Protocolo: 1104464
Data: 26/08/2025
Título: DECRETO RIO Nº 56649
Página(s): a

DECRETO RIO Nº 56649 DE 25 DE AGOSTO DE 2025

Regulamenta a norma de Controle de Acesso aos 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 o controle de acesso aos ativos tecnológicos que suportam os processos e serviços municipais é medida imprescindível à redução dos riscos de segurança da informação,

DECRETA:

Art. 1º Este Decreto Regulamenta a norma de Controle de Acesso aos Ativos Tecnológicos no âmbito da Administração Pública Municipal.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º A presente norma estabelece as regras a serem observadas na gestão de contas e credenciais de acesso dos usuários de ativos tecnológicos no âmbito da Administração Pública Municipal, sendo complementar à Política de Segurança da Informação (PSI).

Art. 3º Esta norma aplica-se a todos os ativos tecnológicos que integram a rede corporativa da Administração Pública Municipal.

Art. 4º 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 - 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 - autorização: concessão ao usuário, após sua autenticação, de um conjunto de permissões de acesso aos recursos e funcionalidades de um ativo tecnológico;

VII - conta de acesso: identificador único, pessoal e intransferível de um usuário, que o identifica durante os acessos realizados a ativos tecnológicos;

VIII - credencial de acesso: componente físico ou lógico responsável por autenticar a identidade de um usuário durante os acessos realizados a ativos tecnológicos, por exemplo, senhas, PINs, certificados digitais e biometria;

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

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 - gestor de acesso: agente público responsável pelo gerenciamento do ciclo de vida das contas de acesso dos usuários do órgão ou entidade a um conjunto de ativos tecnológicos;

XII - gestor do ativo tecnológico: agente público responsável por tomar decisões referentes à segurança do ativo, definir seus perfis de acesso, garantir sua conformidade com políticas e normas vigentes e relatar quaisquer incidentes ou problemas de segurança aos agentes competentes;

XIII - 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.;

XIV - perfil de acesso: conjunto de privilégios atribuído a um usuário;

XV - privilégio: direito e permissão de acesso a um ativo tecnológico concedido a um usuário;

XVI - 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;

XVII - *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);

XVIII - suspensão da conta: refere-se à desativação temporária de contas em resposta a eventos de desconformidade a políticas ou normas de segurança vigentes;

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

Art. 5º A utilização dos ativos tecnológicos corporativos deve estar alinhada aos interesses da Administração Pública Municipal e ocorrer dentro de um comportamento profissional, ético e legal.

Art. 6º O acesso dos usuários aos ativos tecnológicos deve ocorrer por intermédio de conta de uso pessoal e intransferível.

Parágrafo único. Os usuários dos ativos tecnológicos devem ser identificados por sua conta de acesso, autenticados e autorizados a usar somente as funcionalidades que sejam imprescindíveis ao desempenho de suas competências e responsabilidades.

Art. 7º A Administração Pública Municipal se reserva o direito de monitorar e avaliar, a qualquer tempo, a utilização das contas e credenciais de acesso aos seus ativos tecnológicos de modo a salvaguardar seus interesses no que diz respeito à gestão de riscos de segurança da informação.

CAPÍTULO II
DA GESTÃO DE CONTAS E CREDENCIAIS

Art. 8º Um processo de gestão de contas e credenciais de acesso aos ativos tecnológicos deve ser criado, implantado e mantido em todos os órgãos e entidades municipais, atendendo aos seguintes requisitos:

I - o processo deve contemplar ações para as seguintes etapas do ciclo de vida da gestão de contas e credenciais de acesso:

a) credenciamento: refere-se à recepção e verificação da identidade dos novos usuários;

b) criação de conta: refere-se à criação das contas dos novos usuários regularmente credenciados;

c) criação e emissão de credenciais: refere-se à criação e ao fornecimento ao usuário de senhas, certificados digitais, *tokens*, crachás ou quaisquer outras credenciais necessárias à utilização de suas contas;

d) utilização de conta e credencial: refere-se à utilização pelos usuários de suas contas e credenciais para acesso aos ativos tecnológicos que suportam o desempenho de suas competências e responsabilidades;

e) manutenção de acesso: refere-se à gestão das alterações de permissões de acesso dos usuários diante de eventos como mudanças de função ou ausências prolongadas;

f) encerramento da conta: refere-se à desativação permanente da conta e revogação de suas credenciais diante do término do vínculo de seu usuário com a Administração Pública Municipal.

