As diferentes métricas de prestação de serviço e de pagamento;
Inciso II, letra “j” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

O pagamento dos serviços contratados serão realizados mensalmente **conforme demanda** e quantidades mínimas e máximas estimadas.

8 – Análise comparativa de custos das soluções técnica e funcionalmente viáveis:
Inciso III, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

8.1 – Comparação de custos totais de propriedade:
Inciso III, letra “a” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

8.2 – Memória de cálculo que referencie os preços e os custos utilizados na análise
Inciso III, letra “b” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

9 – Estimativa do custo total da contratação:
Inciso IV, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

- 9.1. Em conformidade com a Instrução Normativa SEGES/ME Nº 65 de 07 de julho de 2021-SLTI/MPOG, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral.
- 9.2. Método estatístico aplicado: Média aritmética dos preços unitários obtidos na pesquisa de mercado.
- 9.3. Após ampla pesquisa não foram encontrados preços em sistemas oficiais do governo, como Painel de Preço, nem contratações similares feitas pela Administração Pública, e tampouco em mídia especializada, devido as particularidades do objeto desta forma não foi possível atender os incisos I, II e III do artigo 5º.



9.5. A pesquisa de preço foi obtida diretamente com fornecedores, conforme disposto no artigo 5º inciso IV:

IV – pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital;

9.6. Após análise e recebimento de propostas comparativas e viáveis para a aquisição da solução idealizada, abaixo listamos o valor médio.

9.7. Tabela de serviços solicitados neste estudo técnico preliminar:

Código do Serviço	Descrição
01-SVRCAP	Servidores Virtuais e Recursos Computacionais (Ambiente de Produção)
02-SVRCDR	Servidores e Recursos Computacionais (Ambiente de Desastre - DR)
03-ARMAZE	Armazenamento
04-CONNECT	Conectividade
05-SOPRDA	Solução de Proteção dos Dados
06-SOBACK	Solução de Backups
07-DEREEN	Detecção e Resposta de EndPoint
08-RECDES	Recuperação de Desastres
09-SOFTLIC	Softwares e Licenciamentos
10-OPSUGE	Operação, Suporte e Gerenciamento
11-SERVRA	Servidor Rack
12-APPMON	Appliance de Monitoramento
13-COLLOC	Rack Unit

9.8. Preços apurados através de pesquisa de mercado.

9.8.1. Fornecedor A



SERVIÇO PÚBLICO FEDERAL
CONSELHO REGIONAL DE QUÍMICA IV REGIÃO – SÃO PAULO
RUA OSCAR FREIRE, 2039 – PINHEIROS – 05409-011 – SÃO PAULO/SP
WWW.CRQSP.ORG.BR

