Protocolo: 1037390
Data: 05/12/2024
Título: INSTITUI A POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS DA EMPRESA MUNICIPAL DE INFORMÁTICA S.A. - IPLANRIO (3)
Página(s): a

PORTARIA "N" Nº 317 DE 03 DE DEZEMBRO DE 2024

INSTITUI **A POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS DA EMPRESA MUNICIPAL DE INFORMÁTICA S.A. - IPLANRIO**

O DIRETOR-PRESIDENTE, no uso das atribuições legais que lhe são conferidas pela legislação em vigor e:

CONSIDERANDO a Lei Federal nº 13.709, de 14 de agosto de 2018, que institui a Lei Geral de Proteção de Dados Pessoais (LGPD), estabelecendo normas gerais de proteção de dados pessoais de interesse nacional, obrigatórias para a União, Estados, Distrito Federal e Municípios;

CONSIDERANDO o Decreto Rio Nº 54.984, de 21 de agosto de 2024, que institui a Política Municipal de Proteção de Dados Pessoais, no âmbito do Município do Rio de Janeiro;

CONSIDERANDO que a IplanRio é a maior operadora de dados pessoais tratados por meio de sistemas e serviços de Tecnologia da Informação e Comunicação (TIC) no âmbito da Administração Pública Municipal, desempenhando papel essencial na gestão e mitigação dos riscos relacionados à privacidade desses dados,

Art. 1º. Fica instituída a **POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS da Empresa Municipal de Informática S.A.** - **IplanRio**, nos termos do anexo que integra esta portaria.

Art. 2º. Esta portaria entra em vigor na data de sua publicação, revogando-se as disposições em contrário.

ANEXO

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º. A presente política estabelece as diretrizes para a proteção de dados pessoais no âmbito da IplanRio - Empresa Municipal de Informática S.A.
Art. 2º. Esta política aplica-se a todos os agentes públicos municipais e prestadores de serviços que estejam autorizados a tratar de dados pessoais no âmbito da IplanRio.
Art. 3º. Para fins desta Política considere-se:
I.**Acesso**: Capacidade de utilizar um ativo da informação seja físico ou tecnológico, como, por exemplo: ler, criar, modificar ou excluir arquivos; executar programas; conectar-se a dispositivos, redes, sistemas ou serviços; ou acesso a áreas restritas que hospedem informações confidenciais;
II.**Ambiente de Desenvolvimento**: Ambiente de Tecnologia da Informação e Comunicação (TIC) destinado a atividades de desenvolvimento e manutenção de sistemas e aplicativos de uma organização;
III.**Ambiente de Homologação**: Ambiente de TIC projetado para simular o ambiente de produção, destinado a testes de acessibilidade realizados pelos usuários, com o objetivo de garantir que sistemas e aplicativos atendam a todos os requisitos necessários para sua entrada em produção;
IV.**Ambiente de Produção**: Ambiente de TIC responsável por suportar os sistemas e aplicativos que sustentam os serviços e processos de negócio de uma organização;
V.**Ameaça**: Evento com potencial de comprometer os objetivos de uma organização, seja por causar danos diretos aos seus ativos ou prejuízos decorrentes de situações inesperadas como incêndios, falhas de equipamentos, indisponibilidade de sistemas ou serviços, ou destruição de informações sensíveis, dentre outros);

