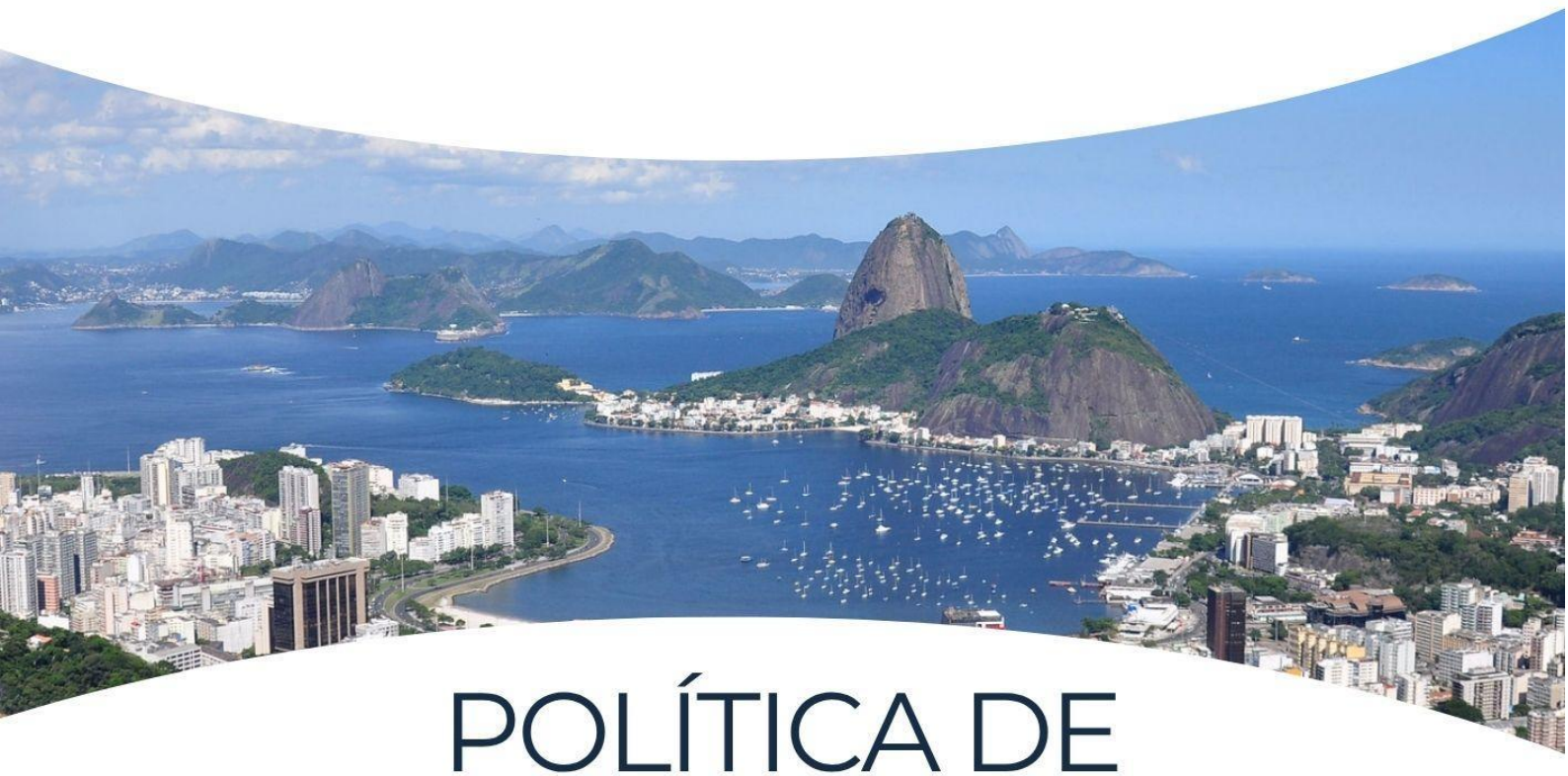
PREFEITURA RIO | Controladoria Geral do Município



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Princípios, diretrizes, responsa bilidades e controles para assegurar a proteção das informações e dos dados pessoais sob custódia da CGM-Rio.

