Governo do Estado do Rio de Janeiro

Secretaria de Estado de Defesa do Consumidor

RESOLUÇÃO SEDCON Nº74 DE 18 DE NOVEMBRO DE 2025

INSTITUI A POLÍTICA DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD NO ÂMBITO DA SECRETARIA DE ESTADO DE DEFESA DO CONSUMIDOR – SEDCON

O SECRETÁRIO DE ESTADO DE DEFESA DO CONSUMIDOR, no uso das atribuições legais que lhes são conferidas pela legislação em vigor, tendo em vista o disposto no Processo nº SEI- 240001/000913/2025,

RESOLVE:

CAPÍTULO I – ESCOPO

Art. 1º – Fica instituído, no âmbito da Secretaria de Estado de Defesa do Consumidor – SEDCON, a Política de Adequação à Lei Geral de Proteção de Dados Pessoais – LGPD, com fundamento na Lei Federal nº 13.709, de 14 de agosto de 2018, no Decreto Estadual nº 48.891, de 10 de janeiro de 2024, e na Resolução SEDCON nº 50, de 09 de maio de 2025.

Art. 2º – Esta política tem por finalidade estabelecer diretrizes, responsabilidades e mecanismos técnicos e administrativos destinados a assegurar a conformidade da SEDCON com as normas de proteção de dados pessoais, promovendo uma cultura institucional de respeito à privacidade, à segurança da informação e à transparência no tratamento de dados.

§ 1º – Para os fins desta política, considera-se “tratamento de dados pessoais” toda e qualquer operação realizada com dados, incluindo, mas não se limitando a: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, transferência, difusão ou extração.

§ 2º – Esta política abrange dados e informações institucionais, pessoais e sensíveis relacionados a cidadãos, servidores, fornecedores, prestadores de serviço e demais partes envolvidas em processos e contratos administrativos, estabelecendo deveres, obrigações e penalidades relativas à segurança e à privacidade da informação no âmbito da SEDCON.

Seção I – Dos Princípios

Art. 3º – As diretrizes estabelecidas nesta política aplicam-se ao tratamento de dados e

informações, conforme definido no § 1º do art. 2º, observando-se os seguintes princípios:

I – confidencialidade: garantia de que o acesso aos dados será restrito às pessoas devidamente autorizadas;

II – integridade: preservação da exatidão, consistência e confiabilidade das informações ao longo de seu ciclo de vida;

III – disponibilidade: garantia de acesso contínuo e seguro aos dados sempre que necessário;

IV – autenticidade: asseguramento da veracidade dos dados e da rastreabilidade das operações de tratamento;

V – legalidade: conformidade com as disposições legais e normativas aplicáveis ao tratamento de dados pessoais;

VI – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e previamente informados ao titular;

VII – necessidade: limitação do tratamento ao mínimo necessário para a realização das finalidades pretendidas.

Seção II – Da Abrangência

Art. 4º – As disposições desta política aplicam-se a todos que atuem, direta ou indiretamente, no âmbito da SEDCON ou em seu nome, independentemente do vínculo jurídico mantido.

Parágrafo único. Para os fins desta política, todos os servidores públicos (estatutários, comissionados), estagiários, prestadores de serviços, fornecedores e demais colaboradores serão denominados, em conjunto, como “colaboradores”, expressão que será utilizada nos demais dispositivos deste instrumento.

Art. 5º – Para os fins desta norma, adotam-se as seguintes definições:

I – Acesso básico: nível de acesso que permite o uso de ativos de informação comuns a todos os colaboradores, sob gestão da Assessoria de Tecnologia de Informação;

II – Ameaça: condição ou agente, interno ou externo, com potencial de comprometer a confidencialidade, integridade ou disponibilidade de um ativo da informação por meio da exploração de vulnerabilidades;

III – Ameaça cibernética: ação intencional, realizada em ambiente digital, por agentes maliciosos ou programas automatizados, com o objetivo de causar danos, interrupções ou acessos indevidos a sistemas, redes ou dados;

IV – Ativo de informação: qualquer meio, tecnológico ou não, utilizado para criar, transmitir, processar, armazenar, recuperar ou descartar informações com valor para a SEDCON;

