1. Do objetivo

Este anexo detalha os serviços e os recursos de computação em nuvem que deverão ser disponibilizados pela empresa pré-qualificada habilitada, doravante chamada de PROPONENTE, neste anexo.

2. Requisitos da infraestrutura na nuvem

2.1. Além dos requisitos definidos no item 9.2 do anexo I, a PROPONENTE deverá garantir que todas as informações da PRODEMGE estarão armazenadas nos data centers dos CSP que estará representando, incluindo as cópias de segurança (ex: backup, snapshots) destas informações.

2.1.1. O armazenamento considera a guarda de informações de forma persistente e não volátil.

2.1.2. As informações poderão ser tratadas por serviços processados em data centers localizados fora do território brasileiro pela Cloud Service Provider (Provedora de Serviços em Nuvem – **CSP**), quando **explicitamente esta condição for definida no Termo de Referência específico** para a Chamada de Oportunidade e somente para os serviços da categoria **Serviços cognitivos e especializados** (item 4.4 deste anexo).

2.2. Conectividade e Integração

2.2.1. A comunicação do CSP com a infraestrutura tecnológica da PRODEMGE poderá ser feita por meio de enlace de rede dedicado (link dedicado), por meio de VPN (Internet) ou por ambas alternativas, a critério da PRODEMGE.

2.2.1.1. O Termo de Referência específico da Chamada de Oportunidade irá detalhar o cenário de conexão.

2.2.1.2. No caso da opção da PRODEMGE por link dedicado, este será fornecido pela PRODEMGE, cabendo à PROPONENTE a liberação de portas de conexão dedicada no CSP, conforme definido no item 3.7 deste anexo.

2.2.2. A taxa de transferência mínima na conexão VPN deve ser de 100 Mbps, podendo, entretanto, ser inferior quando limitada pela capacidade da conexão (link dedicado) da PRODEMGE.

2.2.3. Tráfego de rede:

2.2.3.1. Não será permitida a cobrança de tráfego ENTRANTE para data centers do CSP localizados no território brasileiro.

2.2.3.2. Não será permitida a cobrança de tráfego LATERAL DENTRO DE DATA CENTER do CSP, independentemente da localização do data center.

2.2.3.3. É permitida a cobrança de tráfego SAINTE de data center do CSP e de tráfego LATERAL ENTRE DATA CENTERS do CSP, independentemente da localização dos data centers, desde que a proposta técnica para atendimento à Chamada de Oportunidade explicite de forma clara e inequívoca as regras de cobrança e inclua todos os custos na proposta comercial.

2.2.4. A solução fornecida pela PROPONENTE deverá permitir a interoperabilidade com as plataformas de monitoramento e Service Desk da PRODEMGE.

2.2.4.1. Para monitoramento a PRODEMGE utiliza os produtos CA-Infrastructure Management 2.0 (que contempla, entre outros aplicativos o Spectrum e o Performance Management) e o Zabbix.

2.2.4.2. Para gestão de incidentes a PRODEMGE utiliza o CA-Service Desk Manager Package..

2.2.4.3. Os produtos CA são do fabricante Broadcom

2.2.5. A interoperabilidade com os sistemas legados deverá ocorrer conforme regras de conectividade e segurança definidos pela PRODEMGE no Termo de Referência específico da Chamada de Oportunidade.

2.3. Os data centers propostos pelas PROPONENTES deverão dispor de recursos que garantam a segurança da informação dos dados da PRODEMGE, incluindo os seguintes itens:

2.3.1. Solução de controle de tráfego de borda do tipo firewall (norte-sul, leste/oeste, e de aplicações),

2.3.2. Solução de prevenção e detecção de intrusão.

2.3.3. Solução anti-DDoS.

2.4. Deverão ser oferecidos pela PROPONENTE mecanismos que permitam à PRODEMGE, verificar, online, a situação de determinado serviço contratado, de forma a oferecer rastreabilidade das alterações, monitoramento de uso dos recursos e provisionamento do mesmo.

2.4.1. A PROPONENTE deverá manter registros de todos acessos e operações realizadas nos ambientes da nuvem (logs de acesso) contratada.

2.4.2. Os logs deverão ser mantidos durante 6 (seis) meses, cabendo à PROPONENTE disponibilizar as informações em formato .csv, mensalmente, em um site, de forma a permitir o download destes dados pela PRODEMGE.

2.4.2.1. Estes dados sempre deverão estar disponíveis para a PRODEMGE quando solicitados e no encerramento do contrato.

2.4.2.2. A PROPONENTE deverá documentar e repassar para a PRODEMGE o layout destas informações.

2.5. A PROPONENTE deverá permitir o uso de licenciamento próprio de software (Bring Your Own License – BYOL) da PRODEMGE.