EDIÇÃO **2025**

ACESSE O CÓDIGO DE INTEGRIDADE DO AGENTE PÚBLICO MUNICIPAL

Controladoria Geral do Município ● Assessoria de Inovação e Tecnologia ● Coordenadoria Técnica de Controles Internos ● Comitê de Proteção de Dados Pessoais

Rua Afonso Cavalcanti 455, 14º andar

Anexo único à Resolução CGM-RIO nº 2.099/2025

V.1 - FECHAMENTO DESTA EDIÇÃO: 05/11/2025

Fotografia Capa: Riotur ● Disponível em https://www.flickr.com/photos/riotur/

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança da Informação (PSI) da Controladoria Geral do Município do Rio de Janeiro (CGM-Rio), com a finalidade de estabelecer princípios, diretrizes, responsabilidades e controles para assegurar a proteção das informações e dos dados pessoais sob custódia desta Controladoria.

§ 1º Estão sujeitos às regras desta Política todos os agentes públicos, colaboradores, prestadores de serviço, visitantes e quaisquer pessoas que tenham acesso a instalações ou ambientes computacionais e a ativos de informação pertencentes ou sob custódia da CGM-Rio, devendo:

I - observar as regras de segurança previstas nesta Resolução;

II - zelar pela confidencialidade, integridade e disponibilidade dos dados acessados;

III - aplicar essas regras em todos os sistemas de informação, aplicativos, dispositivos, redes, processos corporativos e relacionamentos institucionais da CGM-Rio.

§ 2º Fica a Assessoria de Comunicação Social da CGM-Rio responsável pela ampla divulgação desta política, devendo manter ininterruptamente ao alcance de todos, cópia da política em meio digital de fácil acesso através de QR Code afixado nos murais de comunicação interna ou outra tecnologia de maior alcance.

Art. 2º Para fins desta Política, considera-se:

I - *access point*: equipamento que possibilita a interconexão de clientes de uma rede sem fio com uma rede cabeada por meio de ondas de rádio;

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

III - 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.);

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 - autenticidade: propriedade que garante que uma informação, comunicação ou transação é genuína, confirmando a identidade de quem a criou, enviou ou executou. Visa assegurar que os dados são provenientes de uma fonte legítima e não foram falsificados;

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

VII - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em

vários locais, em suporte eletrônico ou físico;

VIII - caixa postal: área de armazenamento de mensagens recebidas, enviadas ou em elaboração, associada a uma conta de correio eletrônico individual ou institucional;

IX - cavalo de troia: programa malicioso disfarçado de software legítimo, criado para induzir o usuário a instalá-lo voluntariamente. Uma vez executado, permite o acesso não autorizado ao sistema, podendo roubar informações, alterar configurações ou instalar outros tipos de malware;

X - 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*);

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

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

XIII - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

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

XV - 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;

XVI - 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);

XVII - custodiante da informação: servidor ou unidade responsável por armazenar, manter e assegurar a integridade, disponibilidade e confidencialidade das informações sob sua guarda, conforme as diretrizes estabelecidas pelo responsável pela informação;

XVIII - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

XIX - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

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

XXI - *download*: transferência de arquivo(s) residente(s) em *sites* da Internet para equipamentos pertencentes à rede corporativa da Administração Pública Municipal;

XXII - encarregado de dados: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados – ANPD;

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

XXIV - gestor da informação: servidor responsável por zelar pela correta classificação, tratamento e guarda das informações sob responsabilidade de seu setor, assegurando a observância das normas institucionais de segurança da informação e de proteção de dados;

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

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

XXVII - *peer-to-peer* (P2P): tipo de rede de comunicação onde os participantes compartilham os recursos de seus computadores para troca de arquivos entre si;

XXVIII - *phishing*: técnica de fraude digital que visa enganar o usuário para obter informações confidenciais, como senhas, dados pessoais ou bancários, por meio de mensagens falsas, geralmente enviadas por e-mail, aplicativos ou sites que imitam comunicações legítimas;

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

XXX - *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;

XXXI - 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;

XXXII - redes sem fio: redes de comunicação de dados que fazem uso de ondas de rádio para estabelecer os enlaces de comunicação entre seus componentes;

XXXIII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XXXIV - responsável pela informação: autoridade ou servidor designado formalmente para supervisionar o ciclo de vida da informação em seu âmbito de atuação, definindo níveis de acesso, classificações e medidas de proteção adequadas, conforme as normas institucionais;

XXXV - 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;

XXXVI - *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.);

XXXVII - *switches*: dispositivos de rede responsáveis por interligar vários equipamentos dentro de uma mesma rede local (LAN), encaminhando os dados apenas aos destinos corretos;

