Protocolo: 1104461
Data: 26/08/2025
Título: DECRETO RIO Nº 56646
Página(s): a

DECRETO RIO Nº 56646 DE 25 DE AGOSTO DE 2025

Estabelece a norma de Segurança para Utilização de Solução de Computação em Nuvem no âmbito da Administração Pública Municipal.

O PREFEITO DA CIDADE DO RIO DE JANEIRO, no uso das atribuições que lhe são conferidas pela legislação em vigor e,

CONSIDERANDO o disposto no inciso II, do art. 7º, do Decreto Rio nº 53.700, de 08 de dezembro de 2023, que instituiu a Política de Segurança da Informação - PSI no âmbito do Poder Executivo Municipal, o qual atribui competência à Secretaria Municipal da Casa Civil - CVL para deliberar, analisar e revisar normas complementares;

CONSIDERANDO a crescente transformação digital da Administração Pública, em que processos e serviços encontram-se cada vez mais apoiados por ativos tecnológicos;

CONSIDERANDO que o uso da computação em nuvem impactou a avaliação e mitigação de riscos de segurança da informação nas organizações, devido às mudanças significativas na utilização e governança dos recursos computacionais.

DECRETA:

Art. 1º Fica estabelecida a norma de Segurança para Utilização de Solução de Computação em Nuvem no âmbito da Administração Pública Municipal.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º Esta norma aplica-se a todas as pessoas, físicas ou jurídicas, envolvidas na definição, contratação e utilização de solução de computação em nuvem no âmbito da Administração Pública Municipal.

Art. 3º Para fins deste Decreto, considera-se:

I - autenticação: processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica; há diversas técnicas de autenticação como senhas, impressão digital, certificado digital e reconhecimento da íris;

II - autorização: concessão de um conjunto de permissões de acesso às informações ou funcionalidades de um sistema de informação a um usuário após sua autenticação;

III - ativo da informação: informação, processo ou ativo físico, tecnológico ou humano que suporta as operações de coleta, armazenamento, processamento, compartilhamento ou descarte de informações;

IV - classificação da informação: diz respeito ao grau de sensibilidade de uma informação para o negócio de uma organização diante de uma possível quebra de segurança, ou seja, do comprometimento dos princípios básicos de Segurança da Informação: confidencialidade, integridade e disponibilidade;

V - *cloud broker*: indivíduo ou organização que oferece consultoria, intermedeia e facilita a seleção de soluções de computação em nuvem em nome de uma organização. Um *cloud broker* serve como um terceiro entre um provedor de serviço de nuvem e uma organização que contrata serviços de computação em nuvem;

VI - computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais

configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem;

VII - controle de acesso: conjunto de controles que visam proteger as informações residentes em ativos tecnológicos contra acessos não autorizados;

VIII - incidente de segurança: conjunto de eventos adversos, confirmados ou sob suspeita, que tenham capacidade de comprometer a confidencialidade, integridade ou disponibilidade das informações residentes nos ativos de uma organização;

IX - risco: probabilidade de ameaças explorarem vulnerabilidades, comprometendo a confidencialidade, integridade ou disponibilidade da informação, causando impactos para uma organização;

X - tratamento: toda operação realizada com as informações durante seu ciclo de vida, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle, modificação, comunicação, transferência, difusão ou extração;

XI - usuário: qualquer pessoa autorizada a utilizar o sistema de informação;

XII - vulnerabilidade: fragilidade presente ou associada a ativos tecnológicos que, ao ser explorada por ameaças, permite a ocorrência de um incidente de segurança.

CAPÍTULO II
DOS REQUISITOS DE SEGURANÇA

Seção I
Da transferência de serviços para um provedor de serviço de nuvem

Art. 4º Antes de transferir serviços para um provedor de serviço de nuvem, os órgãos e entidades devem, no mínimo:

I - definir o modelo de serviço e de implementação de computação em nuvem que será adotado;

II - avaliar e definir quais informações serão tratadas pelo serviço, considerando:

a) a classificação da informação de acordo com a legislação pertinente;

b) a relevância da informação com respeito à sua missão;

c) a criticidade da informação considerando a possibilidade da ocorrência de um incidente de segurança que possa comprometer sua confidencialidade, integridade ou disponibilidade; e

d) os controles de segurança e privacidade previstos de forma padrão pelo serviço.