ITEM	DESCRIÇÃO	UNIDADE	VALOR UNITÁRIO	QTD. MINIMA	QTD. MÁXIMA	MINIMO MENSAL	TOTAL MENSAL
1	SERVIDORES VIRTUAIS E RECURSOS COMPUTACIONAIS (AMBIENTE DE PRODUÇÃO)	Processador	vCPU R\$ 106,99	0	20	R\$ -	R\$ 2.139,80
		Memória	GB R\$ 13,05	0	150	R\$ -	R\$ 1.957,50
2	SERVIDORES VIRTUAIS E RECURSOS COMPUTACIONAIS (AMBIENTE DE DESASTRES)	Instâncias Protegidas	Instância R\$ 30,90	6	13	R\$ 185,40	R\$ 401,70
		Processador	vCPU R\$ 32,00	22	40	R\$ 704,00	R\$ 1.280,00
		Memória	GB R\$ 4,01	132	180	R\$ 529,32	R\$ 721,80
		SSD	GB R\$ 0,20	6500	13000	R\$ 1.300,00	R\$ 2.600,00
		HDD	GB R\$ 0,10	0	3000	R\$ -	R\$ 300,00
		SSD	GB R\$ 0,18	0	15000	R\$ -	R\$ 2.700,00
3	ARMAZENAMENTO	HDD	GB R\$ 0,06	0	25000	R\$ -	R\$ 1.500,00
		Object Storage	GB R\$ 0,17	17000	25000	R\$ 2.890,00	R\$ 4.250,00
		L2L	Gbps R\$ 3.499,00	0	1	R\$ -	R\$ 3.499,00
4	CONECTIVIDADE	Internet	Mbps R\$ 2,50	0	500	R\$ -	R\$ 1.250,00
		IPv4	Un. R\$ 11,19	0	10	R\$ -	R\$ 111,90
		IPv6	Un. R\$ 2,59	0	10	R\$ -	R\$ 25,90
		Firewall	Instância R\$ 899,00	1	2	R\$ 899,00	R\$ 1.798,00
5	SOLUÇÃO DE PROTEÇÃO DOS DADOS	Licença de Backup	Instância R\$ 79,90	1	15	R\$ 79,90	R\$ 1.198,50
		Backup Office 365	Caixa R\$ 9,30	170	200	R\$ 1.581,00	R\$ 1.860,00
		Respositório de Backup	GB R\$ 0,10	18000	25000	R\$ 1.800,00	R\$ 2.500,00
6	DETECÇÃO E REPOSTA DE ENDPOINT	Endpoint	Instância R\$ 22,30	0	30	R\$ -	R\$ 669,00
		Recuperação de Desastre Padrão	Instância R\$ 47,80	0	10	R\$ -	R\$ 478,00
7	RECUPERAÇÃO DE DESASTRES	Recuperação de Desastre Avançado	Instância R\$ 99,10	0	10	R\$ -	R\$ 991,00
		SSD	GB R\$ 0,20	0	20000	R\$ -	R\$ 4.000,00
		HDD	GB R\$ 0,06	0	20000	R\$ -	R\$ 1.200,00
		Windows Server	vCPU R\$ 24,80	0	30	R\$ -	R\$ 744,00
8	SOFTWARES E LICENCIAMENTO	Windows Remote Desktop	Dispositivo R\$ 55,60	0	150	R\$ -	R\$ 8.340,00
		Red Hat Enterprise	Instância R\$ 659,00	0	3	R\$ -	R\$ 1.977,00
		Microsoft SQL Standard	vCPU R\$ 752,30	0	2	R\$ -	R\$ 1.504,60
		Microsoft SQL Enterprise	vCPU R\$ 2.869,00	0	1	R\$ -	R\$ 2.869,00
		Suporte Ambiente Microsoft	Hora R\$ 250,00	0	50	R\$ -	R\$ 12.500,00
9	OPERAÇÃO, SUPORTE E GERENCIAMENTO	Suporte Ambiente Red Hat	Hora R\$ 220,00	0	10	R\$ -	R\$ 2.200,00
		Suporte a Banco de Dados	Hora R\$ 350,00	0	50	R\$ -	R\$ 17.500,00
		Suporte a Firewall	Hora R\$ 200,00	0	50	R\$ -	R\$ 10.000,00
		Servidor 2U	Servidor R\$ 3.999,00	0	2	R\$ -	R\$ 7.998,00
10	SERVIDOR RACK	Appliance	R\$ 400,00	0	1	R\$ -	R\$ 400,00
11	APPLIANCE DE MONITORAMENTO	Rack Unit	R\$ 350,00	0	6	R\$ -	R\$ 2.100,00
12	COLLOCATION						
TOTAL MENSAL						R\$ 9.968,62	R\$ 105.564,70