XXXVIII - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

XXXIX - tratamento de dados pessoais: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

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

XLI - usuário: qualquer pessoa autorizada a usar um ativo tecnológico;

XLII - usuário da informação: pessoa que utiliza informações ou sistemas de informação para a execução de suas atividades laborais, devendo observar as normas e controles estabelecidos pela organização para garantir o uso adequado e seguro dos recursos tecnológicos;

XLIII - 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; e

XLIV - *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. 3º São objetivos da Política de Segurança da Informação da CGM-Rio:

I - definir princípios e diretrizes para a proteção dos ativos de informação e dos ativos tecnológicos da CGM-Rio;

II - orientar as práticas de segurança da informação, contribuindo para a gestão de riscos e assegurando a confidencialidade, a integridade e a disponibilidade das informações;

III - estabelecer competências e responsabilidades relacionadas à segurança da informação;

IV - direcionar a elaboração de normas e procedimentos relacionados à segurança da informação; e

V - alinhar as ações de segurança da informação ao planejamento estratégico da CGM-Rio.

Art. 4º A segurança da informação na CGM-Rio tem como princípios e diretrizes:

I - proteger a imagem da Prefeitura da Cidade do Rio de Janeiro (PCRJ);

II - assegurar a integridade, a autenticidade e disponibilidade das informações produzidas ou recebidas;

III - promover a transparência no acesso às informações de caráter público;

IV - respeitar o direito de acesso à informação, a proteção dos dados pessoais e a preservação da privacidade;

V - planejar ações de segurança da informação com base na gestão de riscos;

VI - adaptar-se a mudanças tecnológicas e institucionais, aproveitando oportunidades de inovações;

VII - integrar a segurança da informação ao ciclo de vida dos dados, aos processos institucionais e à cultura organizacional da CGM-Rio;

VIII - observar a publicidade como regra geral e o sigilo como exceção;

IX - atribuir ao usuário a responsabilidade pelos atos que comprometam a segurança dos ativos de informação; e

X - zelar pela conformidade legal e normativa dos procedimentos relativos à segurança da informação, principalmente no que se refere à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD) e à Agenda Regulatória da ANPD.

Parágrafo único. A segurança da informação na CGM-Rio deverá contemplar dimensões físicas, tecnológicas, organizacionais e humanas, de modo a manter-se alinhada às diretrizes da ABNT NBR ISO/IEC 27001:2022.

Art. 5º Toda informação produzida, armazenada, processada ou utilizada pela CGM-Rio integra seus ativos de informação e deve ser protegida conforme as normas vigentes.

Parágrafo único. O uso dos ativos de informação está sujeito a monitoramento e auditoria, devendo ser adotados mecanismos que assegurem a rastreabilidade, o controle e a verificação dos acessos aos sistemas corporativos e à rede interna.

Art. 6º A gestão de riscos de segurança da informação deve ocorrer de forma permanente e estruturada, abrangendo todos os ativos de informação da CGM-Rio, com objetivo de identificar e tratar riscos que possam comprometer a confidencialidade, a integridade, ou a disponibilidade das informações, seguindo as diretrizes previstas na Política de Gerenciamento de Riscos da CGM-Rio, instituída pela Resolução CGM-Rio nº 1.794, de 08 de fevereiro de 2022.

Parágrafo único. A gestão de riscos deverá seguir metodologias qualitativas e quantitativas e deverá incluir análises periódicas e planos de tratamento de riscos, integrados a relatórios de impacto à proteção de dados.

Art. 7º A segurança da informação em recursos humanos tem por finalidade assegurar que as pessoas com vínculo estatutário, funcional, contratual ou processual com a CGM-Rio

compreendam seus direitos, suas responsabilidades e ajam em conformidade com esta Política, prevenindo riscos de furto, fraude ou uso indevido de informações.

Art. 8º A conscientização em segurança da informação visa incorporar conceitos e boas práticas à cultura da CGM-Rio, por meio de ações contínuas de divulgação, capacitação e educação.

§ 1º Todos os usuários devem receber capacitação periódica sobre os procedimentos de segurança e o uso adequado dos ativos de informação no desempenho de suas atribuições.

§ 2º A capacitação poderá incluir e-learning, workshops e simulações de phishing, acompanhados de avaliações de efetividade voltadas à melhoria contínua das ações de conscientização.