III - realizar processo de gestão de riscos de segurança e privacidade, garantindo que as informações que serão tratadas pelo serviço possuam os controles adequados ao seu nível de relevância e criticidade, e que todas as suas operações de tratamento sejam mantidas em conformidade com a regulamentação vigente;

IV - definir uma estratégia de gestão de custos para o serviço, de forma a garantir que este possa manter-se adequado no que tange à sua capacidade de atender os requisitos de qualidade previstos durante o período de contratação planejado.

V - definir as medidas de mitigação de riscos e de custos para a implementação de solução de computação em nuvem e para a possibilidade de crescimento dessa solução com a migração das informações e dos serviços.

Seção II
Do controle de acesso

Art. 5º Em relação ao controle de acesso, os órgãos e entidades devem garantir que os provedores

do serviço atendam, no mínimo, aos seguintes requisitos:

I - os mecanismos de identificação, autenticação, autorização e auditoria ofertados devem possibilitar a conformidade com toda a regulamentação municipal relativa a controle de acessos;

II - o ambiente que suportará o serviço contratado deve ser logicamente segregado dos demais ambientes suportados pelo provedor de serviço, garantindo o isolamento adequado à manutenção dos níveis de segurança acordados.

Seção III
Do gerenciamento dos serviços de nuvem

Art. 6º Em relação ao gerenciamento dos serviços de nuvem, os seguintes requisitos devem ser atendidos:

I - as equipes responsáveis pelo gerenciamento dos serviços de nuvem dos órgãos e entidades devem ser formadas por profissionais capacitados nas soluções tecnológicas de gerenciamento disponibilizadas pelo provedor do serviço;

II - um plano de resposta a incidentes deve ser elaborado pelas equipes responsáveis pelo gerenciamento dos serviços de nuvem dos órgãos e entidades em parceria com as equipes do provedor de serviço de nuvem;

III - as competências e responsabilidades relativas à segurança e gestão do serviço de nuvem devem estar formalizadas em uma matriz de responsabilidades;

IV - as equipes responsáveis pela gestão do serviço em nuvem do órgão ou entidade e do provedor devem definir e implantar um conjunto de procedimentos de suporte à comunicação de incidentes de segurança;

V - todos os ativos hospedados na nuvem devem constar dos inventários de ativos do órgão ou entidade;

VI - as seguintes especificações mínimas referentes ao processo de cópias de segurança devem ser solicitadas ao provedor do serviço em nuvem:

a) escopo e cronograma das cópias de segurança;

b) períodos de retenção;

c) procedimentos para verificação da integridade;

d) formato de dados e tipos de *backup*.

Seção IV
Do tratamento da informação

Art. 7º Em relação ao tratamento da informação em ambiente de computação em nuvem, os órgãos e entidades, além de cumprirem toda a regulamentação vigente relacionada à segurança da informação e à proteção de dados pessoais, devem observar as seguintes determinações:

I - as informações sem restrição de acesso podem ser tratadas, considerados os riscos de segurança;

II - as informações sujeitas à restrição de acesso previstas em legislação específica podem ser tratadas, considerados os riscos de segurança;

III - os dados pessoais podem ser tratados, considerados os riscos de segurança e privacidade, assim como a legislação e regulamentação de proteção de dados pessoais vigentes.

CAPÍTULO III
DOS REQUISITOS DO PROVEDOR DE SERVIÇO DE NUVEM

Art. 8º Para que esteja habilitado a prestar serviços de computação em nuvem para órgãos ou entidades da Administração Pública Municipal, o provedor de serviço de nuvem deve cumprir, no mínimo, os seguintes requisitos:

I - apresentar termo de confidencialidade que impeça o provedor de serviço de nuvem de realizar quaisquer tratamentos das informações do órgão ou entidade que não estejam previstos no contrato;

II - prover garantia da exclusividade de direitos, por parte do órgão ou da entidade, sobre todas as informações tratadas durante o período contratado, incluindo eventuais cópias disponíveis;