2.5.1. Somente será aplicado a política de BYOL sobre aqueles produtos cujo licenciamento do fabricante do software esteja de acordo com a instalação na infraestrutura de um CSP.

2.5.2. Nestas situações a PRODEMGE será a responsável por fornecer comprovação das licenças de software, caso seja necessário.

2.6. Os serviços, quando contratados, deverão ser disponibilizados em regime 24 x 7, incluindo finais de semana e feriados, com disponibilidade, qualidade e segurança, conforme indicadores que serão detalhados no Termo de Referência específico de cada Chamada de Oportunidade.

2.6.1. O nível de serviço, de 24x7, poderá ser reduzido em função de necessidades especificas de um projeto e, neste caso, o Termo de Referência específico da Chamada de Oportunidade irá especificar de forma clara e inequívoca este novo cenário.

2.7. A PROPONENTE compromete-se á a não replicar ou realizar cópias de segurança (backups) dos dados da PRODEMGE, exceto com o aceite formal da PRODEMGE, para fora do território brasileiro, devendo informar imediatamente e formalmente à PRODEMGE qualquer tentativa neste sentido.

3. Serviços obrigatórios:

A solução ofertada pela PROPONENTE deverá suportar, obrigatoriamente, no mínimo, os serviços abaixo, mas não se limitando a estes:

3.1. Acesso à infraestrutura – Com autenticação de, pelo menos, dois fatores (multi-factor authentication – MFA).

3.2. Provisionar Máquinas Virtuais, com, no mínimo, os seguintes recursos:

3.2.1. Capacidade de agrupar instâncias logicamente no mesmo data center.

3.2.2. Capacidade de dividir e hospedar instâncias de servidores virtuais específicas em diferentes hosts físicos.

3.2.3. Capacidade de aumentar e reduzir automaticamente (elasticidade) o número de instâncias de servidores virtuais durante picos de uso para manter o desempenho.

3.2.4. Capacidade de importar imagens existentes e salvá-las como imagens novas e privadas, que podem ser usadas para provisionar instâncias de novos servidores virtuais.

3.2.5. Capacidade de clonar, na infraestrutura de data center CSP representada pela PROPONENTE, uma instância de servidor virtual em execução ou uma cópia de uma instância e exportar para o formato de Máquina Virtual.

3.2.6. Possuir mecanismos que possam minimizar os impactos em instâncias de servidores virtuais, quando o CSP estiver executando algum tipo de manutenção de hardware ou serviço no nível do host.

3.2.7. Possuir mecanismos de snapshot sob demanda.

3.2.8. Permitir a disponibilização da Máquina Virtual por uso em período fixo (reserva) ou por demanda.

3.3. Provisionar Infraestrutura como código (IaC – Infrastructure as Code)

3.4. Provisionar armazenamento em nível de bloco com no mínimo, os seguintes recursos:

3.4.1. Capacidade de aumentar o tamanho de um volume de armazenamento em bloco existente, sem precisar provisionar um novo volume e copiar/mover os dados.

3.4.2. Capacidade de snapshots.

3.4.3. Suporte a exclusão completa de dados, de modo que os dados não sejam mais legíveis ou acessíveis por usuários não autorizados e/ou terceiros.

3.4.4. Suporte a criptografia.

3.4.5. Possuir opções de armazenamento do tipo SSD e HDD.

3.5. Provisionar armazenamento de objetos com, no mínimo, os seguintes recursos:

3.5.1. Suporte a criptografia do volume.

3.5.2. Permitir definir em qual região os dados serão armazenados de forma que os mesmos nunca saiam desta região, a menos que o usuário os transfira explicitamente para outra região.

3.5.3. Suporte ao versionamento de objetos.

3.5.4. Permitir o envio de parte de um conjunto de objetos, sendo que cada parte é uma porção contínua de dados de um objeto e essas partes de um objeto podem ser enviadas independentemente e em qualquer ordem.

3.5.5. Possuir capacidade de gerar logs de auditoria.

3.5.6. Deverá possuir interface web para inclusão, exclusão e consultas de informações.

3.5.7. Possuir capacidade de recuperar um subconjunto de dados, usando API, webservice ou outro mecanismo de extração de dados.