9.8.2. Fornecedor B

ITEM	DESCRIÇÃO	UNIDADE	VALOR UNITÁRIO	QTD. MINIMA	QTD. MÁXIMA	MINIMO MENSAL	TOTAL MENSAL
1	SERVIDORES VIRTUAIS E RECURSOS COMPUTACIONAIS (AMBIENTE DE PRODUÇÃO)	Processador	vCPU R\$ 114,10	0	20	R\$ -	R\$ 2.282,00
		Memória	GB R\$ 14,07	0	150	R\$ -	R\$ 2.110,50
2	SERVIDORES VIRTUAIS E RECURSOS COMPUTACIONAIS (AMBIENTE DE DESASTRES)	Instâncias Protegidas	Instância R\$ 29,29	6	13	R\$ 175,74	R\$ 380,77
		Processador	vCPU R\$ 33,76	22	40	R\$ 742,72	R\$ 1.350,40
		Memória	GB R\$ 4,23	132	180	R\$ 558,36	R\$ 761,40
		SSD	GB R\$ 0,23	6500	13000	R\$ 1.495,00	R\$ 2.990,00
		HDD	GB R\$ 0,05	0	3000	R\$ -	R\$ 150,00
		SSD	GB R\$ 0,19	0	15000	R\$ -	R\$ 2.850,00
3	ARMAZENAMENTO	HDD	GB R\$ 0,06	0	25000	R\$ -	R\$ 1.500,00
		Object Storage	GB R\$ 0,18	17000	25000	R\$ 3.060,00	R\$ 4.500,00
		L2L	Gbps R\$ 3.691,71	0	1	R\$ -	R\$ 3.691,71
4	CONECTIVIDADE	Internet	Mbps R\$ 2,64	0	500	R\$ -	R\$ 1.320,00
		IPv4	Un. R\$ 11,81	0	10	R\$ -	R\$ 118,10
		IPv6	Un. R\$ 2,73	0	10	R\$ -	R\$ 27,30
		Firewall	Instância R\$ 960,00	1	2	R\$ 960,00	R\$ 1.920,00
5	SOLUÇÃO DE PROTEÇÃO DOS DADOS	Licença de Backup	Instância R\$ 84,30	1	15	R\$ 84,30	R\$ 1.264,50
		Backup Office 365	Caixa R\$ 9,81	170	200	R\$ 1.667,70	R\$ 1.962,00
		Respositório de Backup	GB R\$ 0,07	18000	25000	R\$ 1.260,00	R\$ 1.750,00
6	DETECÇÃO E REPOSTA DE ENDPOINT	Endpoint	Instância R\$ 23,53	0	30	R\$ -	R\$ 705,90
		Recuperação de Desastre Padrão	Instância R\$ 50,43	0	10	R\$ -	R\$ 504,30
7	RECUPERAÇÃO DE DESASTRES	Recuperação de Desastre Avançado	Instância R\$ 104,56	0	10	R\$ -	R\$ 1.045,60
		SSD	GB R\$ 0,21	0	20000	R\$ -	R\$ 4.200,00
		HDD	GB R\$ 0,06	0	20000	R\$ -	R\$ 1.200,00
		Windows Server	vCPU R\$ 26,17	0	30	R\$ -	R\$ 785,10
8	SOFTWARES E LICENCIAMENTO	Windows Remote Desktop	Dispositivo R\$ 58,66	0	150	R\$ -	R\$ 8.799,00
		Red Hat Enterprise	Instância R\$ 695,29	0	3	R\$ -	R\$ 2.085,87
		Microsoft SQL Standard	vCPU R\$ 793,73	0	2	R\$ -	R\$ 1.587,46
		Microsoft SQL Enterprise	vCPU R\$ 3.027,01	0	1	R\$ -	R\$ 3.027,01
		Suporte Ambiente Microsoft	Hora R\$ 263,77	0	50	R\$ -	R\$ 13.188,50
9	OPERAÇÃO, SUPORTE E GERENCIAMENTO	Suporte Ambiente Red Hat	Hora R\$ 232,12	0	10	R\$ -	R\$ 2.321,20
		Suporte a Banco de Dados	Hora R\$ 369,28	0	50	R\$ -	R\$ 18.464,00
		Suporte a Firewall	Hora R\$ 211,01	0	50	R\$ -	R\$ 10.550,50
		Servidor 2U	Servidor R\$ 4.219,24	0	2	R\$ -	R\$ 8.438,48
10	SERVIDOR RACK	Appliance	R\$ 422,03	0	1	R\$ -	R\$ 422,03
11	APPLIANCE DE MONITORAMENTO	Rack Unit	R\$ 369,28	0	6	R\$ -	R\$ 2.215,68
12	COLLOCATION						
TOTAL MENSAL						R\$ 10.003,82	R\$ 110.469,31



