Protocolo: 1104456
Data: 26/08/2025
Título: DECRETO RIO Nº 56641
Página(s): a

DECRETO RIO Nº 56641 DE 25 DE AGOSTO DE 2025

Estabelece norma para a Proteção Contra Códigos Maliciosos 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 os códigos maliciosos, uma vez inseridos nos ambientes de Tecnologia da Informação e Comunicação (TIC), podem comprometer a confidencialidade, integridade ou disponibilidade das informações residentes nestes ambientes;

CONSIDERANDO que os códigos maliciosos têm se mantido há anos como uma das principais ameaças aos sistemas de informação, causando danos de toda ordem em organizações públicas e privadas em todo o mundo,

DECRETA:

Art. 1º Fica estabelecida a norma para a Proteção Contra Códigos Maliciosos, no âmbito da Administração Pública Municipal.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º Esta norma aplica-se a todos os usuários e ativos tecnológicos que integram a rede corporativa da Administração Pública Municipal.

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 - 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);

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

IV - 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.);

V - 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;

VI - código malicioso: qualquer *software* que tem por finalidade comprometer a segurança (confidencialidade, integridade ou disponibilidade) das informações presentes nos ativos tecnológicos (por exemplo: vírus, *worms*, cavalos de tróia e *ransomwares*);

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

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

IX - *download*: transferência de arquivo(s) residente(s) em sites da Internet para equipamentos internos da PCRJ;

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

XI - 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.;

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

XIII - *ransomware*: tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário (fonte: Cert.br);

XIV - 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;

XV - *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);

XVI - usuário: qualquer pessoa autorizada a usar os serviços de TIC da Prefeitura da Cidade do Rio de Janeiro;

XVII - vírus: classe de programas maliciosos que tem a habilidade de se auto replicar e provocar danos à confidencialidade, integridade e disponibilidade das informações. O vírus depende de outro programa (hospedeiro) para se tornar ativo;

XVIII - *worm*: programa capaz de criar cópias de si mesmo e distribuí-las automaticamente entre os computadores de uma rede de comunicação que, diferentemente de um vírus, não necessita de outro programa para realizar as suas ações de contaminação.

Art. 4º Todos os acessos aos ativos tecnológicos corporativos são passíveis de monitoração e auditoria e a Administração Pública Municipal reserva-se o direito de:

I - identificar, monitorar e avaliar, a qualquer tempo, o uso de seus ativos tecnológicos de modo a salvaguardar seus interesses no que diz respeito à gestão de riscos de segurança;

II - utilizar quaisquer meios legais que permitam a prevenção, detecção e o bloqueio ou exclusão de códigos maliciosos presentes em seus ativos tecnológicos.

CAPÍTULO II
DAS MEDIDAS DE SEGURANÇA

Art. 5º Devem ser observadas as seguintes medidas de proteção contra códigos maliciosos:

I - os ativos tecnológicos dos órgãos e entidades municipais devem possuir instalada a solução de proteção contra códigos maliciosos homologada por suas respectivas áreas de gestão de TIC;

II - soluções de proteção contra códigos maliciosos que apresentarem funcionamento atípico ou anormal devem ser reinstaladas e, ao término da reinstalação, devem ter seus equipamentos hospedeiros verificados quanto à presença de códigos maliciosos;

III - é vedada ao usuário de equipamento de TIC corporativo a desinstalação, desativação ou alteração de configuração de sua solução de proteção contra códigos maliciosos;

IV - os equipamentos de TIC devem se manter atualizados quanto a seus patches de segurança e perfis de configuração segura conforme as recomendações dos respectivos fabricantes;

V - os equipamentos de TIC devem estar configurados de acordo com os padrões mais restritivos de segurança possíveis, de maneira que prestem apenas os serviços para os quais foram instalados;

VI - antes de sua utilização, toda e qualquer mídia portátil de armazenamento deve ser verificada quanto à existência de códigos maliciosos;

VII - antes de sua utilização, todo e qualquer arquivo recebido deve ser verificado quanto à existência de códigos maliciosos.

Art. 6º O correio eletrônico, as redes sociais, os aplicativos de mensagens instantâneas e a Internet são os principais meios para a disseminação de códigos maliciosos, motivo pelo qual, durante sua utilização, devem ser adotadas as seguintes medidas preventivas:

I - não abrir arquivos ou "clicar" em *links* anexados a mensagens de origem desconhecida, suspeita ou não confiável, hipótese em que estas devem ser removidas imediatamente;

II - não realizar *downloads* de arquivos de origem desconhecida, suspeita ou não confiável.

III - não efetuar o tratamento e correção de códigos maliciosos por iniciativa própria.

Art. 7º Uma vez identificada uma infecção por códigos maliciosos, seja esta provável ou confirmada, devem ser realizadas as seguintes ações imediatas de contenção:

I - desconexão do equipamento de TIC da rede corporativa;

II - abertura de chamado junto ao setor de atendimento da área de gestão de TIC responsável pela administração do ativo.

CAPÍTULO III
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 8º Compete aos Órgãos e Entidades promover as ações internas necessárias para que seus ativos tecnológicos sejam mantidos em conformidade às determinações descritas nesta norma.

Art. 9º Compete às áreas de gestão de TIC dos órgãos e entidades:

I - pesquisar, implementar e administrar as soluções de proteção contra códigos maliciosos, garantindo que os equipamentos de TIC corporativos estejam executando corretamente suas soluções de proteção e que estas se mantenham atualizadas;

II - planejar, implementar e administrar os processos, atividades e procedimentos de gerenciamento de riscos relacionados a códigos maliciosos;

III - prover serviço de tratamento de incidentes relacionados a códigos maliciosos;

IV - homologar as soluções de proteção contra códigos maliciosos a serem instaladas nos equipamentos corporativos;

V - prestar suporte aos usuários em incidentes de segurança que envolvam códigos maliciosos.

Art. 10. Compete aos usuários:

I - mesmo com a presença da ferramenta para proteção contra códigos maliciosos nos ativos de TIC, os(as) usuários(as) deverão adotar um comportamento cauteloso, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos.

II - abrir chamado para o setor de atendimento de sua área de gestão de TIC, o mais rapidamente possível, diante de qualquer suspeita de ataque por código malicioso a equipamento de TIC sob sua custódia, ou mesmo à sua rede local;

III - sempre que iniciar a utilização de equipamento de TIC sob sua custódia, verificar se a solução de proteção contra códigos maliciosos residente está ativa, atualizada e funcionando normalmente, caso contrário, deve abrir chamado para o setor de atendimento da área de Gestão de TIC responsável pela administração do equipamento.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 11. Aplicam-se à proteção contra códigos maliciosos, no que couber, as disposições da Política de Segurança da Informação e de suas normas complementares.

Art. 12. Os usuários que violarem esta norma ficam sujeitos às sanções administrativas cabíveis, conforme a legislação em vigor.

Art. 13. 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