V – Ativo tecnológico: componente físico (ex: dispositivos tecnológicos) ou lógico (ex: softwares), pertencente à infraestrutura de Tecnologia de Informação da SEDCON ou homologado para atividades institucionais, inclusive dispositivos pessoais autorizados;

VI – Cliente: cidadão que utiliza os serviços públicos prestados pela SEDCON;

VII – Dado pessoal: informação relacionada à pessoa natural identificada ou identificável, nos termos da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

VIII – Evento de privacidade da informação: ocorrência relacionada à segurança da informação envolvendo dados pessoais, incluindo falhas, violações ou incidentes com potencial de comprometer a privacidade;

IX – Evento de segurança da informação: ocorrência que represente violação, tentativa ou suspeita de violação das diretrizes desta norma ou de seus documentos complementares, afetando a

confidencialidade, integridade ou disponibilidade de ativos;

X – Fornecedor: pessoa física ou jurídica, de direito público ou privado, que forneça bens ou serviços à SEDCON;

XI – Incidente de privacidade da informação: evento que envolva dados pessoais e possa acarretar risco ou dano relevante aos respectivos titulares;

XII – Incidente de segurança da informação: ação que comprometa a confidencialidade, integridade ou disponibilidade dos ativos de informação;

XIII – Informação sensível: informação com grau de sigilo, que deve ser protegida contra acesso ou divulgação não autorizados, incluindo, mas não se limitando a dados pessoais sensíveis nos termos da LGPD;

XIV – Inteligência de ameaças: processo de coleta, correlação e análise de informações sobre ameaças cibernéticas, visando antecipar tendências e aprimorar os mecanismos de resposta;

XV – Login: identificação do usuário em sistema computacional, realizada mediante credencial de acesso, como nome de usuário e senha;

XVI – Oportunidade de privacidade da informação: circunstância favorável que possa ser aproveitada para aprimorar a proteção de dados pessoais;

XVII – Oportunidade de segurança da informação: condição favorável, resultante da interação entre fatores internos e externos, que contribui para o fortalecimento da segurança institucional;

XVIII – Processo: sequência de atividades estruturadas que transforma entradas (insumos) em saídas (produtos ou serviços) com valor agregado;

XIX – Registro de auditoria: log textual, cronológico e detalhado de ações executadas em sistemas computacionais, permitindo rastreabilidade e identificação de autoria, tempo e natureza da ação;

XX – Risco de privacidade da informação: possibilidade de ocorrência de eventos que comprometam a proteção de dados pessoais;

XXI – Risco de segurança da informação: possibilidade de que uma ameaça, ao explorar vulnerabilidades, comprometa a confidencialidade, integridade ou disponibilidade de ativos da informação;

XXII – Usuário: agente humano ou de software que interage com os ativos tecnológicos da SEDCON;

XXIII – Vulnerabilidade técnica: fragilidade em ativo tecnológico que pode ser explorada por ameaças para comprometer a segurança da informação.

CAPÍTULO II – PAPÉIS E RESPONSABILIDADES

Art. 6º – Compete a cada servidor, estagiário e trabalhador terceirizado:

I – responder por prejuízos ou danos decorrentes do descumprimento das diretrizes estabelecidas nesta política;

II – responsabilizar-se por quaisquer acessos realizados com seu login, considerando-se que se trata de credencial pessoal, única e intransferível;

III – participar dos treinamentos e capacitações sobre segurança e privacidade da informação fornecidos pela SEDCON;

IV – notificar, de forma imediata, eventos e incidentes relacionados à segurança e à privacidade da informação.

Art. 7º – Compete a cada gestor, ou o servidor formalmente por ele delegado:

I – monitorar o cumprimento desta política pelos colaboradores sob sua supervisão;

II – definir e gerenciar perfis, direitos e níveis de acesso aos sistemas e softwares sob sua

responsabilidade;

III – revisar periodicamente os acessos concedidos;

IV – segregar funções que apresentem conflito de interesses nos processos sob sua responsabilidade;

V – identificar e notificar continuamente os riscos de segurança e privacidade da informação associados aos ativos sob sua supervisão;

VI – disponibilizar, após o ingresso dos colaboradores:

a) esta política;

b) orientações básicas sobre segurança e privacidade da informação;

c) Termo de Responsabilidade de Segurança da Informação, para assinatura;

VII – solicitar, quando necessário, o acesso básico aos ativos e dispositivos tecnológicos para trabalhadores terceirizados sob sua supervisão.