9.8.3. Fornecedor C

ITEM	DESCRIÇÃO		UNIDADE	VALOR UNITÁRIO	QTD. MINIMA	QTD. MÁXIMA	MINIMO MENSAL	TOTAL MENSAL
2	SERVIDORES VIRTUAIS E RECURSOS COMPUTACIONAIS (AMBIENTE DE PRODUÇÃO)	Processador	vCPU	R\$ 107,60	0	20	R\$ -	R\$ 2.152,00
		Memória	GB	R\$ 13,50	0	150	R\$ -	R\$ 2.025,00
2.9	SERVIDORES VIRTUAIS E RECURSOS COMPUTACIONAIS (AMBIENTE DE DESASTRES)	Instâncias Protegidas	Instância	R\$ 31,50	6	13	R\$ 189,00	R\$ 409,50
		Processador	vCPU	R\$ 32,27	22	40	R\$ 709,94	R\$ 1.290,80
		Memória	GB	R\$ 4,05	132	180	R\$ 534,60	R\$ 729,00
		SSD	GB	R\$ 0,20	6500	13000	R\$ 1.300,00	R\$ 2.600,00
		HDD	GB	R\$ 0,06	0	3000	R\$ -	R\$ 180,00
7	ARMAZENAMENTO	SSD	GB	R\$ 0,20	0	15000	R\$ -	R\$ 3.000,00
		HDD	GB	R\$ 0,06	0	25000	R\$ -	R\$ 1.500,00
		Object Storage	GB	R\$ 0,20	17000	25000	R\$ 3.400,00	R\$ 5.000,00
8	CONECTIVIDADE	L2L	Gbps	R\$ 3.510,00	0	1	R\$ -	R\$ 3.510,00
		Internet	Mbps	R\$ 2,70	0	500	R\$ -	R\$ 1.350,00
		IPv4	Un.	R\$ 11,25	0	10	R\$ -	R\$ 112,50
		IPv6	Un.	R\$ 2,70	0	10	R\$ -	R\$ 27,00
9	SOLUÇÃO DE PROTEÇÃO DOS DADOS	Firewall	Instância	R\$ 914,00	1	2	R\$ 914,00	R\$ 1.828,00
10	SOLUÇÃO DE BACKUP	Licença de Backup	Instância	R\$ 81,80	1	15	R\$ 81,80	R\$ 1.227,00
		Backup Office 365	Caixa	R\$ 9,45	170	200	R\$ 1.606,50	R\$ 1.890,00
		Respositório de Backup	GB	R\$ 0,07	18000	25000	R\$ 1.260,00	R\$ 1.750,00
11	DETECÇÃO E REPOSTA DE ENDPOINT	Endpoint	Instância	R\$ 23,30	0	30	R\$ -	R\$ 699,00
12	RECUPERAÇÃO DE DESASTRES	Recuperação de Desastre Padrão	Instância	R\$ 49,80	0	10	R\$ -	R\$ 498,00
		Recuperação de Desastre Avançado	Instância	R\$ 99,60	0	10	R\$ -	R\$ 996,00
		SSD	GB	R\$ 0,20	0	20000	R\$ -	R\$ 4.000,00
		HDD	GB	R\$ 0,06	0	20000	R\$ -	R\$ 1.200,00
13	SOFTWARES E LICENCIAMENTO	Windows Server	vCPU	R\$ 25,50	0	30	R\$ -	R\$ 765,00
		Windows Remote Desktop	Dispositivo	R\$ 57,60	0	150	R\$ -	R\$ 8.640,00
		Red Hat Enterprise	Instância	R\$ 665,00	0	3	R\$ -	R\$ 1.995,00
		Microsot SQL Standard	vCPU	R\$ 756,50	0	2	R\$ -	R\$ 1.513,00
		Microsoft SQL Enterprise	vCPU	R\$ 2.850,00	0	1	R\$ -	R\$ 2.850,00
14	OPERAÇÃO, SUPORTE E GERENCIAMENTO	Suporte Ambiente Microsoft	Hora	R\$ 225,00	0	50	R\$ -	R\$ 11.250,00
		Suporte Ambiente Red Hat	Hora	R\$ 270,00	0	10	R\$ -	R\$ 2.700,00
		Suporte a Banco de Dados	Hora	R\$ 360,00	0	50	R\$ -	R\$ 18.000,00
		Suporte a Firewall	Hora	R\$ 270,00	0	50	R\$ -	R\$ 13.500,00
15	SERVIDOR RACK	Servidor 2U	Servidor	R\$ 4.095,00	0	2	R\$ -	R\$ 8.190,00
16	APPLIANCE DE MONITORAMENTO	Appliance	Appliance	R\$ 337,50	0	6	R\$ -	R\$ 2.025,00
17	COLLOCATION	Rack Unit	Rack Unit	R\$ 270,00	0	6	R\$ -	R\$ 1.620,00
TOTAL MENSAL							R\$ 9.995,84	R\$ 111.021,80

