PREFEITURA RIO | Juventude Carioca

# POLÍTICA DE CONTROLE DE ACESSOS
# SECRETARIA ESPECIAL DA JUVENTUDE CARIOCA

## 1. INTRODUÇÃO

A presente Política de Controle de Acessos tem como finalidade estabelecer diretrizes, responsabilidades, critérios e procedimentos aplicáveis à gestão de acessos aos sistemas, serviços, recursos tecnológicos, informações e dados sob responsabilidade da Secretaria Especial da Juventude Carioca (JUVRio).

Esta Política tem como propósito assegurar que o acesso aos ativos de informação da Secretaria seja concedido exclusivamente a pessoas, órgãos ou entidades devidamente autorizados, conforme suas atribuições institucionais e necessidades operacionais, promovendo a confidencialidade, integridade, disponibilidade, rastreabilidade e proteção dos dados tratados pela JUVRio.

O documento está fundamentado nos princípios da segurança da informação e da privacidade, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), com o Decreto Rio nº 54.984/2024 e com a Resolução SEGOVI nº 91/2022, que regulamenta o Programa de Governança em Privacidade e Proteção dos Dados Pessoais (PGPPDP) no âmbito da Administração Pública Municipal do Rio de Janeiro.

## 2. OBJETIVO

Esta Política tem como objetivo estabelecer regras para assegurar que o acesso aos sistemas, serviços, informações e recursos tecnológicos da JUVRio seja realizado de maneira controlada, segura, proporcional e rastreável, observando os princípios do menor privilégio, da necessidade de acesso, da segregação de funções e da proteção dos dados pessoais.

## 3. ABRANGÊNCIA

Esta Política aplica-se a todos os servidores públicos, estagiários, colaboradores terceirizados, consultores, fornecedores e demais prestadores de serviços que, no exercício de suas atividades, utilizem ou tenham acesso a sistemas, aplicações, bancos de dados, documentos, dispositivos tecnológicos, recursos de rede ou quaisquer informações sob responsabilidade ou gestão da Secretaria Especial da Juventude Carioca (JUVRio). As diretrizes estabelecidas nesta Política abrangem todos os ambientes, meios e recursos utilizados para armazenamento, processamento, transmissão ou consulta de informações institucionais, independentemente do formato ou localização dos dados.

## 4. PRINCÍPIOS

A Política de Controle de Acessos da JUVRio é orientada pelos seguintes princípios:

I. Necessidade e finalidade: o acesso aos recursos, sistemas e informações deve ser concedido exclusivamente quando necessário ao desempenho das atribuições institucionais do usuário e em conformidade com a finalidade previamente definida;
II. Menor privilégio: cada usuário deve possuir somente os níveis de acesso estritamente necessários para a execução de suas atividades;
III. Segurança e prevenção: devem ser adotadas medidas técnicas e administrativas adequadas para prevenir acessos não autorizados, uso indevido de informações, vazamentos, fraudes e demais incidentes de segurança;
IV. Responsabilização e rastreabilidade: os acessos devem ser individualizados, registrados e passíveis de monitoramento e auditoria, permitindo a identificação dos responsáveis pelas ações realizadas nos sistemas e recursos institucionais;
V. Transparência: as regras, critérios e procedimentos relacionados ao controle de acessos devem ser divulgados de forma clara aos usuários, promovendo a conscientização quanto às responsabilidades e obrigações aplicáveis;
VI. Revisão periódica: os perfis, permissões e níveis de acesso devem ser avaliados regularmente, garantindo sua contínua adequação.

## 5. PAPÉIS E RESPONSABILIDADES

5.1. Encarregado de Dados Setorial:

- Acompanhar e supervisionar a aplicação desta Política no âmbito da Secretaria;
- Promover a articulação com o Encarregado de Dados da Prefeitura quanto a orientações, incidentes, atualizações normativas e necessidades de revisão dos controles de acesso;
- Apoiar a disseminação das diretrizes de proteção de dados pessoais e controle de acessos junto aos agentes públicos e demais usuários abrangidos por esta Política.

5.2. Comitê de Privacidade e Proteção de Dados Pessoais da JUVRio:

- Apoiar a implementação, avaliação e o monitoramento dos controles de acesso;
- Analisar riscos relacionados ao uso inadequado de acessos e propor medidas preventivas e corretivas;
- Acompanhar ocorrências de segurança da informação e proteção de dados pessoais relacionadas ao controle de acessos.

