Protocolo: 1104463
Data: 26/08/2025
Título: DECRETO RIO Nº 56648
Página(s): a

DECRETO RIO Nº 56648 DE 25 DE AGOSTO DE 2025

Estabelece a norma para Segurança Física dos Ambientes de Processamento de Informação 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, visando à proteção destes processos e serviços, torna-se crucial prevenir acessos não autorizados, danos e interferências nas instalações responsáveis por hospedar os ativos tecnológicos que os suportam,

DECRETA:

Art. 1º Fica estabelecida norma para Segurança Física dos Ambientes de Processamento da Informação da Administração Pública Municipal.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º Esta norma aplica-se a todos os agentes públicos municipais independentemente de sua função, cargo, ou vínculo empregatício, aos prestadores de serviços ou quaisquer pessoas físicas ou jurídicas que estejam autorizadas a acessar os ambientes de processamento da informação da Administração Pública Municipal.

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

I - 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;

II - ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos seus ativos ou prejuízos decorrentes de situações inesperadas (por exemplo: incêndio, falha de equipamentos, indisponibilidade de sistemas ou serviços, destruição de informações sensíveis, dentre outros);

III - análise de riscos: processo sistemático que identifica e avalia os níveis de risco relacionados à segurança da informação presentes numa organização;

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

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

VI - auditoria: processo de registro contínuo de informações que identifique a autoria, assim como as ações realizadas sobre um objeto (por exemplo: alterações ou exclusões de registros de arquivos, de tabelas de um banco de dados, de campos de uma tabela etc.);

VII - autenticação: processo de reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica. Há diversos métodos de autenticação utilizando mecanismos como senhas, impressão digital, certificado digital, reconhecimento da íris, dentre outros;

VIII - autorização: concessão ao usuário, após sua autenticação, de um conjunto de permissões de acesso às funcionalidades de um ativo tecnológico;

IX - avaliação de riscos: processo de comparar o risco estimado com critérios de risco pré-definidos para determinar a criticidade (grau) do risco;

X - confidencialidade: propriedade que garante que a informação só está disponível a indivíduos ou processos autorizados;

XI - disponibilidade: propriedade que garante que a informação está disponível às pessoas e aos processos autorizados a qualquer momento em que sejam requeridas;

XII - distância segura: distância definida com base em análise de riscos, especificações técnicas realizadas por entidades de notória especialização e normas técnicas vigentes;

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

XIV - identificação: processo pelo qual um usuário fornece sua identidade para acesso ao ambiente de processamento de informação;

XV - 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 tecnológicos de uma organização;

XVI - informação: resultado do processamento, manipulação e organização de dados de tal forma que represente um acréscimo ao conhecimento da pessoa que a recebe, podendo se apresentar de diversas formas, como texto, imagem, áudio etc.;

XVII - integridade: propriedade que garante que informação está intacta e protegida contra perda, dano ou modificação não autorizada;

XVIII - perímetro de segurança: refere-se a linha que delimita a fronteira de proteção dos ativos tecnológicos, podendo, para tanto, serem usadas barreiras como paredes, portões de entrada, balcões de recepção, etc.;

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

XX - *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);

XXI - usuário: qualquer pessoa autorizada a acessar os ambientes de processamento da informação da PCRJ;

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

Art. 4º Considerando o caráter institucional dos ambientes corporativos de processamento da informação, todos os acessos a estes ambientes são passíveis de monitoração e auditoria, podendo a Administração Pública Municipal, a qualquer tempo, utilizar quaisquer meios legais que permitam identificar e bloquear, o acesso aos ambientes corporativos de processamento da informação de modo a salvaguardar seus interesses no que diz respeito à gestão de riscos de segurança da informação.

CAPÍTULO II
DA SEGURANÇA FÍSICA E DO AMBIENTE

Seção I
Do Perímetro de Segurança Física

Art. 5º Os perímetros de segurança dos ambientes de processamento de informação dos órgãos e entidades municipais devem ser claramente definidos, possuindo localização e capacidade de resistência a ameaças físicas definidas em função dos requisitos de segurança dos ativos tecnológicos hospedados em seu interior e dos resultados de processos periódicos de análise e avaliação de riscos.