9.8.4. Quadro resumo dos valores apresentados em proposta comercial para o fornecimento dos serviços baseados em computação em nuvem:

Fornecedor C		Fornecedor A		Fornecedor B	
Valor para Qtde. Mínima/mês	Valor para a Qtde. Máxima/mês	Valor para Qtde. Mínima/mês	Valor para a Qtde. Máxima/mês	Valor para Qtde. Mínima/mês	Valor para a Qtde. Máxima/mês
R\$ 9.995,84	R\$ 111.021,80	R\$ 9.968,62	R\$ 105.564,70	R\$ 10.003,82	R\$ 110.469,31

9.9. Tabela de valores estimados Unitários, Mínimo e Máximos dos serviços:

Subi tem	Descrição		Unidade	Quantidade Mínima	Quantidade Máxima	Valor Unitário Fornecedor B	Valor Unitário Fornecedor A	Valor Unitário Fornecedor C	Valor Médio Unitário	Valor Est Mínimo Mensal	Valor Est Máximo Mensal
1	SERVIDORES VIRTUAIS E RECURSOS COMPUTACIONAIS (AMBIENTE DE PRODUÇÃO)	Processador	vCPU	1	20	R\$ 114,10	R\$ 106,99	R\$ 107,60	R\$ 109,56	R\$ 109,56	R\$ 2.191,20
		Memória	GB	12	150	R\$ 14,07	R\$ 13,05	R\$ 13,50	R\$ 13,54	R\$ 162,48	R\$ 2.031,00
2	SERVIDORES VIRTUAIS E RECURSOS COMPUTACIONAIS (AMBIENTE DE DESASTRES)	Instâncias Protegidas	Instância	6	10	R\$ 29,29	R\$ 30,90	R\$ 31,50	R\$ 30,56	R\$ 183,36	R\$ 305,60
		Processador	vCPU	22	40	R\$ 33,76	R\$ 32,00	R\$ 32,27	R\$ 32,68	R\$ 718,96	R\$ 1.307,20
		Memória	GB	132	160	R\$ 4,23	R\$ 4,01	R\$ 4,05	R\$ 4,10	R\$ 541,20	R\$ 656,00
		SSD	GB	4.500	11.000	R\$ 0,23	R\$ 0,20	R\$ 0,20	R\$ 0,21	R\$ 945,00	R\$ 2.310,00
		HDD	GB	2.000	3.000	R\$ 0,05	R\$ 0,05	R\$ 0,06	R\$ 0,05	R\$ 100,00	R\$ 150,00
3	ARMAZENAMENTO	SSD	GB	1	11.000	R\$ 0,19	R\$ 0,18	R\$ 0,20	R\$ 0,19	R\$ 0,19	R\$ 2.090,00
		HDD	GB	1	25.000	R\$ 0,06	R\$ 0,06	R\$ 0,06	R\$ 0,06	R\$ 0,06	R\$ 1.500,00
		Object Storage	GB	17.000	25.000	R\$ 0,18	R\$ 0,17	R\$ 0,20	R\$ 0,18	R\$ 3.060,00	R\$ 4.500,00
4	CONECTIVIDADE	L2L	Gbps	-	1	R\$ 3.691,71	R\$ 3.499,00	R\$ 3.510,00	R\$ 3.566,90	R\$ -	R\$ 3.566,90
		Internet	Mbps	-	300	R\$ 2,64	R\$ 2,50	R\$ 2,70	R\$ 2,61	R\$ -	R\$ 783,00
		IPv4	Un.	-	10	R\$ 11,81	R\$ 11,19	R\$ 11,25	R\$ 11,42	R\$ -	R\$ 114,20
		IPv6	Un.	-	10	R\$ 2,73	R\$ 2,59	R\$ 2,70	R\$ 2,67	R\$ -	R\$ 26,70
5	SOLUÇÃO DE PROTEÇÃO DOS DADOS	Firewall	Instância	1	2	R\$ 960,00	R\$ 899,00	R\$ 914,00	R\$ 924,33	R\$ 924,33	R\$ 1.848,66



SERVIÇO PÚBLICO FEDERAL
CONSELHO REGIONAL DE QUÍMICA IV REGIÃO – SÃO PAULO
RUA OSCAR FREIRE, 2039 – PINHEIROS – 05409-011 – SÃO PAULO/SP
WWW.CRQSP.ORG.BR