VI.**Anonimização**: Processo que utiliza meios técnicos razoáveis e disponíveis no momento do tratamento, pelo que um dado pessoal perde a possibilidade de ser associado, direta ou indireta, a um indivíduo;
VII.**Ativo da Informação**: Qualquer recurso físico, tecnológico ou humano que apoie as operações de coleta, armazenamento, processamento, compartilhamento ou descarte de informações, como locais físicos, documentos, equipamentos, sistemas e pessoas;
VIII.**Autenticidade**: Garantia de que os ativos da informação identificada em um processo de comunicação como remetentes ou destinatários específicos, de fato, a quem afirma ser, garantindo a veracidade das identidades envolvidas no processo;
IX.**Autorização**: Concessão de um conjunto de permissões de acesso a ativos de informação a um usuário, realizada após a autenticação;
X.**Classificação da Informação**: Processo que determina o grau de sensibilidade de uma informação para os negócios de uma organização, considerando os impactos potenciais de uma violação de segurança que compromete os princípios básicos da Segurança da Informação: confidencialidade, integridade e disponibilidade;
XI.**Colaborador**: Agente Público ou prestador de serviço autorizado a realizar o tratamento de dados pessoais no âmbito da IplanRio;
XII.**Conscientização**: Processo educacional que busca capacitar indivíduos, a incorporá-los, em suas rotinas pessoais e profissionais, boas práticas relacionadas à proteção de dados pessoais;
XIII.**Confidencialidade**: Propriedade que garante que a informação esteja disponível exclusivamente para indivíduos ou processos devidamente autorizados;
XIV.**Conta de Acesso**: Identificador único, pessoal e intransferível de um usuário utilizado para identificá-lo durante os acessos realizados a ativos da informação;
XV.**Controlador**: Pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões relacionadas ao tratamento de dados pessoais;
XVI.**Controle de Acesso**: Conjunto de mecanismos destinados a proteger as informações armazenadas em ativos da informação contra acessos não autorizados;
XVII.**Dado Pessoal**: Qualquer informação relacionada a pessoa natural identificada ou identificável;
XVIII.**Dado Pessoal Sensível**: Dado pessoal que revela origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dados referentes à saúde, à vida sexual, genética ou biometria, quando vinculados a uma pessoa natural;
XIX.**Dado Anonimizado**: Dado relativo a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis no momento do de seu tratamento;
XX.**Disponibilidade**: Propriedade que garante que a informação esteja disponível a pessoas e processos autorizados sempre que necessário;
XXI.**Encarregado**: Pessoa designada pelo controlador e operador para atuar como canal de comunicação entre o controlador, o operador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
XXII.**Gestor de Sistema**: Funcionário responsável pelo gerenciamento do ciclo de vida de um sistema;
XXIII.**Identificação**: Processo pelo qual um usuário fornece sua identidade para acessar um ativo da informação;
XXIV.**Incidente de Segurança com Dados Pessoais**: Conjunto de eventos adversos que comprometem a segurança de dados pessoais, podendo gerar riscos à privacidade de seus titulares;
XXV.**Informação**: Resultado do processamento, manipulação e organização de dados, de forma a representar um acréscimo ao conhecimento do receptor. A informação pode ser apresentada de diversas formas: como texto, imagem, áudio, entre outras;
XXVI.**Integridade**: Propriedade que garante a informação permaneça intacta, protegida contra perda, danos ou modificações não autorizadas;
XXVII.**Operador**: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
XXVIII.**Plano de Gerenciamento de Incidentes**: Documento que define de forma clara e detalhada o plano de ação a ser seguido em caso de incidentes. O plano deve abranger todos os ativos físicos, tecnológicos e humanos necessários para a implementação eficaz do processo de gerenciamento de incidentes;
XXIX.***Privacy by Default*:** Abordagem da Engenharia de Sistemas que garante que todas as configurações iniciais relacionadas a sejam de privacidade definidas com o maior nível de restrição possível. Desta forma, o usuário não precisa realizar ajustes adicionais para aumentar a privacidade dos dados pessoais tratados pelo sistema.

XXX.***Privacy by Design*:** Abordagem da Engenharia de Sistemas que integra a identificação, análise e tratamento dos riscos à privacidade desde a fase de concepção do sistema, mantendo essas práticas ao longo de todo o ciclo de vida do sistema;
XXXI.**Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**: Documento do controlador que contém a descrição dos processos de tratamento de dados pessoais que apresentam riscos civis e aos direitos fundamentais, bem como as medidas, salvaguardas e mecanismos adotados para mitigar esses riscos;
XXXII.**Rede Corporativa de Computadores:** Conjunto de recursos de Tecnologia da Informação e Comunicação (TIC) interligados, por meio dos quais circulam as informações corporativas da Prefeitura da Cidade do Rio de Janeiro (PCRJ);
XXXIII.**Risco de Segurança da Informação**: Probabilidade de ameaças comprometerem a confidencialidade, integridade ou disponibilidade da informação, gerando impactos negativos para a organização;
XXXIV.**Risco de Privacidade**: Probabilidade de ameaças que afetam os princípios de tratamento de dados pessoais previstos na legislação vigente sobre proteção de dados pessoais;
XXXV.**Segurança Física**: Processo destinado a proteger todos os ativos da informação contra ameaças naturais (como incêndios) e humanas (como acessos não autorizados);
XXXVI.**Sensibilização**: Conjunto de ações voltadas a identificar, recomendar, criar e implantar programas de conscientização, com o objetivo de promover melhorias e mudanças de atitude e educação organizacional em relação à proteção de dados pessoais;
XXXVII.**Sistema de Informação:** Conjunto de ativos da informação organizados para coletar, armazenar, transportar e processar informações, com objetivo de apoiar produtos, serviços ou processos de uma organização;
XXXVIII.***Software***: Conjunto de programas existentes em um computador, incluindo sistemas operacionais e outros softwares;
XXXIX.**Titular**: Pessoa Natural a quem se referem os dados pessoais objeto de tratamento;
XL.**Tratamento**: Qualquer operação realizada com dados pessoais, incluindo coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, alteração, comunicação, transferência, difusão ou extração de informações;
XLI.**Treinamento**: Conjunto de ações específicas ao desenvolvimento de competências e habilidades específicas em proteção de dados pessoais, permitindo o desempenho das atribuições funcionais do indivíduo na organização;
XLII.**Vulnerabilidade**: A fragilidade associada aos ativos da informação que, ao ser explorada por uma ameaça, pode resultar num incidente de segurança comprometendo um ou mais princípios de segurança da informação: confidencialidade, integridade e disponibilidade.
Art. 4º. Os riscos de privacidade decorrentes de quaisquer tratamentos de dados pessoais realizados por meio de produtos, serviços, processos ou atividades eventualmente devem ser identificados, avaliados e gerenciados ao longo de todo ciclo de vida desses dados.
Art. 5º. Os agentes públicos devem ser regularmente capacitados, de forma a manterem um nível de conhecimento em gestão de riscos de privacidade compatível com suas competências e responsabilidades.
Parágrafo Único: A periodicidade e o conteúdo dos processos de capacitação devem ser definidos com base no volume, sensibilidade e regularidade do tratamento de dados pessoais, bem como nas competências e responsabilidades inerentes ao cargo ou função desempenhada pelo agente.
Art. 6º. A implantação ou utilização de qualquer nova solução tecnológica deve incluir, como uma de suas dimensões de gerenciamento de riscos operacionais, os riscos de privacidade, incluindo a conformidade com a legislação e as normas vigentes relativas à proteção de dados pessoais.