Art. 8º – Compete à Coordenadoria de Recursos Humanos:

I – selecionar novos servidores mediante verificação de antecedentes, conforme leis, regulamentos e princípios éticos, proporcionalmente aos riscos inerentes ao cargo;

II – solicitar, para novos servidores e estagiários:

a) os dispositivos tecnológicos e acessos básicos necessários;

b) os acessos físicos correspondentes (no caso dos servidores);

III – elaborar Termo de Compromisso de Estágio padronizado, contendo cláusula específica de responsabilidade quanto à segurança e à privacidade da informação;

IV – elaborar instrumentos padronizados de responsabilização, incluindo:

a) Termo de Responsabilidade de Segurança da Informação, para servidores;

b) contrato ou instrumento equivalente para fornecedores e demais partes envolvidas.

Art. 9º – Compete à Assessoria de Tecnologia da Informação:

I – restringir, ao mínimo necessário, os privilégios administrativos e a quantidade de administradores com permissão para excluir registros de auditoria;

II – definir e gerenciar perfis, direitos e níveis de acesso nos sistemas sob sua responsabilidade;

III – revisar periodicamente os acessos concedidos;

IV – homologar os dispositivos tecnológicos e softwares autorizados para uso institucional;

V – prover, de forma contínua, os controles técnicos necessários à conformidade com esta política;

VI – monitorar o ambiente tecnológico por meio de ferramentas que acompanhem a disponibilidade, desempenho e capacidade dos ativos críticos;

VII – executar plano anual de conscientização e capacitação sobre segurança e privacidade da informação, incluindo treinamentos específicos para as equipes técnicas.

Art. 10 – Compete à Superintendência de Administração e Finanças:

I – identificar e monitorar ameaças cibernéticas, mediante aplicação de inteligência de ameaças;

II – reconhecer e tratar vulnerabilidades técnicas;

III – monitorar e tratar registros de auditoria;

IV – tratar incidentes de segurança da informação;

V – reportar ao Encarregado pelo Tratamento de Dados Pessoais os incidentes que

envolvam dados pessoais;

VI – compartilhar eventos de segurança da informação com demais órgãos e entidades da Administração Pública Estadual, imediatamente após sua ocorrência, para fins de prevenção e disseminação de boas práticas.

Art. 11 – Compete ao Encarregado pelo Tratamento de Dados Pessoais:

I – mapear, de forma contínua, as atividades de tratamento de dados pessoais realizadas no âmbito da SEDCON;

II – assegurar a conformidade das operações de tratamento com a Lei Federal nº 13.709, de 14 de agosto de 2018.

Art. 12 – Compete ao Comitê de Segurança e Privacidade da Informação:

I – reunir-se sempre que houver risco, evento ou incidente que demande atuação imediata do Comitê;

II – revisar periodicamente esta política, conforme estabelecido no Capítulo X;

III – avaliar e monitorar, de forma contínua, os riscos relacionados à segurança e à privacidade da informação;

IV – analisar infrações às diretrizes desta política e, quando caracterizado incidente de segurança ou privacidade, adotar as seguintes providências:

a) recomendar ao gestor do contrato a aplicação de sanções a fornecedores, trabalhadores terceirizados ou demais partes envolvidas, conforme instrumento vigente;

b) recomendar à Corregedoria a instauração de sindicância para avaliar a abertura de processo disciplinar contra servidor infrator;

V – propor soluções para o tratamento de riscos, oportunidades, eventos e incidentes relacionados à segurança e à privacidade da informação.

Parágrafo único. O Comitê será composto por representantes da Coordenadoria de Recursos Humanos, da Assessoria de Tecnologia de Informação e pelo Encarregado pelo Tratamento de Dados Pessoais, podendo contar, quando convocado para deliberação de pauta específica, com a participação de representante da Alta Administração, todos vinculados à SEDCON.

Art. 13 – Compete à Corregedoria:

I – apurar, mediante sindicância, as infrações cometidas por servidores que violem esta política ou os termos de responsabilidade firmados.

