1. Objetivo

Este anexo apresenta um glossário com os termos técnicos utilizados neste edital e seus anexos.

2. Glossário

2.1. Backup

2.1.1. Cópia de dados de um dispositivo de armazenamento para outro com vistas à recuperação em caso de perda dos dados originais.

2.2. Backup Físico

2.2.1. Backup físico é a cópia física dos dados, independente da origem (VM, filesystem, objeto, etc) dos mesmos.

2.3. Backup Lógico

2.3.1. Cópia da estrutura e dos dados de um determinado banco de dados

2.4. Computação em nuvem

2.4.1. Modelo de negócio que permite acesso universal e sob demanda, por intermédio da Internet e/ou links dedicados, a um conjunto de recursos de infraestrutura de TIC configuráveis por um portal (por exemplo: redes, servidores, armazenamento, aplicações, banco de dados), que podem ser rapidamente provisionados e disponibilizados, substituindo e/ou integrando a infraestrutura de TIC tradicional (hospedada em data centers próprios).

2.5. Consumo por demanda (serviço mensurado)

2.5.1. Os provedores de serviços de nuvem automaticamente controlam e apuram o consumo de recursos de infraestrutura através de medições específicas por tipo de serviço, como armazenamento, processamento, comunicação de rede etc. O uso dos recursos é facilmente gerenciado pelo cliente, com transparência, e a bilhetagem dos serviços é balizada por esta apuração.

2.6. CSA - Cloud Security Alliance

2.6.1. É uma organização sem fins lucrativos com a missão de “promover o uso de melhores práticas para fornecer garantias de segurança na computação em nuvem, bem como educar sobre os usos da computação em nuvem para ajudar a proteger todas as outras formas de computação”.

2.7. CSP – (Cloud Service Provider) – Provedor de Serviços de Nuvem

2.7.1. Empresas especializadas em disponibilizar, em data centers (públicos ou privados), com redundância, serviços de TIC sob demanda (servidores, armazenamento, rede, de plataformas de software serviços cognitivos e outros serviços especializados (comunicação, desktop, voz, etc). São responsáveis pelas operações de data center, que dão suporte aos serviços de nuvem.

2.8. DaaS – (Desktop as a Service) - desktop como serviço

2.8.1. Desktop virtual em nuvem, que pode ser acessado em qualquer dispositivo, sendo necessário apenas estar conectado à internet.

2.9. Data Center

2.9.1. Ambiente projetado especificamente para abrigar, com segurança, recursos de infraestrutura de TIC, como servidores, unidades de armazenamento de dados (storages) e ativos de rede (switches, roteadores). Seu objetivo principal é garantir a disponibilidade dos ambientes que suportam os sistemas de informações hospedados.

2.10. Elasticidade

2.10.1. Característica de determinados recursos de infraestrutura da nuvem que podem ser provisionados e liberados de forma flexível, automaticamente, para rapidamente aumentar ou diminuir os recursos alocados de acordo com a demanda.

2.11. HPC – (High Performance Computing) – Computação com alto desempenho

2.11.1. O provedor disponibiliza soluções compostas por equipamentos desenvolvidos para tratar grandes conjuntos de dados ou processamento intensivo, com arquitetura tecnológica (memoria, cpu, barramento, gpu etc) especializada em processamento com alto desempenho.

2.12. IaaS – (Infrastructure as a Service) - Infraestrutura como serviço

2.12.1. O recurso fornecido é a capacidade de processamento, armazenamento, comunicação de rede e outros recursos de computação fundamentais nos quais o contratante pode instalar e executar softwares em geral, incluindo sistemas operacionais e aplicativos. O contratante não gerencia nem controla a infraestrutura na nuvem, mas tem controle sobre os sistemas operacionais, armazenamento, e aplicativos instalados.

2.12.2. São considerados IaaS, mas não se limitando a estes, os serviços de disponibilização de Máquinas Virtuais (servidores e desktops), Armazenamento, Backup e serviços de rede.

2.13. ISO 27001

2.13.1. Padrão internacional de gestão de segurança que especifica melhores práticas para o gerenciamento da segurança e controles abrangentes de segurança seguindo a orientação de melhores práticas do ISO 27002.

2.14. ISO 27017

2.14.1. A norma oferece instruções sobre os aspectos de segurança da informação da computação em nuvem, fazendo recomendações sobre a implementação de controles de segurança específicos da nuvem que complementam as instruções dos padrões da ISO 27002 e da ISO 27001. Esse código de práticas disponibiliza instruções de implementação de controles adicionais de segurança da informação específicos para provedores de serviços de nuvem.

2.15. ISO 27018

2.15.1. A norma é o primeiro código de práticas internacional que enfatiza a proteção de dados pessoais na nuvem. Ela baseia-se no padrão de segurança da informação ISO 27002 e disponibiliza diretrizes sobre a implementação dos controles desse padrão aplicáveis às Informações Pessoalmente Identificáveis (PII) da nuvem pública. E também fornece um conjunto de diretrizes associadas e controles adicionais destinados a abordar os requisitos de proteção de PII da nuvem pública, que não foram contemplados no conjunto de controles da ISO 27002 atual.

2.16. MaaS – (Metal as a Service) – Servidor físico (host dedicado) - como serviço

2.16.1. O provedor disponibiliza servidores físicos (Bare Metal) em seu data center.

2.16.2. O contratante não gerencia nem controla a infraestrutura na nuvem, mas tem controle sobre os sistemas operacionais, armazenamento, e aplicativos instalados.

2.17. PaaS – (Platform as a Service) - Plataformas de tecnologias como serviço

2.17.1. O provedor disponibiliza plataformas tecnológicas criadas ou adquiridas por ele. O contratante não gerencia nem controla a infraestrutura utilizada (rede, servidores, sistema operacional ou armazenamento), tendo apenas controle sobre as aplicações instaladas e algumas configurações do ambiente de hospedagem.