3.6. Provisionar serviço para armazenamento de arquivos com, no mínimo, os seguintes recursos:

3.6.1. Suporte a tolerância a falhas.

3.6.2. Suporte a criptografia.

3.7. Provisionar portas para conexão dedicada

3.7.1. Provisionar portas de 1 Gbps e 10 Gbps, no data center da CSP, para conexão dedicada com o data center da PRODEMGE, possibilitando a interconexão segura e rápida entre os dois pontos, sem tráfego pela internet;

3.7.2. A disponibilização dos links de conexão entre os data centers, conforme definido no item 2.2, deste anexo, é de responsabilidade da PRODEMGE.

3.8. Provisionar serviços de redes virtuais com, no mínimo, os seguintes recursos:

3.8.1. Capacidade de criar uma rede virtual isolada e lógica que representa a própria rede de um usuário na nuvem.

3.8.2. Suporte à conexão de duas redes virtuais na mesma região para rotear o tráfego entre eles usando endereços IP (Internet Protocol) privados.

3.8.3. Capacidade de criar redes e sub-redes virtuais (privadas) totalmente isoladas, nas quais as instâncias podem ser provisionadas sem nenhum endereço de IP público ou roteamento da Internet.

3.8.4. Suporte aos protocolos de controle de transmissão (TCP), protocolo de datagrama de usuário (UDP) e protocolo de mensagem de controle da Internet (ICMP).

3.8.5. Suporte a endereços de protocolo da Internet (IP) associados a uma conta de usuário (tenant) e não a uma instância específica. O endereço IP deve permanecer associado à conta até ser explicitamente liberado.

3.8.6. Suporte aos protocolos da Internet versão 4 (IPV4) e versão 6 (IPV6) no nível do gateway e da instância de Máquina Virtual.

3.8.7. Suporte a capacidade de atribuir várias placas de interface de rede (NICs) a uma determinada instância de Máquina Virtual.

3.8.8. Permitir adicionar ou remover regras aplicáveis ao tráfego de entrada nas instâncias dos servidores virtuais.

3.8.9. Permitir adicionar ou remover regras aplicáveis ao tráfego de saída de instâncias de servidores virtuais.

3.8.10. Possuir suporte à conectividade de rede virtual privada (VPN) entre o CSP e o data center da PRODEMGE

3.8.11. Possuir suporte a múltiplas conexões de rede virtual privada (VPN).

3.8.12. Permitir que os usuários acessem serviços em nuvem por meio de um túnel de rede virtual privada (VPN), com segurança de protocolo de Internet (IPsec).

3.8.13. Suporte a BGP (Border Gateway Protocol) para melhorar o failover nos túneis da rede virtual privada (VPN), com segurança do protocolo Internet (IPsec).

3.8.14. Disponibilizar balanceamento de carga, dentro de um mesmo data center da CSP, com os seguintes requisitos:

3.8.14.1. Serviço de balanceamento de carga front-end.

3.8.14.2. Serviço de balanceamento de carga de back-end, que permite rotear o tráfego para instâncias hospedadas em sub-redes privadas.

3.8.14.3. Serviço de balanceador de carga, camada 7 (HTTP), capaz de balancear o tráfego de rede de múltiplas instâncias de servidores virtuais.

3.8.14.4. Serviço de balanceador de carga, camada 4 (TCP) capaz de balancear o tráfego de rede de múltiplas instâncias de servidores virtuais.

3.8.14.5. Serviço de balanceamento de carga com suporte a afinidade de sessão.

3.9. Provisionar containers

3.9.1. Permitir orquestração automatizada de containers, compatível com kubernetes e containers Docker.

3.9.2. Permitir controlar e automatizar as implantações, atualizações e rollback de aplicações.

3.9.3. Permitir escalar e balancear rapidamente as aplicações em containers e os recursos relacionados.

3.9.4. Permitir gerenciar serviços de forma declarativa e programática, garantindo que as aplicações sejam executadas sempre da mesma maneira como foram implantadas.

3.9.5. Deve verificar a integridade e autorrecuperação das aplicações com posicionamento, reinício, replicação e escalonamento automáticos.

3.9.6. Permitir implantação em qualquer lugar, incluindo de maneira híbrida.

3.9.7. Permitir o gerenciamento de identidade e acesso.

3.9.8. Possuir segurança de rede e carga de trabalho.

3.10. Provisionar serviços de backup (cópia de segurança) e restore (restauração da cópia de segurança), contemplando:

3.10.1. Backup físico dos servidores virtuais

3.10.2. Backup físico de Banco de Dados

3.10.3. Backup de filesystem NFS e CIFS

3.10.4. Permitir snapshot

3.10.5. Permitir o serviço de armazenamento das cópias de backup durante a duração do contrato.

3.10.5.1. As cópias devem ser persistidas com redundância, de forma a prevenir a perda de dados em caso de falhas.

3.10.6. Registrar logs de execuções de backup

3.10.7. Permitir backup e restore granular, com transferência de dados ilimitada, para os dois processos.

3.10.8. Emissão de relatórios gerenciais detalhando por instância, no mínimo, mas sem se limitar a estes indicadores: volumetria, politica, retenção e data.