Parágrafo único. A penalidade de suspensão de até 30 (trinta) dias será aplicável, nos termos do art. 50, inciso II, do Decreto-Lei nº 220, de 18 de julho de 1975, quando apurado o desrespeito consciente ou premeditado às obrigações de segurança e privacidade da informação, conduta esta considerada falta grave para fins disciplinares. Outras penalidades previstas no referido Decreto-Lei, como advertência e repreensão, poderão ser aplicadas, conforme a natureza e a gravidade da infração.

Art. 14 – Compete ao Secretário de Estado da Secretaria de Estado de Defesa do Consumidor:

I – aplicar sanções aos servidores, conforme recomendação da Corregedoria, nos casos de infrações às disposições desta política;

II – aplicar sanções aos estagiários, conforme recomendação do Comitê de Segurança e Privacidade da Informação;

III – aplicar sanções aos fornecedores e demais partes envolvidas, conforme recomendação do Comitê de Segurança e Privacidade da Informação.

CAPÍTULO III – SEGURANÇA DA INFORMAÇÃO E TECNOLOGIA

Seção I – Gestão de Acesso

Art. 15 – A SEDCON deve vincular, ao Cadastro de Pessoas Físicas (CPF), todos os meios de identificação utilizados para fins laborais, como número de registro, crachá, login, certificado, assinatura digital, dado biométrico e reconhecimento facial.

Parágrafo único. As identidades atribuídas a mais de uma pessoa ou a sistemas, dispositivos ou aplicações automatizadas (identidades não humanas) devem ser restritas, justificadas, aprovadas e controladas pela Assessoria de Tecnologia de Informação.

Art. 16 – A concessão de acesso físico a áreas restritas, bem como o acesso lógico a sistemas, redes e informações institucionais, somente será autorizada mediante assinatura prévia, pelo usuário, do Termo de Responsabilidade de Segurança da Informação, devidamente registrado e arquivado pela área competente.

Art. 17 – A SEDCON deve restringir e gerenciar o acesso à informação e às funcionalidades dos softwares, observando:

I – a definição de perfis de acesso com base nos princípios da necessidade de conhecer, da necessidade de uso e do menor privilégio;

II – a criação de identidades e a atribuição de direitos de acesso mediante solicitação formal e autorização;

III – a exclusão de identidades e a revogação de direitos de acesso mediante solicitação formal e autorização;

IV – a remoção imediata de direitos de acesso que se tornarem desnecessários.

Art. 18 – Todos os softwares utilizados pela SEDCON devem exigir senhas complexas que atendam aos seguintes critérios:

I – conter, no mínimo, 14 (quatorze) caracteres;

II – incluir, obrigatoriamente:

a) uma letra minúscula;

b) uma letra maiúscula;

c) um número;

d) um caractere especial.

Parágrafo único. Caso o software não imponha automaticamente os critérios estabelecidos, cabe ao colaborador criar uma senha que os atenda.

Art. 19 – Nos dispositivos que aceitam apenas senhas numéricas, é vedado ao colaborador utilizar sequências facilmente identificáveis, como datas de aniversário, números de telefone, entre outros.

Art. 20 – É vedado ao colaborador expor, compartilhar ou revelar suas senhas a terceiros.

Seção II – Uso Aceitável dos Ativos de Informação

Art. 21 – É vedado ao colaborador utilizar os ativos de informação da SEDCON para finalidades alheias às atividades institucionais.

Parágrafo único. Consideram-se ativos de informação todos os recursos tecnológicos, sistemas, dados, documentos e demais elementos que suportam o tratamento, armazenamento, processamento e transmissão de informações institucionais.

Art. 22 – O colaborador deve zelar pelo uso adequado dos dispositivos tecnológicos fornecidos, observando que:

I – é proibida a remoção, alteração ou acréscimo de componentes de hardware sem

autorização;

II – é proibida a instalação de softwares não homologados;

III – não é permitido realizar download de softwares ou arquivos executáveis da internet sem autorização prévia da Assessoria de Tecnologia de Informação.

Art. 23 – O uso de mídias removíveis nos dispositivos da SEDCON será, por padrão, bloqueado. Quando autorizado, deve estar sujeito a controle rigoroso, incluindo a verificação automática de códigos maliciosos no momento da inserção.