III - garantir conformidade da política de segurança da informação do provedor de serviço de nuvem com relação às políticas e normas de segurança da informação vigentes na Administração Pública Municipal;

IV - permitir o uso de autenticação multifator no acesso aos serviços disponibilizados pelo provedor de serviço de nuvem;

V - promover a devolução integral dos ativos da informação sob custódia do provedor de serviço de nuvem ao órgão ou entidade contratante ao término da prestação do serviço;

VI - efetuar a eliminação ao término do contrato, no fim do ciclo de vida ou se considerado inservível, de qualquer ativo da informação do órgão ou entidade sob sua custódia, observadas as exceções cabíveis amparadas em legislação que trate de obrigatoriedade de sua retenção;

VII - notificar, imediatamente, aos órgãos ou entidades, qualquer incidente de segurança que comprometa os ativos da informação sob sua custódia;

VIII - apresentar conformidade com pelo menos um dos seguintes padrões de segurança da informação: CSA STAR Nível II nas modalidades atestação ou certificação.

CAPÍTULO IV
DA UTILIZAÇÃO DE *CLOUD BROKERS*

Art. 9º Caso o órgão ou a entidade contrate, por meio do*cloud broker*, plataforma de gestão multinuvem, devem ser atendidos os seguintes requisitos:

I - o *cloud broker* deve atuar como integrador dos serviços de computação em nuvem entre o órgão ou a entidade e os provedores de serviço de nuvem;

II - a gestão do ambiente multinuvem deve ocorrer através de um único portal integrado de gerenciamento;

III - a plataforma de gestão deve prover, no âmbito das competências da contratante, soluções de suporte às seguintes funcionalidades:

a) gerenciamento de falhas;

b) gerenciamento de configuração;

c) gerenciamento de desempenho; e

d) gerenciamento de segurança.

IV - o *cloud broker* deve ser o responsável por garantir que os provedores de serviço de nuvem que ele representa:

a) cumpram os requisitos previstos nesta norma e na legislação vigente; e

b) operem de acordo com as melhores práticas de segurança e privacidade.

CAPÍTULO V
DAS COMPETÊNCIAS

Art. 10. Compete aos órgãos e entidades municipais contratantes de serviços em nuvem disponibilizar e qualificar os recursos humanos necessários ao atendimento desta norma.

Art. 11. Compete às equipes responsáveis pelo gerenciamento dos serviços de nuvem dos órgãos e entidades:

I - realizar as configurações necessárias ao funcionamento seguro da solução de computação em nuvem;

II - promover a gestão da solução de computação em nuvem, tomando as providências necessárias para prevenção e remediação de eventuais falhas;

III - gerenciar mensagens e registros de auditoria da solução de computação em nuvem;

IV - disponibilizar informações que subsidiem as decisões referentes à gestão da solução de computação em nuvem;

V - solicitar inclusão ou remoção de serviços e informações no ambiente de computação em nuvem, com anuência dos setores competentes;

VI - garantir a contínua efetividade da comunicação com o provedor de serviço de nuvem, de forma a assegurar que os controles e os níveis de serviço acordados sejam cumpridos;

VII - supervisionar a aplicação das medidas de atualização corretiva ou evolutiva realizadas pelo provedor de serviço de nuvem;

VIII - comunicar os incidentes de segurança informados pelo provedor de serviço de nuvem aos agentes competentes do órgão ou entidade;

IX - promover a aplicação desta norma, da legislação vigente e das melhores práticas sobre uso seguro de computação em nuvem.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 12. Aplicam-se à utilização de solução de computação em nuvem, no que couber, as disposições da Política de Segurança da Informação e de suas normas complementares.

Art. 13. Os agentes públicos que desempenham papéis no suporte à utilização de solução de computação em nuvem, desde que comprovada imperícia, imprudência ou negligência em sua atuação que tenha contribuído para incidente de segurança confirmado, ficam sujeitos às sanções administrativas cabíveis, conforme a legislação em vigor.

Art. 14. Este Decreto entra em vigor na data de sua publicação.

Rio de Janeiro, 25 de agosto de 2025; 461º ano da fundação da Cidade.

EDUARDO PAES