3.11. Disponibilizar Segurança de Acesso

3.11.1. Serviço de cofre de senha - serviço para controle de chaves criptográficas e outros segredos usados por aplicativos e serviços

3.11.2. Serviço de Autenticação por usuário e por domínio.

3.11.2.1. Deverá permitir aos usuários a alteração e redefinição de suas senhas e a integração com outros serviços de diretórios não hospedadas na CSP.

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

3.11.2.3. Deverá fornecer uma identidade comum para acesso aos recursos na nuvem;

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

3.12. Provisionar PaaS obrigatórios:

3.12.1. Banco de dados relacionais e não relacionais,

3.12.2. Balanceamento de carga,

3.12.3. WAF,

3.12.4. Firewall,

3.12.5. DNS.

4. Serviços Opcionais:

4.1. São serviços opcionais que a PROPONENTE poderá disponibilizar para a PRODEMGE.

4.2. Os serviços poderão ser disponibilizados pela PROPONENTE, via CSP representado por ela, ou seja, os serviços fazem parte do catálogo de serviços do CSP, ou podem ser disponibilizados pela própria PROPONENTE, a partir de uma combinação de serviços deste CSP e plataformas de software específicas, fornecidas pela PROPONENTE, integrados em uma solução e hospedados no CSP representado por ela.

4.2.1. Em qualquer uma das opções, os serviços deverão ser contabilizados e bilhetados por recursos consumidos.

4.3. XaaS - Everything as a Service

4.3.1. **PaaS** – Serviços de plataformas especializadas, agregando software e hardware, conforme lista abaixo, mas não se limitando a eles:

4.3.1.1. Serverless Computing,

4.3.1.2. Concentrador de log

4.3.1.3. Containers e orquestradores
4.3.1.4. IPS
4.3.1.5. SIEM
4.3.1.6. CDN
4.3.1.7. GSLB - Balanceamento de Carga de Serviço Global

4.3.2. **SaaS** – Plataformas de software conforme lista abaixo, mas não se limitando a eles:
4.3.2.1. Correio eletrônico (e-mail),
4.3.2.2. Suíte colaborativa de automação de escritório (editor de texto, planilha),
4.3.2.3. Webconferência e/ou Videoconferência.

4.3.3. **DaaS** – Desktop (estação de trabalho) como serviço na nuvem, que pode ser acessado em qualquer dispositivo, sendo necessário apenas estar conectado à internet.

4.3.4. Outros serviços, de acordo com a relação abaixo, mas não se limitando a estes:
4.3.4.1. MaaS – Host físico (bare metal) como serviço.
4.3.4.2. Soluções de processamento de alta performance (HPC)
4.3.4.3. Registry de imagens Dockers - Disponibilizar um serviço PARTICULAR OU PRIVADO de Registry de imagens Dockers, que não seja um Registry de acesso PUBLICO, e que tenha as funcionalidades básicas de um repositório de imagens.
4.3.4.4. Vulnerabilidade de containers - disponibilizar um serviço que realize a Análise (Scan) de Vulnerabilidade mínima dos containers no ciclo de implantação da uma imagem.
4.3.4.5. Possuir capacidade de capturar logs de fluxo de tráfego de rede dentro do CSP.
4.3.4.6. Permitir que os usuários acessem serviços em nuvem por meio de um túnel de rede virtual privada (VPN) de SSL (Secure Sockets Layer) pela Internet pública

4.4. Serviços cognitivos e especializados

4.4.1. Serviços de IoT – Internet das Coisas,
4.4.2. Bots,
4.4.3. Blockchain,
4.4.4. Big Data,
4.4.5. Data Analytics,
4.4.6. Geoprocessamento,
4.4.7. Serviços baseados no uso de Inteligência Artificial, mas não se limitando a estes:

4.4.7.1. Reconhecimento Facial,
4.4.7.2. Machine Learning,
4.4.7.3. Deep Learning.

5. <u>Serviços técnicos de consultoria e suporte obrigatórios:</u>

A PROPONENTE deverá ter profissionais capacitados para realizar o atendimento das solicitações técnicas, oriundas das demandas de Chamadas de Oportunidade, devendo estar aptas a fornecer, no mínimo, mas não se restringindo a eles, os seguintes serviços, na plataforma de computação em nuvem ofertada.