Art. 9º A proteção de dados pessoais tem por finalidade resguardar os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. A proteção de dados pessoais observará medidas necessárias e proporcionais ao interesse público, garantindo o devido processo legal, os princípios gerais de proteção e os direitos dos titulares.

Art. 10. A gestão de incidentes em segurança da informação tem por objetivo assegurar que vulnerabilidades e incidentes sejam prontamente identificados, tratados e comunicados, permitindo a adoção de medidas corretivas e a melhoria contínua de controles e processos.

CAPÍTULO II
DAS RESPONSABILIDADES E VEDAÇÕES

Art. 11. Compete aos usuários de informação conhecer, cumprir e zelar pelo cumprimento desta PSI.

Parágrafo único. Cada usuário de informação é responsável pela proteção e pelo uso adequado dos ativos de informação que estejam sob sua guarda ou responsabilidade.

Art. 12. Compete aos responsáveis por informações produzidas ou custodiadas pela CGM-Rio:

I - garantir a proteção das informações sob sua responsabilidade;

II - classificar as informações e estabelecer procedimentos e critérios de acesso, em conformidade com a legislação e normativos aplicáveis à confidencialidade e demais critérios pertinentes;

III - propor regras específicas para o uso das informações; e

IV - definir os requisitos de segurança da informação necessários ao negócio, com base na aceitação e no tratamento dos riscos associados aos processos de trabalho.

Art. 13. São deveres do custodiante da informação:

I - zelar pela segurança das informações sob sua guarda, em conformidade com os critérios definidos pelo respectivo responsável;

II - comunicar tempestivamente ao responsável pela informação quaisquer eventos que comprometam sua segurança; e

III - informar ao responsável pela informação eventuais limitações que impeçam o cumprimento integral dos critérios estabelecidos para sua proteção.

Art. 14. São responsabilidades dos dirigentes e gestores da CGM-Rio:

I - promover a conscientização de servidores e colaboradores sob sua supervisão quanto aos conceitos e práticas de segurança da informação;

II - integrar aos processos de trabalho da unidade ou área as práticas relacionadas à segurança da informação; e

III - adotar as medidas administrativas necessárias para assegurar a implementação de ações corretivas em tempo adequado diante de eventuais vulnerabilidades à segurança da informação.

Art. 15. Compete ao Encarregado de Dados da CGM-Rio, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na LGPD e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.

Art. 16. Dirigentes, gestores, servidores, colaboradores da CGM-Rio e quaisquer pessoas que tenham acesso a dados pessoais custodiados ou tratados pela CGM-Rio devem:

I - comunicar imediatamente ao Encarregado de Dados quaisquer incidentes ou suspeitas de incidentes em segurança da informação de que tenham conhecimento; e

II - cooperar, dentro de sua área de competência, na identificação e no tratamento de incidentes em segurança da informação.

Art. 17. As unidades organizacionais da CGM-Rio devem realizar ações de capacitação e conscientização para que seus colaboradores compreendam suas responsabilidades e adotem os procedimentos relacionados à segurança da informação e à proteção de dados.

Art. 18. É vedado aos usuários de recursos de tecnologia da informação da CGM-Rio:
I - acessar, armazenar ou divulgar conteúdos incompatíveis com o ambiente de trabalho, que violem direitos autorais ou infrinjam a legislação vigente;

II - utilizar ou instalar recursos de tecnologia da informação não homologados ou não adquiridos pela CGM-Rio;

III - compartilhar com terceiros credenciais pessoais e intransferíveis de identificação,

autenticação ou autorização, tais como contas, senhas ou certificados digitais; e

IV - explorar vulnerabilidades, as quais devem ser imediatamente comunicadas às instâncias competentes quando identificadas.

Art. 19. É vedado aos servidores públicos, prestadores de serviço e quaisquer outros colaboradores que atuem no âmbito da CGM-Rio armazenar, sem a devida proteção, dados pessoais de terceiros em computadores locais, dispositivos removíveis, mídias portáteis ou similares ou quaisquer dispositivos eletrônicos de uso individual ou compartilhado.

CAPÍTULO III
DO CONTROLE DE ACESSO

Art. 20. 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. 21. 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; e

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

Art. 22. Compete ao usuário de ativo tecnológico:

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.

