

DECRETO RIO Nº 56647 DE 25 DE AGOSTO DE 2025

Estabelece a norma sobre Cópia de Segurança (backup) e Recuperação de Dados (restore) 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 transformação digital em curso no âmbito da Administração Pública Municipal, em que processos e serviços encontram-se, cada vez mais, suportados por ativos tecnológicos; e

CONSIDERANDO que a capacidade de recuperação das informações tratadas pelos ativos tecnológicos que suportam os processos e serviços municipais é medida imprescindível à redução dos riscos de segurança da informação,

DECRETA:

Art. 1º Fica estabelecida a norma sobre Cópia de Segurança (*backup*) e Recuperação de Dados (*restore*) no âmbito da Administração Pública Municipal.

CAPÍTULO I DAS DISPOSIÇÕES PRELIMINARES

Art. 2º Esta norma aplica-se a todos os órgãos e entidades municipais.

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

I - acesso: capacidade de usar um ativo tecnológico (por exemplo: ler, criar, modificar ou excluir um arquivo; executar um programa; se conectar a um dispositivo, a uma rede, a um sistema ou a um serviço);

II - Ambiente de processamento da informação: área restrita que hospeda um conjunto de ativos tecnológicos responsáveis pelo armazenamento, compartilhamento, processamento e transmissão das informações que suportam os processos e serviços de uma organização;

III - aplicação: sistema de informação ou serviço digital desenvolvido especificamente para suporte aos processos de negócio e serviços de uma organização (por exemplo: SIAFIC, SINAIE, Matrícula Digital, PSM, TaxiRio etc);

IV - ativo tecnológico: equipamento de TIC, software ou aplicação que suporta as atividades, processos de negócio e serviços de uma organização;

V - *backup* ou cópia de segurança - conjunto de procedimentos que permitem que os dados de um ativo tecnológico sejam salvos. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

VI - *backup completo (full)*: conjunto de procedimentos que permitam que todos os dados sejam salvos;

VII - *backup* incremental/cumulativo: conjunto de procedimentos que permitam que os dados modificados ou criados desde o último backup (seja completo, diferencial ou incremental) sejam salvos;

VIII - *backup* diferencial: conjunto de procedimentos que permitam que somente os dados que mudaram ou foram criados depois do último backup completo sejam salvos;

IX - equipamento de TIC: equipamento componente da infraestrutura de Tecnologia da Informação e Comunicação - TIC (por exemplo: computador, notebooks, *tablets*, *smartphones*, servidores, roteadores, *switches* etc);

X - recuperação (*restore*): conjunto de procedimentos que permitam a recuperação dos dados de um *backup*;

XI - rede corporativa: conjunto de equipamentos de TIC interligados responsáveis pelo armazenamento, compartilhamento e processamento das informações que suportam as atividades, processos e serviços de uma organização;

XII - servidor: computador de alta capacidade que faz parte de uma rede corporativa, e que fornece serviços a outros computadores;

XIII - servidor de arquivos: servidor onde são armazenados os arquivos, dados e informações corporativos;

XIV - *software*: sistema operacional ou aplicativo de terceiros utilizado no suporte às atividades de uma organização (por exemplo: Microsoft Windows, Linux, Microsoft Office, Oracle, Microsoft SQL Server, MariaDB, Thunderbird etc);

XV - usuário: qualquer pessoa autorizada a usar um ativo tecnológico.

Art. 4º Todas as informações corporativas tratadas pelos usuários devem ser armazenadas na rede corporativa ou nas plataformas de nuvem corporativa.

Parágrafo único. Os arquivos armazenados nas estações de trabalho não integrarão o escopo do processo de *backup* e, portanto, não estarão disponíveis para recuperação.

Art. 5º Um processo de gestão de cópias de segurança (*backup*) e recuperação de dados (*restore*) deve ser criado, documentado, implementado e mantido por todos os órgãos, entidades ou prestadores de serviço que administram ativos tecnológicos que hospedam informações que suportem processos ou serviços da Administração Pública Municipal.

I - a elaboração do processo deve considerar os riscos a que as informações estejam expostas e o nível de impacto nos processos e serviços que estas suportam diante de sua indisponibilidade;

II - as rotinas de *backup* devem ser executadas regularmente e orientadas para possibilitar a recuperação das informações em prazos que sejam compatíveis com os níveis de sensibilidade dos processos e serviços que suportam a períodos de indisponibilidade;

III - o processo deve ser revisado, no mínimo, anualmente.