Parágrafo único. A criptografia de documentos com informações sensíveis armazenadas em mídias removíveis deverá ser orientada pela Assessoria de Tecnologia de Informação, sendo responsabilidade do colaborador seguir os procedimentos definidos.

Art. 24 – É vedado aos colaboradores, nos dispositivos tecnológicos da SEDCON, acessar conteúdos das seguintes categorias:

I – ilegais ou em desacordo com a legislação;

II – pornográficos ou sexualmente explícitos;

III – relacionados a jogos de azar ou apostas;

IV – redes sociais, salvo quando expressamente autorizadas para fins institucionais;

V – potencialmente prejudiciais à segurança da informação.

Art. 25 – O colaborador deve observar as seguintes orientações:

I – não armazenar conteúdos ilegais, não éticos ou de caráter pessoal nos ativos institucionais;

II – utilizar apenas os locais apropriados fornecidos pela Secretaria para armazenar informações institucionais;

III – não alterar as configurações de segurança dos dispositivos, nem conectar dispositivos não homologados à rede;

IV – desligar o computador ao final do expediente, salvo orientação em contrário da Assessoria de Tecnologia de Informação;

V – retirar imediatamente da impressora documentos que contenham dados sensíveis;

VI – manter o ambiente de trabalho organizado, armazenando adequadamente documentos e mídias;

VII – proteger informações exibidas na tela contra visualização não autorizada, evitando exposições em ambientes públicos;

VIII – bloquear ou desconectar o dispositivo sempre que se ausentar de sua estação de trabalho.

Seção III – Trabalho Remoto e Uso de Dispositivos Móveis

Art. 26 – Em caso de furto ou roubo de dispositivo móvel, institucional ou pessoal homologado, o colaborador deverá notificar imediatamente a SEDCON e registrar boletim de ocorrência junto à autoridade competente.

Art. 27 – É vedado conectar dispositivos móveis da SEDCON a redes públicas de Wi-Fi.

Seção IV – Ambiente Físico

Art. 28 – A SEDCON deve garantir:

I – controle de acesso físico às suas instalações;

II – proteção contra incêndios, inundações, descargas elétricas, explosões e manifestações civis;

III – sobrescrição segura ou destruição física de dispositivos de armazenamento antes de descarte;

IV – proteção do cabeamento contra danos físicos e interferências;

V – proteção contra falhas de energia, telecomunicações ou ar-condicionado, por meio de sistemas redundantes.

Art. 29 – É vedado ao colaborador remover, instalar ou movimentar dispositivos tecnológicos da SEDCON sem autorização, exceto quando se tratar de dispositivos móveis previamente autorizados.

Seção V – Códigos Maliciosos

Art. 30 – O colaborador deve adotar condutas preventivas contra códigos maliciosos, abstendo-se de interromper varreduras de segurança e de interagir com anexos ou links suspeitos.

Seção VI – Serviços em Nuvem

Art. 31 – A SEDCON deve assegurar que, para cada serviço em nuvem contratado, sejam documentadas:

I – as responsabilidades compartilhadas entre a SEDCON e o provedor;

II – os controles aplicáveis de segurança e privacidade, e seus responsáveis;

III – os procedimentos para uso dos recursos disponibilizados pelo provedor;

IV – o processo de devolução das informações ao término da contratação;

V – o local de armazenamento dos dados e a legislação aplicável.

Seção VII – Incidentes de Segurança e Privacidade da Informação

Art. 32 – A SEDCON deve implementar processo estruturado para gestão de incidentes, contemplando: detecção, classificação, priorização, escalonamento, análise, resolução, comunicação, registro e tratamento das lições aprendidas.

Parágrafo único. Durante a resolução de incidentes, devem ser seguidas as etapas de contenção, eliminação da causa e restauração dos serviços afetados.

Seção VIII – Vulnerabilidades Técnicas

Art. 33 – Compete à SEDCON:

I – manter processo contínuo de avaliação e tratamento de vulnerabilidades técnicas;

II – produzir inteligência de ameaças por meio de coleta e análise de informações;

III – aplicar criptografia de forma adequada para proteger as informações.