Art. 23. O processo de gestão de contas e credenciais de acesso aos ativos tecnológicos,

definido pelo Decreto Rio nº 56.649, de 25 de agosto de 2025, encontra-se regulamentado pela Portaria "N" CGM-Rio nº 001, de 08 de fevereiro de 2023, e pela Resolução CGM-Rio "N" nº 2093, de 8 de outubro de 2025.

§ 1º O processo deve contemplar procedimentos para todas as etapas do ciclo de vida:

I - credenciamento de usuários;

II - criação de conta;

III - criação e emissão de credenciais;

IV - utilização de conta e credencial;

V - manutenção de acesso; e

VI - encerramento da conta.

§ 2º O processo de concessão de perfis de acesso deve contemplar somente os privilégios imprescindíveis à execução das competências e responsabilidades de seus usuários.

Art. 24. A CGM-Rio 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 IV
DA CRIAÇÃO E MANUTENÇÃO DE SENHAS DE ACESSO

Art. 25. As senhas devem conter tamanho mínimo de 10 (dez) posições, além dos seguintes tipos de caracteres: letras minúsculas, letras maiúsculas, números e caracteres especiais.

Art. 26. Quanto à criação e atualização de senhas:

I - o usuário pode alterar sua senha a qualquer tempo;

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

III - deve-se evitar a utilização de informações pessoais na criação da senha de acesso; e

IV - é vedada a reutilização de senhas expiradas.

Art. 27. Quanto à proteção e ao uso das senhas:

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-it, 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); e

IX - 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*).

CAPÍTULO V
DO USO DA INTERNET

Art. 28. O uso do serviço de Internet corporativo deve ser realizado, majoritariamente, para suporte às atividades de trabalho, sendo vedada toda e qualquer utilização de serviços disponibilizados pela Internet cujas características de consumo de recursos possam comprometer a eficiência ou a disponibilidade dos demais serviços disponíveis na rede corporativa.

Art. 29. São vedados quaisquer tipos de uso do serviço de Internet corporativo que possam acarretar riscos operacionais ou legais à Administração Pública Municipal, assim como aos seus agentes públicos, por exemplo:

I - acessos a portais ou páginas de conteúdo pornográfico, de apologia à violência ou pedofilia, erótico, racista, neonazista, antissemita, ilegal ou qualquer outro que venha a incitar a discriminação ou atentar contra a integridade moral de terceiros ou de quaisquer grupos da sociedade;

II - acessos a sites de orientações para invasão de segurança, de suporte à pirataria, de propaganda ilegal ou quaisquer outros que possam conter códigos maliciosos;

III - tentativas de ataques ou invasões a computadores internos ou externos à rede corporativa;

IV - realização de mineração de criptomoedas;

V - realização de qualquer tipo de fraude ou atividade de pirataria, como cópia, uso e distribuição de material ou *software* protegido por leis de direito autoral;

VI - realização de atividades político-partidárias, pregação religiosa, ou de natureza similar;

VII - propagação intencional de códigos maliciosos;

VIII - acesso a páginas de jogos on-line, sites de relacionamento e fóruns não profissionais;

IX - uso de navegadores ou aplicativos com tecnologia *peer to peer*;

X - realização de *downloads* ou *uploads* de conteúdos não alinhados aos interesses da Administração Pública Municipal;

XI - transmissão de qualquer informação corporativa sem os controles e os níveis de autorização adequados à sua classificação;

XII - realização de *downloads* de *softwares* comerciais ou qualquer material proprietário, a menos que esta operação já esteja prevista e permitida por contrato comercial ou outra forma legal de licenciamento;

XIII - uso de programas de envio de mensagens em massa ou mala direta não previstos institucionalmente;

XIV - envio, distribuição ou armazenamento na Internet de informações não públicas de propriedade da Administração Pública Municipal, a não ser que expressamente autorizados pelo gestor da informação; e

XV - uso de ferramentas de monitoração do conteúdo transmitido e programas para obtenção de senhas.

Art. 30. O usuário deverá certificar-se da procedência do sítio, verificando, quando cabível, seu certificado digital, principalmente para realizar transações eletrônicas sensíveis via internet, digitando o endereço do sítio diretamente no navegador da estação de trabalho, evitando clicar em *links* existentes em páginas Web ou em mensagens de correio eletrônico e quando verificar que o site acessado contém conteúdo impróprio, o usuário deve abandonar o site imediatamente e abrir um incidente de Segurança da Informação.