5.1. Instalação e Configuração de Sistema Operacional de Máquina Virtual
5.2. Configuração de Armazenamento de blocos
5.3. Configuração de Armazenamento de objetos
5.4. Configuração de escalabilidade automática (autoscaling)
5.5. Configuração de certificado SSL
5.6. Configuração de IP público
5.7. Configuração de Rede virtual
5.8. Configuração de serviços de rede (DNS, PROXY, FTP)
5.9. Configuração de Filtro de Firewall
5.10. Configuração de VPN site-to-site e client-to-site
5.11. Configuração de Gestão de identidade, permissões e acessos
5.12. Configuração de Serviço de Autenticação
5.13. Configuração de Sistema de arquivos em rede
5.14. Configuração de Concentrador de logs
5.15. Serviço de Auditoria e Análise de Log
5.16. Configuração de Balanceamento de Carga Local e Global
5.17. Configuração de WAF
5.18. Configuração dos serviços de IPS
5.19. Configuração dos serviços de SIEM
5.20. Consultoria nas ferramentas de Compliance de segurança da plataforma ofertada
5.21. Instalação, Configuração e Tuning de Banco de Dados
5.22. Instalação e Configuração de Application Server como Tomcat, Jboss, Apache e outros
5.23. Instalação e Configuração de software diversos como PHP, Python, Java, VB.net, c#, c, c++, Ruby, JavaScript e seus frameworks tais como AngularJS, NodeJS e outros.
5.24. Instalação e Configuração de serviços de Container e seus orquestradores.
5.25. Configuração de serviços de Serverless Computing.
5.26. Configuração de serviços IaC – Infrastructure as Code

5.27. Serviços de snapshot de máquinas virtuais

5.28. Serviços de configuração de backup de maquinas virtuais e banco de dados, contemplando a criação e personalização de políticas de backup automatizadas e criptografadas

5.29. Serviço para Restauração (restore) de Máquinas Virtuais, Container e Banco de Dados

5.30. Configuração de site backup.

5.31. Configuração de VDI (Virtual Desktop Infrastructure)

5.32. Configuração de Correio e Software de Automação de escritório

5.33. Configuração dos serviços cognitivos e especializados

5.34. Configuração do Serviço de Videoconferência e Webconferência

5.35. Configuração de integração de serviços de AD

5.36. Operação assistida (remota ou on-site) no uso das funcionalidades do conjunto de API disponibilizadas

5.37. Operação assistida (remota ou on-site) no uso das funcionalidades do portal de serviços disponibilizado

5.38. Consultoria técnica para planejamento e migração

5.38.1. Este serviço contempla os serviços técnicos necessário para planejamento e migração de uma infraestrutura de TIC entre data centers, sejam eles públicos ou privados.

5.38.2. O termo de referência da chamada de oportunidade irá definir as aplicações e infraestrutura que serão migrados de data centers e os serviços que farão parte desta consultoria.

5.38.3. Os serviços técnicos abrangem as atividades de migração abaixo relacionadas, mas não se limitando a elas:

5.38.3.1. Levantamento das informações sobre o ambiente atual incluindo arquitetura da aplicação e dos bancos de dados, estruturas de dados e metadados.

5.38.3.2. Levantamento dos níveis de serviços do ambiente atual e das cargas de trabalho dos servidores,

5.38.3.3. Mapeamento das interdependências entre o ambiente a migrar e os demais sistemas de informações,

5.38.3.4. Desenho da solução no novo data center, preservando a segurança, os níveis de serviços e rotinas de backup do ambiente atual,

5.38.3.5. Definição da estratégia de migração,

5.38.3.6. Análise de risco

5.38.3.7. Plano de condição de retorno em caso de falha,

5.38.3.8. Preparação do novo ambiente,

5.38.3.9. Testes do novo ambiente, incluindo rotinas de backup e testes de segurança,

5.38.3.10. Testes e homologação do ambiente, incluindo avaliação do desempenho do novo ambiente,

5.38.3.11. Migração do ambiente,

5.38.3.12. Acompanhamento dos problemas pós-migração.

6. Transição contratual

6.1. Por ocasião do encerramento de um contrato, com a consequente finalização da prestação dos serviços pela PROPONENTE, poderá ser necessária a migração dos dados de um data center para outro.

6.2. O anexo i.c, deste termo de referência, trata deste processo de transição contratual, que fará parte do termo de referência de um contrato oriundo de uma chamada de oportunidade.