Art. 34 – O descarte de documentos, mídias e ativos com dados pessoais ou sensíveis deve ser realizado de forma segura, conforme norma complementar.

Parágrafo único. O descarte de informações institucionais não classificadas também deve seguir critérios de segurança e confidencialidade.

Seção IX – Registro de Auditoria

Art. 35 – A SEDCON deve garantir que seus ativos tecnológicos estejam com auditoria habilitada, sincronizados com fonte confiável de data e hora, e que os registros sejam monitorados e analisados periodicamente.

Seção X – Desenvolvimento de Software Interno ou Terceirizado

Art. 36 – O desenvolvimento de softwares, próprios ou contratados, deve: utilizar métodos estruturados, aplicar técnicas de prevenção de vulnerabilidades e respeitar as normas de proteção de dados pessoais.

Seção XI – Cópia de Segurança

Art. 37 – A realização de cópias de segurança (backups) regulares é de responsabilidade da SEDCON, com o objetivo de garantir a integridade e a recuperação das informações institucionais

Seção XII – Continuidade do Negócio

Art. 38 – A SEDCON deve manter o Plano de Continuidade do Negócio com orientações para garantir a manutenção dos serviços essenciais em situações de emergência ou desastre.

Parágrafo único. O plano deve assegurar a proteção da segurança e da privacidade das informações durante períodos críticos.

Art. 39 – A SEDCON deve garantir a disponibilidade dos equipamentos e sistemas tecnológicos, por meio de recursos redundantes que evitem interrupções.

CAPÍTULO IV – GOVERNANÇA, PRIVACIDADE E TRANSFERÊNCIA DE INFORMAÇÃO

Seção I – Classificação da Informação

Art. 40 – A SEDCON deve classificar e rotular suas informações quanto ao grau e ao prazo de sigilo, nas categorias ultrassecreta, secreta ou reservada, conforme previsto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Parágrafo único. No caso de informação pessoal, independentemente da classificação de sigilo atribuída, o acesso deverá ser restrito por até 100 (cem) anos, contados a partir da data de produção. Nesse período, a informação somente poderá ser acessada por agentes públicos autorizados e pelo próprio titular, conforme a Lei de Acesso à Informação.

Art. 41 – As informações da SEDCON devem ser classificadas e rotuladas no sistema SEIRJ segundo os níveis de sigilo: público, restrito e sigiloso, conforme disposto no Decreto nº 48.209, de 19 de setembro de 2022.

I – Consideram-se restritos ou sigilosos os documentos e processos que contenham informações pessoais ou assuntos protegidos por sigilo legal.

II – São considerados públicos os documentos e processos que não se enquadrem em hipóteses de sigilo.

III – É vedada a inclusão, no SEI-RJ, de documentos classificados como ultrassecretos, secretos ou reservados, nos termos dos artigos 23 e 24 da Lei nº 12.527, de 18 de novembro de 2011 e dos artigos 22, 27, 28 e 29 do Decreto nº 46.205, de 27 de dezembro de 2017.

Seção II – Transferência da Informação Institucional

Art. 42 – O colaborador deve utilizar exclusivamente o e-mail institucional para a comunicação de assuntos relacionados à SEDCON, sendo vedado o uso de e-mails pessoais para fins institucionais.

Art. 43 – Ao utilizar o e-mail institucional, o colaborador deve observar as seguintes proibições:

I – envio de propagandas, mensagens em cadeia (correntes), conteúdos ilegais ou não éticos, bem como comunicações discriminatórias ou ofensivas relacionadas à nacionalidade, raça, orientação sexual, religião ou opinião política;

II – envio de arquivos contendo códigos maliciosos;

III – transmissão de conteúdos que infrinjam direitos autorais ou de propriedade intelectual;

IV – cadastramento do e-mail institucional em sites ou aplicativos externos, salvo com autorização formal da SEDCON.

Parágrafo único. Os e-mails institucionais autorizados a serem cadastrados em plataformas externas devem ser rigorosamente controlados pela Assessoria de Tecnologia da Informação.