CAPÍTULO VI
DO USO DO CORREIO ELETRÔNICO

Art. 31. Todas as comunicações de cunho institucional realizadas por e-mail devem valer-se do serviço de Correio Eletrônico Corporativo, ficando proibida utilização de e-mails pessoais para tratar de dados e assuntos corporativos pertinentes à PCRJ.

Art. 32. A utilização do serviço de Correio Eletrônico Corporativo deve estar alinhada aos interesses da Administração Pública Municipal e ocorrer dentro de um comportamento ético e legal.

Art. 33. O serviço de Correio Eletrônico Corporativo é uma concessão da Administração Pública do Poder Executivo Municipal, sendo assim, seu uso é permitido somente para as atividades profissionais de seus usuários, não sendo permitido enviar ou arquivar mensagens não relacionadas às atividades profissionais ou de cunho estritamente pessoal.

Art. 34. O usuário é responsável por quaisquer ações realizadas por meio de sua conta.

Art. 35. O envio de mensagem eletrônica para múltiplos destinatários (lista de distribuição de alto volume de mensagens) deve estar amparado pelas competências ou responsabilidades do remetente.

Parágrafo único. Os casos de necessidade eventual devem ser formalmente justificados e autorizados junto aos agentes competentes.

Art. 36. Dados pessoais, recebidos por e-mail ou por qualquer outro canal de comunicação, sobre os quais a CGM-Rio não detenha competência ou finalidade legítima de tratamento devem ser imediatamente descartados.

Parágrafo único. O destinatário dos dados pessoais a que se refere o caput deste artigo deve:

I - comunicar ao remetente a ausência de competência legal ou de fundamento legítimo para o tratamento dos dados pela CGM-Rio ou pelo respectivo setor;

II - informar ao remetente que os dados foram descartados em conformidade com esta Política; e

III - adotar todas as medidas necessárias para impedir o acesso, a divulgação ou o tratamento indevido de tais dados no âmbito da CGM-Rio.

Art. 37. Compete ao usuário, segundo estabelece o Decreto Rio nº 56.643 de 25 de agosto de 2025:

I - cumprir com as diretrizes e orientações das normas de segurança da informação da PCRJ, assim como apoiar o desenvolvimento e identificação de novas necessidades;

II - manter-se atualizado quanto às normas e procedimentos relativos à utilização do serviço de Correio Eletrônico Corporativo, assim como quanto às melhores práticas de uso seguro.

III - atentar para os riscos de segurança relacionados às informações constantes de suas mensagens, promovendo o tratamento destes riscos;

IV - manter em sigilo sua senha de acesso ao correio eletrônico, de uso pessoal e intransferível, providenciando sua substituição em caso de suspeita de violação;

V - fechar a página de acesso do e-mail institucional ou bloquear sua estação de trabalho toda vez que se ausentar, evitando o acesso indevido;

VI - informar à IplanRio sobre comportamentos anômalos do serviço de correio eletrônico;

VII - comunicar à IplanRio o recebimento de mensagens que possam portar vírus, ou qualquer tipo de conteúdo inadequado ou suspeito; e

VIII - efetuar a limpeza de sua Caixa Postal, evitando ultrapassar o limite de armazenamento e garantindo o seu funcionamento contínuo.

Art. 38. O usuário deve estar ciente dos requisitos de uso, das práticas de uso indevido do serviço de Correio Eletrônico Corporativo, bem como dos conteúdos de mensagens considerados indevidos e de suas competências, estabelecidos no Decreto Rio nº 56.643 de 25 de agosto de 2025, estando sujeito à responsabilização decorrente do mau uso do serviço e às sanções administrativas cabíveis, conforme legislação em vigor.

CAPÍTULO VII
DA SEGURANÇA EM REDES SEM FIO

Art. 39. É vedada a conexão de equipamentos pessoais à rede sem fio corporativa.

Art. 40. É vedada a instalação de equipamentos de rede, tais como roteadores, *switches* e *access points*, sem a coordenação e o acompanhamento de agentes da área responsável pela administração da rede, os quais devem observar diretrizes e requisitos de segurança estabelecidos no Decreto Rio nº 56.645 de 25 de agosto de 2025.