CAPÍTULO II DAS MEDIDAS DE SEGURANÇA

Art. 6º Um plano formal deve detalhar o processo de *backup* definindo aspectos como:

I - dados a serem cobertos pelo processo de *backup* e sua periodicidade;

II - soluções tecnológicas utilizadas;

III - localização física das mídias de *backups*;

IV - definição dos tipos de *backup* (completo, incremental ou diferencial);

V - definição das mídias de armazenamento;

VI - cálculo dos custos estimados associados às estratégias de *backup* definidas;

VII - seleção e capacitação dos recursos humanos envolvidos;

VIII - procedimentos de revisão e atualização do plano.

§ 1º A definição da estratégia e da periodicidade do *backup* deve estar baseada no entendimento dos requisitos das aplicações que seus dados suportam, de seus ciclos de operação e do seu volume de dados tratados;

§ 2º Toda aplicação desenvolvida ou internalizada pela Administração Pública Municipal deve ter sua estratégia de *backup* e recuperação de dados definida como parte de seus requisitos de segurança. Esta estratégia deve fazer parte da documentação da aplicação.

Art. 7º As informações sensíveis quanto à confidencialidade devem ser armazenadas de forma criptografada.

Art. 8º Sempre que possível, deverá ser utilizada autenticação multifator para acesso às soluções de *backup* e recuperação.

Art. 9º Todas as cópias de segurança devem ser armazenadas em local seguro, protegido por controles de acesso físico compatíveis com seu nível de risco.

Parágrafo único. O local em que os *backups* são armazenados deve ser protegido contra agentes nocivos naturais (ex. poeira, calor, umidade), bem como contra fogo.

Art. 10. Devem ser mantidas três cópias completas dos dados: duas das quais armazenadas localmente, mas em diferentes tipos de mídia, e uma cópia armazenada em um local remoto não conectado à sua rede de origem.

Art. 11. Os procedimentos de *backup* e recuperação devem ser testados regularmente, de modo a certificar que os *backups* estejam funcionando corretamente e que, sempre que necessário, os dados possam ser recuperados de forma eficiente.

§ 1º Um plano para recuperação dos dados deve ser desenvolvido e implantado a fim de permitir a sua pronta recuperação em caso de incidentes de segurança;

§ 2º As rotinas de *backups* devem ser monitoradas de maneira que eventuais falhas sejam identificadas e corrigidas quanto antes;

§ 3º A integridade dos *backups* deve ser testada regularmente por intermédio de procedimentos baseados em amostragem, ou seja, através da recuperação de subconjuntos aleatórios dos dados armazenados;

Art. 12. Toda aplicação a ser descontinuada deve ter seus dados submetidos a um *backup full* com período de retenção definido em conformidade com legislação específica.

Parágrafo único. Caso não exista legislação específica, o período de retenção deverá ser definido de comum acordo pelo gestor da aplicação e pelo provedor do serviço de *backup*, observando requisitos relacionados à relevância dos dados e à capacidade operacional do provedor.

CAPÍTULO III DAS COMPETÊNCIAS

Art. 13. Compete à IplanRio definir e administrar as soluções corporativas de suporte ao *backup* e à recuperação dos dados hospedados no *Datacenter* da IplanRio.

Art. 14. Compete aos órgãos e entidades definir e administrar as soluções corporativas de suporte ao *backup* e à recuperação dos dados hospedados em seus ambientes de processamento da informação.

Art. 15. Compete aos usuários manter as informações corporativas armazenadas na rede ou nas plataformas de nuvem corporativa, visando garantir que estas sempre estejam sendo periodicamente salvas.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 16. Aplicam-se ao serviço de cópia de segurança e de recuperação de dados, no que couber, as disposições da Política de Segurança da Informação e de suas normas complementares.

Art. 17. Os agentes públicos que desempenham papéis no suporte aos processos de cópia de segurança e de recuperação de dados, uma vez comprovada imperícia, imprudência ou negligência em sua atuação, que tenha contribuído para incidente de segurança confirmado, ficam sujeitos a sanções administrativas conforme a legislação em vigor.

Art. 18. 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