Art. 44 – A transferência e comunicação de informações sensíveis devem observar as seguintes diretrizes:

I – utilização exclusiva de plataformas e aplicações homologadas pela SEDCON, garantindo a segurança e confidencialidade dos dados;

II – rotulagem da mensagem eletrônica conforme a classificação da informação estabelecida na Seção I deste Capítulo;

III – realização de dupla verificação dos destinatários antes do envio de informações sensíveis por qualquer meio de comunicação.

Seção III – Privacidade

Art. 45 – A SEDCON deve garantir que todas as operações que envolvam dados pessoais estejam em conformidade com a Lei nº 13.709, de 14 de agosto de 2018, observando as seguintes diretrizes:

I – implementar política de privacidade com o objetivo de informar os titulares sobre o tratamento de seus dados, inclusive os períodos de armazenamento;

II – garantir a licitude das finalidades do tratamento de dados pessoais, mediante mapeamento e definição clara de propósitos;

III – assegurar que os processos e softwares sejam desenhados ou ajustados para limitar o tratamento de dados ao estritamente necessário, de acordo com as finalidades informadas.

Seção IV – Fornecedores

Art. 46 – Os contratos firmados pela SEDCON com fornecedores devem conter cláusulas específicas com os requisitos de segurança e privacidade da informação aplicáveis, bem como as respectivas responsabilidades.

Parágrafo único. No caso de contratos relacionados à área de tecnologia da informação, os requisitos de segurança e privacidade devem ser estendidos à cadeia de suprimentos dos fornecedores, mediante cláusula contratual específica.

Seção V – Uso de Dispositivo Pessoal no Trabalho

Art. 47 – O colaborador que optar por utilizar dispositivo pessoal, como celular ou computador, para atividades laborais, deverá:

I – solicitar autorização prévia da Assessoria de Tecnologia de Informação, que definirá os critérios de segurança aplicáveis ao dispositivo;

II – no caso de uso de computador pessoal, manter a segregação entre uso pessoal e uso profissional, conforme as orientações da área técnica responsável.

Parágrafo único. As diretrizes desta política devem ser integralmente observadas por servidores e trabalhadores terceirizados também em seus dispositivos pessoais, salvo nos casos em que houver orientações específicas aplicáveis apenas a dispositivos da SEDCON.

CAPÍTULO V – DOS DIREITOS DOS TITULARES DE DADOS PESSOAIS

Art. 48 – A SEDCON deverá assegurar mecanismos adequados para o atendimento célere, transparente e acessível às solicitações dos titulares de dados pessoais, garantindo, no mínimo, os seguintes direitos:

I – confirmação da existência de tratamento de dados pessoais;

II – acesso facilitado aos dados pessoais tratados;

III – retificação de dados incompletos, inexatos ou desatualizados;

IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a legislação aplicável;

V – portabilidade dos dados pessoais, observadas as normas da Autoridade Nacional de Proteção de Dados (ANPD) e as regulamentações setoriais aplicáveis;

VI – informação clara e acessível acerca das entidades públicas e privadas com as quais os dados tenham sido compartilhados;

VII – revogação do consentimento, quando este for a base legal para o tratamento.

Parágrafo único. Os prazos e procedimentos para o exercício dos direitos previstos neste artigo deverão observar a legislação vigente e as diretrizes expedidas pela Autoridade Nacional de Proteção de Dados (ANPD).

CAPÍTULO VI – DO FLUXO DE COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA E PRIVACIDADE

Art. 49 – Na hipótese de identificação ou suspeita de incidente de segurança ou de privacidade da informação envolvendo dados pessoais, qualquer servidor, estagiário, fornecedor ou trabalhador terceirizado deverá:

I – comunicar imediatamente o fato à Assessoria de Tecnologia de Informação e ao Encarregado pelo Tratamento de Dados Pessoais;

II – registrar as informações mínimas relativas ao incidente, tais como data, horário, descrição do ocorrido e sistemas ou ativos afetados;

III – colaborar com as etapas de contenção, erradicação, recuperação e análise pós-incidente.

§ 1º O Encarregado, em conjunto com o Comitê de Segurança e Privacidade da Informação, deverá avaliar a gravidade do incidente e o risco potencial aos titulares de dados, decidindo sobre a obrigatoriedade e a forma de comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos próprios titulares dos dados.

§ 2º Quando exigida, a comunicação aos titulares deverá ser redigida em linguagem clara e objetiva, contendo, sempre que possível, orientações sobre medidas preventivas a serem adotadas.