CAPÍTULO VIII
DA PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

Art. 41. 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 - é vedada ao usuário de equipamento de TIC corporativo a desinstalação, desativação ou alteração de configuração de sua solução de proteção contra códigos maliciosos;

III - 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;

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

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

Art. 42. 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; e

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

Art. 43. 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; e

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

Art. 44. 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 IX
DA CÓPIA DE SEGURANÇA (*BACKUP*) E RECUPERAÇÃO DE DADOS (*RESTORE*)

Art. 45. Compete aos usuários manter todas as informações corporativas armazenadas na rede corporativa ou nas plataformas de nuvem corporativa sob a titularidade da conta de e-mail institucional do setor ao qual pertencem.

Parágrafo único. Os arquivos armazenados nas estações de trabalho não integrarão o escopo do processo de *backup* e, portanto, não estarão disponíveis para recuperação.

Art. 46. As informações sensíveis quanto à confidencialidade devem ser armazenadas de forma criptografada, utilizando ferramentas institucionais conforme padrão estabelecido ou aprovado pela Iplanrio.

CAPÍTULO X
DOS INCIDENTES DE SEGURANÇA DE DADOS PESSOAIS

Art. 47. O incidente de segurança pode acarretar risco ou dano relevante aos titulares quando puder afetar significativamente interesses e direitos fundamentais dos titulares desses dados e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

I - dados pessoais sensíveis;

II - dados de crianças, de adolescentes ou de idosos;

III - dados financeiros;

IV - dados de autenticação em sistemas;

V - dados protegidos por sigilo legal, judicial ou profissional; ou

VI - dados em larga escala.

Parágrafo único. O incidente de segurança que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

Art. 48. Constatado indício de incidente de segurança de dados pessoais, caberá ao Encarregado de Dados da CGM-Rio instaurar procedimento sumário de apuração preliminar, com o objetivo de verificar a ocorrência, a natureza e a extensão do evento noticiado.

§ 1º A apuração preliminar deverá compreender, no mínimo, a coleta das evidências disponíveis, o registro das informações obtidas e a avaliação inicial do risco potencial aos titulares.

§ 2º Confirmada a ocorrência de incidente de segurança, o Encarregado deverá comunicar imediatamente o fato ao Controlador-Geral e ao Comitê de Proteção de Dados Pessoais.

§ 3º Caso não sejam confirmados elementos que caracterizem incidente de segurança, o processo de apuração será encerrado, com registro das conclusões e justificativas pertinentes.

Art. 49. Confirmado o incidente de segurança de dados pessoais, o Encarregados de Dados da CGM-Rio dará início ao processo de resposta a incidente de segurança de dados pessoais, devendo convocar imediatamente o Comitê de Proteção de Dados Pessoais para:

I - identificar a natureza e a categoria de dados pessoais afetados;

II - mensurar o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;

III - designar, entre os membros do Comitê, as responsabilidades e funções específicas na condução da análise e do tratamento do incidente;

IV - analisar as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente;

V - avaliar os riscos relacionados ao incidente, identificando os possíveis impactos aos titulares;

VI - determinar a causa principal do incidente, caso seja possível identificá-la;

VII - definir as medidas corretivas a serem imediatamente adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;

VIII - estabelecer as medidas preventivas necessárias para salvaguardar direitos dos titulares, a fim de prevenir, mitigar ou reverter os efeitos do incidente e evitar a ocorrência de dano grave e irreparável ou de difícil reparação;

IX - levantar o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente; e

X - registrar, no relatório de tratamento de incidentes, todas as análises, deliberações e providências adotadas.

§ 1º Na determinação das medidas para reverter ou mitigar os efeitos do incidente, serão consideradas aquelas que possam garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade dos dados pessoais afetados, bem como minimizar os efeitos decorrentes do incidente para os titulares.

§ 2º Se o Encarregado de Dados julgar necessário, poderá consultar a Assessoria de Inovação e Tecnologia para emissão de parecer técnico ou opinativo que subsidie a adoção das medidas cabíveis.

§ 3º O registro no relatório de tratamento de incidentes deverá conter, no mínimo:

I - a data de conhecimento do incidente;

II - a descrição geral das circunstâncias em que o incidente ocorreu;

III - a natureza e a categoria de dados afetados;

IV - o número de titulares afetados;

V - a avaliação do risco e os possíveis danos aos titulares;

VI - as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;

VII - a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e

VIII - os motivos da ausência de comunicação, quando for o caso.

§ 4º O Encarregado deverá comunicar o fato ao Encarregado de dados geral da Prefeitura a

fim de que definam a necessidade e a estratégia de comunicação à Agência Nacional de Proteção de Dados em até 03 (três) dias úteis.

