Protocolo: 1104459
Data: 26/08/2025
Título: DECRETO RIO Nº 56644
Página(s): a

DECRETO RIO Nº 56644 DE 25 DE AGOSTO DE 2025

Estabelece norma para Criação e Manutenção de Senhas de Acesso a Ativos Tecnológicos 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 as senhas constituem um dos tipos de credencial mais utilizados para o controle de acesso aos ativos tecnológicos dos órgãos e entidades municipais;

CONSIDERANDO que a quebra de confidencialidade de senhas pode resultar em acessos não autorizados aos ativos tecnológicos municipais, os quais expõem a Administração Pública Municipal a riscos de segurança da informação,

DECRETA:

Art. 1º Fica estabelecida a norma para criação e manutenção de senhas de acesso a ativos tecnológicos no âmbito 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, estagiários ou quaisquer pessoas físicas ou jurídicas que estejam autorizadas a acessar os ativos tecnológicos 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: SIAFIC, SINAE, Matrícula Digital, PSM, TaxiRio etc);

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

IV - 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;

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

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

VII - criptografia: conjunto de técnicas pelas quais a informação pode ser transformada de sua forma original para outra codificada, de maneira que possa ser reconhecida apenas por seu criador (emissor) e seu destinatário (receptor);

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

IX - 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.;

X - macros: comandos ou ações tipicamente empregados para automatizar sequências de instruções, movimentos ou regras frequentemente usadas;

XI - sistema de informação: sistema composto por um conjunto de ativos tecnológicos que tem por objetivo armazenar, transportar e processar informações visando suportar funções, serviços ou processos de uma organização;

XII - *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);

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

CAPÍTULO II
DAS NORMAS REGULAMENTADORAS

Art. 4º As senhas devem conter, no mínimo, os seguintes tipos de caracteres: letras minúsculas, letras maiúsculas, números e caracteres especiais.

Art. 5º As senhas de acesso aos ativos tecnológicos devem ter o tamanho mínimo de 10 (dez) posições.

Parágrafo único. As senhas das contas de administração devem possuir tamanho mínimo de 14 (catorze) posições.

Art. 6º Quanto à criação e atualização de senhas:

I - a senha inicial deve ser temporária, sendo obrigatória a sua atualização no primeiro acesso;

II - a conta do usuário deve ser automaticamente excluída quando sua senha temporária não for alterada após 30 (trinta) dias;

III - deve ser permitido ao usuário alterar sua senha a qualquer tempo;

IV - a nova senha não poderá ser igual às últimas 5 (cinco) senhas utilizadas;

V - a senha deverá ser alterada, obrigatoriamente, a cada 60 (sessenta) dias;

VI - deve-se evitar a utilização de informações pessoais na criação da senha de acesso.

Art. 7º Quanto à proteção devem ser observadas as seguintes diretrizes:

I - O usuário deve manter a confidencialidade de suas senhas, estando ciente que a inobservância desta prática implicará na sua responsabilidade por qualquer ato praticado por sua utilização indevida;

II - as senhas devem ser alteradas sempre que haja suspeita de comprometimento de sua confidencialidade.

III - as senhas não devem ser inseridas em mensagens de correio eletrônico ou em qualquer outra forma de comunicação eletrônica;

IV - as senhas não devem ser reveladas por quaisquer meios de comunicação a quem quer que seja;

V - as senhas não devem ser reveladas em quaisquer tipos de questionários ou formulários;

VI - as senhas não devem constar de quaisquer registros escritos (por exemplo, em post-its, bloco de notas, agendas etc);

VII - as senhas não devem ser armazenadas sem que estejam criptografadas;

VIII - é vedado o uso do recurso de registro de senhas oferecido por aplicativos (por exemplo: navegadores Web).

Art. 8º Quanto ao uso, devem ser observadas as seguintes diretrizes:

I - as senhas de usuários não devem ser incluídas em nenhum processo automático de acesso a sistemas de informação (por exemplo: senhas armazenadas em macros ou funções de *software*);

II - os sistemas de autenticação devem ser configurados para que o usuário tenha direito a 3 (três) tentativas de autenticação e, ultrapassado este limite, tenha seu acesso suspenso até que acione os procedimentos ou mecanismos de recuperação ou atualização de senhas;

III - os sistemas de informação devem prover mecanismos para que o próprio usuário realize a atualização de suas senhas a qualquer tempo;

IV - as senhas utilizadas pelos sistemas de informação devem ser armazenadas e transmitidas de forma criptografada.

CAPÍTULO III
DAS DISPOSIÇÕES FINAIS

Art. 9º Aplicam-se à criação e manutenção das senhas de acesso, no que couber, as disposições da Política de Segurança da Informação e de suas normas complementares.

Art. 10. Os usuários que violarem esta norma ficam sujeitos às sanções administrativas cabíveis, conforme a legislação em vigor.

Art. 11. 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