2.17.2. São considerados PaaS, mas não se limitando a estes, a disponibilização de serviços de Banco de dados relacionais e não relacionais, Containers e seus orquestradores, ambientes serverless, Balanceamento de carga, Balanceamento de carga de serviço Global - GSLB, WAF, IPS, SIEM, Concentrador de Log, Firewall, DNS, Gestão de identidade e acesso e Servidores de Aplicação.

2.18. Retenção

2.18.1. Período em que os backups ficam retidos e guardados em um dispositivo de armazenamento.

2.19. Restore

2.19.1. Restauração de dados e informações de um backup retido em um dispositivo de armazenamento.

2.20. SaaS – (Software as a Service) – Software como serviço

2.20.1. O provedor disponibiliza aplicações (sistemas de informações) em sua plataforma de nuvem. As aplicações podem ser acessadas por vários dispositivos através de interfaces de usuário (app, browser, etc.) ou por uma interface de programação (API). O contratante não gerencia nem controla a infraestrutura na nuvem (rede, servidores, sistemas operacionais, armazenamento), ou recursos individuais da aplicação.

2.20.2. São considerados SaaS, mas não se limitando a estes, a disponibilização de serviços correio eletrônico (e-mail), suíte colaborativa de automação de escritório (editor de texto, planilha) e videoconferência.

2.21. Serviços Cognitivos e Especializados

2.21.1. São serviços de alto valor agregado, ofertados pelos CSP, como: IoT – Internet das Coisas, Data Analytics, Reconhecimento Facial, Machine Learning, Deep Learning, Bots, Blockchain, Big Data e Geoprocessamento. Estes serviços podem ser disponibilizados como SaaS e/ou PaaS.

2.22. SOC – Service Organization Controls

2.22.1. São estruturas estabelecidas pelo Instituto Americano de Contadores Públicos Certificados (AICPA - American Institute of Certified Public Accountants) para avaliação de controles internos implementados em uma organização. Os relatórios são conhecidos como SOC 1, SOC 2 ou SOC 3,

2.22.1.1. SOC 1 examina os controles internos do prestador de serviços relevantes para emissão dos relatórios financeiros de seus clientes.

2.22.1.2. SOC 2 avalia como uma empresa se compromete e implementa controles internos em torno de um ou mais dos Critérios de Serviços de Confiança do Instituto Americano de Contadores Públicos Certificados (AICPA) em relação à disponibilidade, segurança, integridade de processamento, confidencialidade e privacidade. Os relatórios de auditoria podem ser do Tipo I ou do Tipo II.

i. Tipo I é uma avaliação pontual dos controles;

ii. Tipo II é uma avaliação da eficácia dos controles ao longo de um período de tempo;

2.22.1.3. SOC 3 usa os mesmos critérios que SOC 2, mas o relatório é preparado para fins de ampla distribuição, e é baseado no relatório Tipo II do SOC 2.

2.23. TIA-942

2.23.1. A TIA (Telecommunications Industry Association) é uma organização americana que representa a indústria global de tecnologia da informação e da comunicação, desenvolvendo normas e pesquisas para o setor.

2.23.2. As classificações de Tier da TIA-942A são normas que estabelecem as diretrizes para construção de data centers com determinados níveis de segurança, estabelecidas pela TIA (Telecommunications Industry Association).

2.23.3. A TIA não certifica e não credencia empresas para certificação. A conformidade ou não de um data center com estas classificações Tier são obtidas através de auditorias independentes. Importante ressaltar que os requisitos das classificações Tier da TIA-942 são distintos das classificações Tier da Uptime Institute.

2.24. TIER Uptime Institute

2.24.1. A classificação Tier, adotada em data centers, foi desenvolvida pelo Uptime Institute, nos EUA, e usada desde 1995 e tem reconhecimento mundial.

2.24.2. Os níveis de disponibilidade associados às classificações Tier, da Uptime, foram determinados por meio de resultados de análises de disponibilidade de data centers reais.

2.24.3. A Uptime Institute é a única entidade autorizada a certificar um data center nestas classificações e é importante ressaltar que os requisitos das classificações Tier da Uptime são distintos das classificações Tier da TIA-942.

2.25. Tráfego ENTRANTE

2.25.1. Transmissão de dados de entrada da rede, cujo destino é o datacenter do CSP e sua origem é a internet, a VPN e/ou o link dedicado entre o datacenter da PRODEMGE e do CSP.

2.26. Tráfego LATERAL DENTRO DO DATA CENTER

2.26.1. Transmissão de dados de máquinas (virtuais ou físicas), áreas de armazenamento e backup dentro de um mesmo datacenter.

2.27. Tráfego LATERAL ENTRE DATA CENTERS

2.27.1. Transmissão de dados de máquinas (virtuais ou físicas), áreas de armazenamento e backup, entre data centers distintos do mesmo CSP.

2.28. Tráfego SAINTE

2.28.1. Transmissão de dados de saída da rede, cuja origem é o datacenter do CSP e seu destino é a internet, a VPN e/ou o link dedicado entre o datacenter da PRODEMGE e do CSP.

2.29. VPN - Virtual Private Network

2.29.1. Rede privada virtual - é uma rede de comunicações privada, virtual, construída sobre qualquer outra rede de comunicações, utilizando protocolos padrões.

2.30. XaaS (Everything as a Service) – Tudo fornecido como serviço

2.30.1. Este acrônimo refere-se a um número crescente de serviços que são entregues na Internet em vez de fornecidos localmente. Os exemplos mais conhecidos de **XaaS** são Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e Desktop as a Service (DaaS), já detalhados anteriormente neste glossário.