§ 3º Os indicadores relacionados a incidentes de segurança e privacidade deverão ser avaliados periodicamente pelo Comitê de Segurança e Privacidade da Informação e relatados à Alta Administração anualmente.

CAPÍTULO VII – DOS DOCUMENTOS COMPLEMENTARES

Art. 50. Com o objetivo de assegurar a efetividade desta Política de Segurança e Privacidade da Informação, a SEDCON deverá instituir, manter atualizados e aplicar os seguintes documentos normativos:

I – Gestão de Acessos e Segurança de Redes: define os controles de acesso a ambientes físicos e lógicos, bem como os mecanismos de segmentação e proteção das redes corporativas;

II – Gestão de Ativos e da Informação Documentada: trata do inventário, classificação e monitoramento de ativos, bem como da organização, controle de versões e acesso a documentos institucionais;

III – Gestão de Mudanças, Capacidade e Disponibilidade de Tecnologia de Informação: estabelece diretrizes para mudanças em sistemas e infraestrutura, além do planejamento e garantia de resiliência dos serviços tecnológicos;

IV – Gestão de Riscos, Vulnerabilidades e Ameaças: contempla a identificação, análise e mitigação de riscos técnicos e estratégicos, incluindo falhas de segurança e ameaças cibernéticas;

V – Gestão de Eventos e Incidentes de Segurança e Privacidade: dispõe sobre o monitoramento, registro e tratamento de eventos e incidentes que envolvam a segurança da informação ou dados pessoais;

VI – Gestão de Proteção contra Códigos Maliciosos e Serviços Terceirizados: define controles técnicos e contratuais para prevenção de ameaças digitais e proteção da informação compartilhada com terceiros;

VII – Gestão da Privacidade: estabelece os princípios e medidas para o tratamento legal, justo, transparente e seguro dos dados pessoais e sensíveis, conforme previsto na LGPD;

VIII – Gestão da Continuidade do Negócio: define estratégias para assegurar a manutenção das operações críticas da Secretaria em situações de crise ou interrupção;

IX – Gestão de Pessoas e Conscientização em Segurança da Informação: regula os critérios de contratação, além de promover capacitação contínua dos colaboradores em boas práticas de segurança e privacidade.

CAPÍTULO VIII – DO PROCESSO DISCIPLINAR

Art. 51 – O descumprimento das diretrizes estabelecidas nesta Política sujeita o servidor à responsabilização administrativa, nos termos da legislação aplicável.

Parágrafo único – A responsabilização administrativa referida no caput não exclui a possibilidade de apuração de responsabilidade civil e penal pelas condutas irregulares eventualmente praticadas.

Art. 52 – O Comitê de Segurança e Privacidade da Informação deverá comunicar, de forma imediata, à Corregedoria os casos de descumprimento desta Política por parte dos servidores, a fim de que sejam adotadas as providências cabíveis para a instauração de Procedimento Administrativo de Sindicância.

Art. 53 – Verificada a prática de transgressão disciplinar, com base no conjunto probatório colhido durante a apuração, serão aplicadas as penalidades previstas no:

I – Decreto-Lei nº 220, de 18 de julho de 1975 (Estatuto dos Funcionários Públicos Civis do Poder Executivo do Estado do Rio de Janeiro);

II – Decreto nº 2.479, de 8 de março de 1979 (Regulamento do Estatuto dos Funcionários Públicos Civis do Poder Executivo do Estado do Rio de Janeiro);

III – Plano de Integridade da SEDCON.

CAPÍTULO IX – DA VIGÊNCIA

Art. 54 – Esta Resolução entra em vigor na data de sua publicação, devendo ser revista quanto à sua pertinência a cada 12 (doze) meses ou sempre que houver alterações significativas que impactem a segurança ou a privacidade da informação no âmbito da SEDCON.

Rio de Janeiro, 18 de novembro de 2025

GUTEMBERG DE PAULA FONSECA

Secretário de Estado de Defesa do Consumidor

Documento assinado eletronicamente por **Gutemberg de Paula Fonseca**, **Secretário**, em 18/11/2025, às 17:14, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **119143664** e o código CRC **6256402D**.