5.3. Chefia de Gabinete:

- Executar e supervisionar os controles técnicos de autenticação, autorização, alteração e registro de acessos;
- Manter cópias de segurança e registros de auditoria em conformidade com esta Política;
- Implementar processos formais para habilitação, aprovação, habilitação, suspensão e exclusão de acessos;
- Assegurar a realização de cópias de segurança e a preservação dos registros conforme requisitos institucionais aplicáveis.

5.4. Servidores e Colaboradores:

- Utilizar credenciais de acesso pessoais, individuais e intransferíveis;
- Proteger suas credenciais, não compartilhando senhas com terceiros;
- Utilizar os recursos disponibilizados exclusivamente para fins institucionais e conforme os níveis de acesso autorizados;
- Respeitar os níveis de acesso definidos e comunicar imediatamente qualquer suspeita de irregularidade ou uso indevido.

## 6. DIRETRIZES E REGRAS DE ACESSO

6.1) Concessão de acesso

O acesso aos sistemas, serviços, informações e demais recursos institucionais deverá ser concedido mediante solicitação formal do gestor da área responsável e aprovação da autoridade ou responsável designado pela Secretaria. A definição do perfil de acesso deverá considerar as atribuições funcionais do usuário, a finalidade do acesso, os riscos envolvidos e os princípios do menor privilégio e da necessidade de acesso, garantindo que sejam disponibilizados apenas os recursos indispensáveis para o desempenho das atividades.

6.2) Suspensão e revogação de acesso

A revogação ou alteração dos acessos deverá ocorrer de forma tempestiva, de modo a reduzir riscos de acessos não autorizados ou utilização inadequada dos recursos institucionais. Os acessos concedidos deverão ser suspensos, alterados ou revogados nas seguintes situações:

- Encerramento ou alteração do vínculo funcional ou contratual do usuário;

- Afastamento, desligamento, cessação de contrato ou mudança de atribuições que implique alteração das necessidades de acesso;
- Identificação de uso indevido de credenciais, violação de regras de segurança ou descumprimento desta Política;
- Solicitação da autoridade competente ou da unidade responsável pela gestão do acesso.

6.3) Perfis e categorias de acesso

- Administrativo: destinado aos usuários responsáveis por atividades de configuração, administração, manutenção e gestão de sistemas;

- Operacional: destinado aos usuários que necessitam executar atividades rotineiras, incluindo inclusão, atualização, processamento e registro de informações;

- Consulta: destinado aos usuários que necessitam exclusivamente visualizar informações específicas, sem permissão para alteração ou exclusão de dados;

- Restrito: destinado ao acesso a informações sensíveis, críticas ou sujeitas a controles adicionais, podendo exigir mecanismos reforçados de autenticação, incluindo certificado digital ou outros métodos de autenticação segura.

A concessão de cada perfil deverá observar a compatibilidade entre as responsabilidades do usuário e os recursos acessíveis.

6.4) Registo e armazenamento de acessos

Os registros de acesso e demais evidências relacionadas à utilização dos sistemas deverão ser mantidos pelo período mínimo de 5 (cinco) anos ou por prazo superior quando houver determinação legal, regulatória ou necessidade institucional devidamente justificada.

6.5) Acesso às cópias de segurança

O acesso aos arquivos de backup, cópias de segurança e recursos destinados à recuperação de informações deverá ser restrito aos responsáveis formalmente autorizados, observando critérios de necessidade, confidencialidade e rastreabilidade.

## 7. REVISÃO E MONITORAMENTO

A JUVRio deverá revisar esta Política, bem como os perfis e direitos de acesso dos usuários, no mínimo anualmente ou sempre que ocorrerem alterações relevantes nos sistemas, processos institucionais, estrutura organizacional ou legislação aplicável.

As revisões, avaliações de conformidade, auditorias e eventuais ajustes identificados deverão ser formalmente registrados e encaminhados ao Encarregado de Dados Setorial e à Secretaria Municipal de Integridade e Transparência (SMIT), quando aplicável, para ciência e acompanhamento.

## 8. SANÇÕES E RESPONSABILIDADES

O descumprimento das disposições estabelecidas nesta Política poderá sujeitar os servidores, colaboradores, prestadores de serviço e demais usuários autorizados às medidas administrativas, civis e penais cabíveis, conforme a legislação vigente.

## 9. DIVULGAÇÃO E VIGÊNCIA

Esta Política deverá ser divulgada a todos os agentes públicos, colaboradores, prestadores de serviço e demais usuários abrangidos por suas disposições, garantindo o conhecimento das regras e responsabilidades relacionadas ao controle de acessos. Esta Política entra em vigor em 23 de julho de 2026 e permanecerá válida até sua revisão, atualização ou substituição por novo instrumento normativo.