II - o processo deve constar de controles que garantam a autenticidade das operações realizadas por todos os agentes públicos que atuam na gestão do ciclo de vida das contas e credenciais de acesso, assim como a legitimidade de suas ações considerando suas competências e responsabilidades no referido ciclo;

III - todos os agentes públicos que desempenhem atividades no processo devem ser tecnicamente qualificados para exercer suas competências e responsabilidades;

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

CAPÍTULO III
DA GESTÃO DO CICLO DE VIDA DE CONTAS E CREDENCIAIS

Seção I
Do Credenciamento

Art. 9º Os órgãos e entidades devem implementar procedimentos formais de suporte ao credenciamento de novos usuários atendendo aos seguintes requisitos:

I - devem garantir a autenticidade da identidade dos novos usuários;

II - devem garantir que os novos usuários, uma vez autenticados, sejam orientados a tomar ciência das políticas e normas de segurança e privacidade vigentes.

Seção II
Da Criação de Contas

Art. 10. Na etapa de criação de contas devem ser atendidos os seguintes requisitos:

I - os gestores de ativos tecnológicos devem desenvolver e implantar procedimentos padronizados para a solicitação de criação de contas e credenciais, assim como para a concessão de perfis de acesso;

II - o processo de concessão de perfis de acesso deve contemplar somente os privilégios imprescindíveis à execução das competências e responsabilidades de seus usuários;

III - o perfil de administrador deve ser fornecido apenas para contas de administração;

IV - as contas com perfil de acesso privilegiado devem ser usadas apenas para suportar atividades para as quais este perfil de acesso seja imprescindível;

V - todos os ativos tecnológicos devem conter um inventário de suas contas, que deverá conter, pelo menos, as seguintes informações:

a) matrícula ou CPF, nome do usuário e lotação;

b) nome da conta (login);

c) data de criação;

d) data de encerramento;

e) órgão ou entidade de origem;

f) CNPJ e nome da empresa de origem, em caso de prestadores de serviço;

g) status da conta (ativa, suspensa ou encerrada).

Art. 11. A solicitação de criação de conta de acesso deve conter, pelo menos, as seguintes informações:

I - para agentes públicos: matrícula, nome completo, lotação e perfil de acesso;

II - para estagiários: CPF, nome completo, órgão ou entidade, lotação, perfil de acesso, número e período de vigência do contrato de estágio;

III - para prestadores de serviços: CPF, nome completo, órgão ou entidade, lotação, perfil de acesso, número e período de vigência do contrato, CNPJ e nome da empresa contratada.

Seção III
Da Criação e Emissão de Credenciais

Art. 12. Na etapa de criação e emissão de credenciais devem ser atendidos os seguintes requisitos:

I - os processos de criação, emissão e entrega de credenciais devem dispor de controles de segurança compatíveis com seus respectivos níveis de risco;

II - cada tipo de credencial utilizada deve dispor de regulamentação específica de utilização que leve em conta requisitos de eficiência, eficácia e segurança.

Seção IV
Da Utilização de Contas e Credenciais

Art. 13. Na etapa de utilização de contas e credenciais devem ser atendidos os seguintes requisitos:

I - as contas e credenciais devem ser utilizadas somente para os fins previstos;

II - as contas e credenciais são de uso exclusivo, sendo vedado o seu compartilhamento;

III - sempre que possível, o acesso aos ativos tecnológicos deve ser suportado por autenticação multifator;

IV - as falhas durante o processo de autenticação devem ser registradas e continuamente monitoradas pela área responsável pela administração do respectivo serviço de autenticação;

V - diante de quaisquer incidentes de segurança envolvendo contas ou credenciais, os gestores dos respectivos ativos e os titulares dessas contas devem ser imediatamente notificados.

Seção V
Da Manutenção de Contas e Credenciais

Subseção I
Das Regras Gerais

Art. 14. As contas de acesso padrão de ativos tecnológicos devem ter suas credenciais alteradas antes que estes ativos entrem em operação.

Art. 15. Somente devem ser atendidas solicitações de atualização de perfis de acesso ou suspensão de contas que sejam realizadas por seus respectivos agentes competentes.

Art. 16. Os gestores de ativos tecnológicos devem desenvolver e implantar procedimentos padronizados para a criação e manutenção de contas, credenciais e perfis de acesso.

Subseção II
Da Suspensão de Contas

Art. 17. A conta deve ser suspensa:

I - quando solicitado pela chefia imediata ou superior do usuário, formalmente justificado.

II - sempre que houver suspeita ou confirmação de que sua utilização infrinja a regulamentação de segurança ou privacidade vigentes;

III - por solicitação da área de Gestão de Pessoas quando do afastamento do usuário em decorrência de processo administrativo disciplinar, cessão do funcionário a outro órgão ou outros afastamentos que o justifiquem;

IV - quando permanecer sem uso por período superior a 90 (noventa) dias.