CAPÍTULO II
DA PROTEÇÃO DE DADOS PESSOAIS

Seção I
Do Tratamento de Dados Pessoais

Art. 7º. O tratamento de dados pessoais deve atender os seguintes requisitos:
I.Os dados pessoais devem ser tratados em conformidade com os princípios e as diretrizes estabelecidas pela **Política Municipal de Proteção de Dados Pessoais**;
II.Os dados pessoais serão identificados e classificados quanto à sua sensibilidade, de forma a garantir a proteção adequada;

III.As medidas de segurança e proteção de dados pessoais devem ser proporcionais à sua classificação e ao nível de risco aos quais estão expostos;
IV.Os colaboradores devem garantir o sigilo dos dados pessoais aos quais tenham acesso em decorrência de suas competências e responsabilidades, adotando as disposições necessárias para garantir que o tratamento esteja em conformidade com a legislação e as normas vigentes;
V.Os procedimentos relacionados ao desligamento de pessoal devem prever a devolução dos ativos das informações corporativas usadas no tratamento de dados pessoais, bem como das cópias de segurança desses dados que eventualmente, estejam em sua posse dos colaboradores.

Seção II
Dos Sistemas de Informação

Art. 8º. Os riscos à proteção de dados pessoais decorrentes do projeto, aquisição, desenvolvimento, implementação, configuração, modificação e gerenciamento de sistemas de informação devem ser previamente avaliados. Para tanto, os seguintes requisitos devem ser atendidos:
I.A proteção de dados pessoais deve ser promovida desde as fases iniciais do projeto de um sistema, mantendo-se ao longo de todo o seu ciclo de vida, em conformidade com os conceitos de ***Privacy by Design*** *e* ***Privacy by Default***;
II.A necessidade de criação de um **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)** deve ser avaliada durante a fase inicial do projeto de um sistema, garantindo que este seja capaz de abordar oportunamente os riscos de privacidade identificados;
III.As migrações de sistemas devem passar por processo de análise de riscos à privacidade;
IV.As alterações nos sistemas devem ser avaliadas e testadas quanto ao risco de gerar efeitos adversos na proteção dos dados pessoais tratados pelo sistema, bem como pelos sistemas com os quais há integração;
V.Mecanismos de teste devem ser implementados para garantir que as alterações realizadas em um sistema, mesmo que este não trate dados pessoais, não impactem adversamente o perfil de risco de outros sistemas que tratam dados pessoais;
VI.É vedado o uso de dados pessoais em ambientes de desenvolvimento, teste e homologação, exceto quando esses dados forem pseudonimizados ou anonimizados.