6	SOLUÇÃO DE BACKUP	Licença de Backup	Instância	1	5	R\$ 84,30	R\$ 79,90	R\$ 81,80	R\$ 82,00	R\$ 82,00	R\$ 410,00
		Backup Office 365	Caixa	170	200	R\$ 9,81	R\$ 9,30	R\$ 9,45	R\$ 9,52	R\$ 1.618,40	R\$ 1.904,00
7	DETECÇÃO E REPOSTA DE ENDPOINT	Repositório de Backup	GB	18.000	25.000	R\$ 0,07	R\$ 0,06	R\$ 0,07	R\$ 0,07	R\$ 1.260,00	R\$ 1.750,00
		Endpoint	Instância	-	30	R\$ 23,53	R\$ 22,30	R\$ 23,30	R\$ 23,04	R\$ -	R\$ 691,20
8	RECUPERAÇÃO DE DESASTRES	Recuperação de Desastre Padrão	Instância	-	10	R\$ 50,43	R\$ 47,80	R\$ 49,80	R\$ 49,34	R\$ -	R\$ 493,40
		Recuperação de Desastre Avançado	Instância	-	10	R\$ 104,56	R\$ 99,10	R\$ 99,60	R\$ 101,09	R\$ -	R\$ 1.010,90
		SSD	GB	-	20.000	R\$ 0,21	R\$ 0,20	R\$ 0,20	R\$ 0,20	R\$ -	R\$ 4.000,00
		HDD	GB	-	20.000	R\$ 0,06	R\$ 0,06	R\$ 0,06	R\$ 0,06	R\$ -	R\$ 1.200,00
9	SOFTWARES E LICENCIAMENTO	Windows Server	vCPU	-	30	R\$ 26,17	R\$ 24,80	R\$ 25,50	R\$ 25,49	R\$ -	R\$ 764,70
		Windows Remote Desktop	Dispositivo	-	150	R\$ 58,66	R\$ 55,60	R\$ 57,60	R\$ 57,29	R\$ -	R\$ 8.593,50
		Red Hat Enterprise	Instância	-	2	R\$ 695,29	R\$ 659,00	R\$ 665,00	R\$ 673,10	R\$ -	R\$ 1.346,20
		Microsoft SQL Standard	vCPU	-	2	R\$ 793,73	R\$ 752,30	R\$ 756,50	R\$ 767,51	R\$ -	R\$ 1.535,02
10	OPERAÇÃO, SUPORTE E GERENCIAMENTO	Microsoft SQL Enterprise	vCPU	-	1	R\$ 3.027,01	R\$ 2.869,00	R\$ 2.850,00	R\$ 2.915,34	R\$ -	R\$ 2.915,34
		Suporte Ambiente Microsoft	Hora	-	50	R\$ 263,77	R\$ 250,00	R\$ 225,00	R\$ 246,26	R\$ -	R\$ 12.313,00
		Suporte Ambiente Red Hat	Hora	-	10	R\$ 232,12	R\$ 220,00	R\$ 270,00	R\$ 240,71	R\$ -	R\$ 2.407,10
		Suporte a Banco de Dados	Hora	-	50	R\$ 369,28	R\$ 350,00	R\$ 360,00	R\$ 359,76	R\$ -	R\$ 17.988,00
11	SERVIDOR RACK	Suporte a Firewall	Hora	-	50	R\$ 211,01	R\$ 200,00	R\$ 270,00	R\$ 227,00	R\$ -	R\$ 11.350,00
		Servidor 2U	Servidor	-	2	R\$ 4.219,24	R\$ 3.999,00	R\$ 4.095,00	R\$ 4.104,41	R\$ -	R\$ 8.208,82
12	APPLIANCE DE MONITORAMENTO	Appliance (TIPO I)	Appliance	-	1	R\$ 422,03	R\$ 400,00	R\$ 337,50	R\$ 386,51	R\$ -	R\$ 386,51
13	COLLOCATION	Rack Unit	Rack Unit	-	6	R\$ 369,28	R\$ 350,00	R\$ 270,00	R\$ 329,76	R\$ -	R\$ 1.978,56
Total Estimado										R\$ 9.705,54	R\$ 104.626,71