Seção VI
Do Encerramento de Contas

Art. 18. Na etapa de encerramento devem ser atendidos os seguintes requisitos:

I - os gestores de ativos tecnológicos devem desenvolver e implantar procedimentos padronizados para o encerramento de contas;

II - todas as credenciais do usuário devem ser revogadas e, sempre que cabível, recolhidas imediatamente após o seu desligamento;

III - os mecanismos de autoatendimento para atualização de credenciais não devem permitir a reativação de contas encerradas;

IV - os processos e prazos de retenção e preservação das informações relativas às contas de acesso encerradas, incluindo seus registros de atividade, devem estar em conformidade com a legislação vigente.

CAPÍTULO IV

DAS COMPETÊNCIAS

Art. 19. Compete à IplanRio:

I - definir e administrar as soluções corporativas de suporte ao controle de acesso aos ativos tecnológicos;

II - prestar suporte aos órgãos e entidades na implementação e utilização das soluções corporativas de suporte ao controle de acessos aos ativos tecnológicos;

III - tornar públicos os limites e as restrições de uso definidos para os ativos tecnológicos.

Art. 20. Compete aos órgãos e entidades municipais:

I - definir, implantar e manter um processo de gestão de contas e credenciais de acesso de seus agentes públicos e prestadores de serviço;

II - implementar as soluções corporativas de suporte ao controle de acessos em seus ativos tecnológicos;

III - garantir que as soluções corporativas de suporte ao controle de acessos sejam mantidas atualizadas em todos os seus ativos tecnológicos;

IV - sempre que previsto na estratégia ou regulamentação de acesso a algum ativo tecnológico, designar seu gestor de acesso;

V - para todos os ativos tecnológicos que possuam gestor de acesso, manter atualizados junto aos seus respectivos gestores o cargo/emprego, a matrícula, o nome e o endereço de correio eletrônico do(s) gestor(es) de acesso e de seu(s) substituto(s);

VI - implementar procedimentos que garantam a comunicação eficiente aos gestores de acesso de quaisquer operações ou eventos que possam acarretar mudança de perfil de acesso, suspensão ou cancelamento de contas (por exemplo: mudanças de cargo, emprego ou de lotação, exoneração, demissão ou desligamento).

Art. 21. Compete ao gestor de acesso:

I - solicitar a criação, atualização, suspensão ou cancelamento de contas de usuários dos ativos tecnológicos;

II - criar e manter o inventário de contas de seus usuários;

III - revisar periodicamente a pertinência das contas ativas de seus usuários junto às áreas competentes do órgão ou entidade, com periodicidade definida em função do risco potencial vinculado à criticidade do serviço e o nível de privilégios dos perfis de acesso dessas contas;

IV - gerir o ciclo de vida das contas de seus usuários, de sua criação ao seu encerramento;

V - manter atualizada, para efeito de auditoria e controle, a documentação comprobatória referente às manutenções de contas.

Art. 22. Compete ao gestor do ativo tecnológico:

I - criar e manter o inventário das contas dos usuários do ativo;

II - desenvolver e implantar procedimentos padronizados para o gerenciamento do ciclo de vida das contas, de sua criação ao seu encerramento;

III - definir os perfis de acesso aos ativos tecnológicos, gerenciando todo seu ciclo de vida: criação, utilização, manutenção e término de uso;

IV - administrar e revisar periodicamente a pertinência dos perfis de acesso, com periodicidade de revisão definida em função do risco potencial vinculado aos seus privilégios;

V - implementar e manter registro seguro dos logs de acesso ao ativo.

Art. 23. Compete ao usuário:

I - responder por quaisquer ações realizadas por meio de suas contas de acesso;

II - zelar pela segurança dos ativos tecnológicos sob sua custódia, tomando, no mínimo, as seguintes medidas para reduzir riscos:

a) não permitir a utilização do ativo por agentes não autorizados;

b) atentar para os riscos que possam comprometer a segurança do ativo, assim como suas informações, relatando-os aos agentes competentes;

c) adotar medidas que bloqueiem o acesso de terceiros sempre que completar suas atividades ou quando se ausentar do local de uso do ativo.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 24. Aplicam-se ao controle de acesso aos ativos tecnológicos, no que couber, as disposições da Política de Segurança da Informação e de suas normas complementares.

Art. 25. Os agentes públicos que desempenham papéis no suporte aos processos de controle de acesso aos ativos tecnológicos, 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. 26. Este Decreto entra em vigor na data da sua publicação.

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

EDUARDO PAES