Parágrafo único. Os ativos tecnológicos devem estar abrigados em instalações que estejam em conformidade com as características técnicas mínimas de hospedagem definidas por seus fabricantes, fornecedores e normas técnicas vigentes.

Art. 6º Os perímetros de um edifício ou de um local que contenha instalações de processamento de informação devem possuir paredes externas, de construção robusta, e controles de acesso físico para todas as suas portas, de modo a reduzir o risco de acessos não autorizados ou invasões.

Seção II
Dos Controles de Entrada Física

Art. 7º Os ambientes de processamento de informação dos órgãos e entidades municipais devem possuir área de recepção, ou algum outro meio para controlar o acesso físico ao local, devendo este permanecer restrito somente ao pessoal autorizado.

Art. 8º Os ambientes de processamento da informação devem utilizar controles de identificação, autenticação e auditoria visando identificar, autorizar, validar e registrar todos os acessos a estas instalações.

Art. 9º Um registro físico ou uma trilha de auditoria eletrônica de todos os acessos aos ambientes de processamento de informação dos órgãos e entidades municipais deve ser mantido e armazenado de forma segura.

Art. 10. O acesso de visitantes aos ambientes de processamento da informação deve ocorrer para finalidades específicas, mediante prévia autorização e sob a supervisão de agente representante do setor ou grupo responsável por sua administração.

Art. 11. O acesso e circulação de agentes públicos municipais por ambientes de processamento da informação somente devem ser permitidos mediante o porte, em local visível, de sua identificação funcional.

Art. 12. Os pontos de acesso, tais como áreas de entrega, carregamento, ou outros pontos em que agentes externos aos órgãos e entidades municipais tenham acesso às suas instalações, devem ser controlados e isolados dos ambientes de processamento da informação, visando evitar acessos não autorizados.

Art. 13. Nos ambientes de processamento da informação, a utilização de dispositivos eletrônicos como máquinas fotográficas, câmeras, filmadoras, gravadores, telefones celulares e semelhantes só será permitida mediante autorização formal do responsável pela administração do ambiente.

Seção III
Da Proteção contra Ameaças Internas

Art. 14. Nos ambientes de processamento de informação, é proibida a utilização de quaisquer de seus ativos tecnológicos ou de infraestrutura por agentes externos sem prévia autorização do responsável pela administração do ambiente.

Art. 15. Os ambientes de processamento de informação devem ser permanentemente monitorados por sistemas de câmeras de segurança, com controle de acesso a estes sistemas definido pelo responsável pela administração do ambiente.

Seção IV
Da Proteção contra Ameaças Externas

Art. 16. Deve-se identificar, planejar, implementar e manter os controles para proteção física contra incêndios, enchentes, explosões, vandalismo, sabotagem, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem.

Art. 17. Os materiais perigosos ou combustíveis devem ser armazenados a uma distância segura dos ambientes de processamento da informação.

Art. 18. Todos os recursos de contingência, inclusive os de *backup*, devem permanecer a uma distância segura do local onde residem os recursos para os quais estes estão provendo contingência.

Art. 19. Os sistemas de proteção de incêndio devem ser instalados seguindo legislação específica.

CAPÍTULO III
Das Competências e Responsabilidades

Art. 20. Compete aos Órgãos e Entidades municipais:

I - promover todas as ações necessárias para que seus ambientes de processamento da informação mantenham-se em conformidade às determinações descritas nesta norma;

II - definir os perímetros de segurança dos seus ambientes de processamento da informação;

III - estabelecer regras para o uso de credenciais físicas, que se destinam ao controle de acesso às suas áreas e instalações;

IV - definir, implementar e orientar o uso de barreiras físicas de segurança, bem como equipamentos ou mecanismos de controle de entrada e saída.

Art. 21. É responsabilidade dos agentes públicos municipais reportar aos setores competentes quaisquer ameaças ou vulnerabilidades que tenham ciência, relativas à segurança física dos ambientes corporativos de processamento da informação.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 22. Aplicam-se à segurança física dos ambientes de processamento da informação, no que couber, as disposições da Política de Segurança da Informação e de suas normas complementares.

Art. 23. Os agentes públicos municipais usuários ou administradores dos ambientes de processamento da informação da Administração Pública Municipal que violarem esta norma são passíveis das sanções administrativas cabíveis, conforme a legislação em vigor.

Art. 24. 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