9.9.1. Valores Totais Estimados para contratação:

- Valor Mensal Mínimo: R\$ 9.705,54 (nove mil setecentos e cinco reais e cinquenta e quatro centavos.)
- Valor Mensal Máximo: R\$ 104.626,71 (cento e quatro mil seiscentos e vinte e seis reais e setenta e um centavos)
- Valor Total (36 meses) Mínimo: R\$ 349.399,44 (trezentos e quarenta e nove mil trezentos e noventa e nove reais e quarenta e quatro centavos)
- Valor Total (36 meses) Máximo: R\$ 3.766.561,56 (três milhões setecentos e sessenta e seis mil quinhentos e sessenta e um reais e cinquenta e seis centavos)

9.9.2. Inicialmente será contratado apenas os serviços referentes aos subitens:

- (2) SERVIDORES VIRTUAIS E RECURSOS COMPUTACIONAIS (AMBIENTE DE DESASTRES);
- (3) ARMAZENAMENTO;
- (5) SOLUÇÃO DE PROTEÇÃO DOS DADOS; e
- (6) SOLUÇÃO DE BACKUP.

10 Identificação dos benefícios a serem alcançados

Inciso V, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

10.1 Benefícios a serem alcançados com a solução escolhida:

- 10.1.1 Redução de custos operacionais;



10.1.2 Escalabilidade;

10.1.3 Garantir alta disponibilidade e confiabilidade dos serviços de TIC.

Economicidade	Que a contratação decorrente desse estudo acarrete para CRQ-IV/SP os menores custos possíveis na obtenção da proposta mais vantajosa.
Efetividade	Que os serviços objeto desta contratação auxilie o órgão atingir as metas estabelecidas, apresentando um resultado satisfatório.
Eficiência	Garantir disponibilidade dos serviços de TIC e funcionamento dos dispositivos elétricos que compõem a rede de computadores do órgão.
Eficácia	Cumprir o Planejamento de Segurança da Informação elaborado pela Gerência de Tecnologia e Informática do órgão.
Objetivo Estratégico	OE11 – Adotar as melhores práticas de Governança e Gestão e OE12 – Promover a inovação de processos e serviços, por meio de melhoria contínua e das ferramentas de Inteligência Artificial.

11 – Declaração de Viabilidade da Contratação:

Inciso V, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

- 11.1. A contratação dos serviços baseados em Computação em Nuvem é justificada através da viabilidade técnica e econômica, considerando os benefícios operacionais, financeiros e estratégicos que tal solução oferece à organização.
- 11.2. A computação em nuvem permite o fornecimento de infraestrutura, plataformas e softwares como serviço, de forma remota e escalável. A tecnologia atende aos requisitos técnicos da organização, oferecendo: alta disponibilidade e desempenho, segurança de dados com mecanismos avançados de criptografia e backup, escalabilidade automática de recursos conforme demanda, acesso remoto com autenticação segura, Conformidade com regulamentações como LGPD, ISO 27001, entre outras.
- 11.3. Economicamente os serviços de Computação em nuvem traz ao órgão: redução significativa de custos com hardware, licenças, energia elétrica e pessoal técnico especializado; modelo de pagamento por uso, com melhor previsibilidade orçamentária e sem necessidade de investimento inicial elevado, menor custo de atualização tecnológica e manutenção.
- 11.4. Com relação ao alinhamento estratégico, a contratação está em conformidade com os objetivos definidos no plano estratégico do sistema CFQ/CRQs.



- 11.5. Diante dos benefícios técnicos, operacionais e financeiros apresentados, declara-se viável e recomendável a contratação de um serviço de computação em nuvem para atender às necessidades atuais e futuras do CRQ-IV/SP. A medida contribuirá diretamente para o aumento da eficiência e da segurança das informações sob responsabilidade do órgão.

12 Classificação quanto ao acesso a informação

- 12.1. Nos termos da Lei nº 12.527, de 18 de novembro de 2011, o presente Estudo não se classifica como sigiloso.

São Paulo, 06 agosto de 2025.

Equipe Técnica de Planejamento da Contratação

Alexandre de Paula
Integrante Requisitante
Gerente / Tecnologia da Informação

Claudio A. Gimenez
Integrante Técnico

Waldemir Menezes da Silva
Integrante Administrativo