§ 5º Deve o Encarregado de dados manter cadastro ativo e atualizado junto ao SEI.ANPD, a fim de possibilitar a comunicação junto àquele órgão dentro do prazo previsto na legislação, através do endereço eletrônico disponibilizado no portal da agência na internet.

Art. 50. A CGM-Rio, por meio de seu Encarregado de Dados, deverá comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Art. 51. O Encarregado de Dados da CGM-Rio, antes de realizar qualquer comunicação com a ANPD, deve imediatamente solicitar orientações ao Encarregado de Dados Geral da PCRJ, reportando-se, previamente, ao Controlador de Dados e ao Comitê de Proteção de Dados Pessoais.

Art. 52. A comunicação de incidente de segurança à ANPD deverá ser realizada pelo Encarregado de Dados da CGM-Rio no prazo máximo de 3 (três) dias úteis, ressalvada a existência de prazo para comunicação previsto em legislação específica.

Parágrafo único. O prazo a que se refere o caput será contado do conhecimento pelo controlador de que o incidente afetou dados pessoais.

Art. 53. A comunicação de incidente de segurança aos titulares dos dados deverá ser realizada pelo Encarregado de Dados da CGM-Rio no prazo de 3 (três) dias úteis contados do conhecimento pelo controlador de que o incidente afetou dados pessoais.

§ 1º A comunicação do incidente aos titulares de dados deverá atender aos seguintes critérios:

I - fazer uso de linguagem simples e de fácil entendimento; e

II - ocorrer de forma direta e individualizada, caso seja possível identificá-los.

§ 2º Caso a comunicação direta e individualizada mostre-se inviável ou não seja possível identificar, parcial ou integralmente, os titulares afetados, a CGM-Rio deverá comunicar a ocorrência do incidente, no mesmo prazo, por meio de seu sítio eletrônico, de suas mídias sociais e de quaisquer outros meios de divulgação disponíveis, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, 3 (três) meses.

Art. 54. O processo de resposta a incidente de segurança de dados pessoais será declarado extinto nas seguintes hipóteses:

I - caso não sejam identificadas evidências suficientes da ocorrência do incidente, ressalvada a possibilidade de reabertura caso surjam fatos novos;

II - caso a ANPD considere que o incidente não possui potencial para acarretar risco ou dano relevante aos titulares, nos termos do art. 46 desta Política;

III - caso o incidente não envolva dados pessoais;

IV - caso tenham sido tomadas todas as medidas adicionais para mitigação ou reversão dos efeitos gerados; ou

V - realização da comunicação aos titulares e adoção das providências pertinentes pelo controlador, em conformidade com a LGPD e as determinações da ANPD.

CAPÍTULO XI
DA SEGURANÇA REMOTA E DISPOSITIVOS PESSOAIS (BYOD)

Art. 55. Quando da necessidade de realização de trabalhos fora do ambiente físico da CGM-Rio, devem ser observadas medidas adicionais de segurança, incluindo VPN para acessos remotos, autenticação multifator e políticas de atualização de software.

Art. 56. É vedada a utilização de dispositivos pessoais (BYOD - Bring Your Own Device) nas dependências da CGM-Rio para a execução de atividades laborais ou conexão à rede corporativa.

CAPÍTULO XII
DAS DISPOSIÇÕES FINAIS

Art. 57. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pela CGM-Rio devem observar, no que couber, as disposições da PSI da CGM-Rio.

Art. 58. A PSI, quando necessário, deve ser complementada por normas, metodologias e procedimentos.

Art. 59. A utilização dos recursos de tecnologia de informação da CGM-Rio pode ser monitorada, avaliada e auditada com vistas a identificar inobservâncias à PSI e a fornecer evidências, no caso de incidentes de segurança da informação, respeitados os direitos e as garantias individuais previstos em lei.

Art. 60. A revisão da PSI da CGM-Rio poderá ocorrer a qualquer tempo, quando houver mudanças significativas com impacto nos processos ou requisitos de segurança da informação, devendo ser realizada no máximo a cada quatro anos, de modo a atualizá-la frente a novos requisitos.

Art. 61. A não observância dos dispositivos da PSI sujeita os infratores, isolada ou cumulativamente, a sanções administrativas, civis e penais, nos termos da legislação pertinente, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 62. Esta Política entra em vigor na data de sua publicação.