Seção III
Dos Sistemas de Gerenciamento de Banco de Dados

Art. 9º. Deve ser mantido um inventário de dados pessoais em todas as instâncias de banco de dados de produção. O inventário deverá conter, no mínimo:
I.Os diferentes tipos de dados pessoais armazenados;
II.A localização dos dados pessoais;
III.A descrição das políticas de manutenção e descarte aplicavéis a esses dados.
Art. 10. Devem ser implementados controles para garantir a proteção dos sistemas de gerenciamento de banco de dados (SGDBs) e dos dados pessoais que hospedam. Entre as medidas de segurança a serem cumpridas, devem constar, no mínimo:
I.Uso de criptografia para proteção de dados;
II.Gerenciamento de vulnerabilidades e configuração segura dos SGDBs;
III.Monitoramento de atividades nos bancos de dados; e
IV.Implementação de soluções de alta disponibilidade, backup e recovery.

Seção IV
Da Avaliação e Análise de Riscos de Privacidade

Art. 11. Devem ser definidos processos que possibilitem a identificação, análise, avaliação, tratamento, comunicação e monitoramento periódico dos riscos de privacidade associados às operações de tratamento de dados pessoais realizadas pela IplanRio.
§ **1º.** Esses processos devem ter por objetivo reduzir vulnerabilidades, previnir ameaças, minimizar a exposição aos riscos e mitigar os impactos de eventuais incidentes de segurança relacionados a dados pessoais;
§ **2º.** A avaliação de riscos de privacidade deve ser integrada à avaliação de riscos de segurança da informação, promovendo uma abordagem conjunta e abrangente.

Seção V
Da Gestão de Incidentes de Segurança com Dados Pessoais

Art. 12. Os incidentes de segurança envolvendo dados pessoais devem ser identificados, monitorados, comunicados e tratados de forma adequada e em tempo hábil, conforme estabelecido no **Plano de Gerenciamento de Incidentes de Segurança com Dados Pessoais**. Esse plano deve

incluir, no mínimo, os seguintes elementos:
I.**Procedimentos**: Diretrizes para a identificação, gestão, avaliação da gravidade, escalonamento e resolução de incidentes de segurança com dados pessoais;
II.**Responsabilidades**: Definição clara das responsabilidades relacionadas à identificação e ao tratamento de incidentes;
III.**Conformidade Legal**: Um processo para garantir o cumprimento das diretrizes expressas em leis e disposições aplicáveis ao tratamento de incidentes de segurança com dados pessoais, incluindo, quando necessário, uma notificação às partes interessadas;
IV.**Testes Periódicos**: Procedimentos para a realiação de teste periódico do plano, a fim de validar sua eficácia:
V.**Revisão Anual**: Um processo de revisão periódica, com frequência mínima anual, baseado no histórico de tratamento de incidentes reais e nos resultados dos testes periódicos realizados.

Seção VI
Do Controle de Acesso

Art. 13. O controle de acesso a dados pessoais e aos ativos da informação utilizados em seu tratamento deve ser regido por um processo formal, que gera a criação, manutenção, suspensão e cancelamento desses acessos.
§ **1º.** O acesso aos ativos da informação deve realizado por meio de contas e credenciais de uso pessoais e intransferíveis, responsabilizando o usuário por quaisquer ações realizadas por essas credenciais;
§ **2º.** A autorização de acesso a dados pessoais e aos ativos da informação utilizada em seu tratamento deve ser limitada aos privilégios mínimos necessários para que os usuários desempenhem suas competências e responsabilidades;
§ **3º.** Os direitos de acesso a dados pessoais são concedidos a respeito de serviços devem ser restritos ao período de vigência de seus respectivos contratos;
§ **4º.** Todas as contas e credenciais de acesso aos ativos da informação e instalações físicas que suportam o tratamento de dados pessoais devem ser revogadas ou suspensas assim que deixarem de ser permitidas para os fins a que se destinam.

Seção VII
Da Segurança Física
Art. 14º. As instalações físicas e áreas destinadas ao tratamento de dados pessoais devem ser protegidas contra ameaças naturais e humanas.
§ **1º.** Os controles físicos de proteção de dados pessoais devem fornecer riscos identificados, garantindo a segurança adequada;
§ **2º.** Os ativos da informação utilizados no tratamento de dados pessoais devem ser armazenados em áreas de acesso restrito;
§ **3º.** O acesso de visitantes às áreas que hospedam ativos de informação crítica para o tratamento de dados pessoais deve ser previamente autorizado por um agente competente e acompanhado por um representante designado.

Seção VIII
Da Capacitação
Art. 15º. Os colaboradores que atuam no tratamento de dados pessoais devem possuir conhecimentos de Proteção de Dados Pessoais compatíveis com suas competências e responsabilidades, além de conhecer integralmente a legislação e as normas vigentes.
§ **1º.** Deve ser instruído um programa permanente de sensibilização e conscientização em Proteção de Dados Pessoais, direcionado a todos os colaboradores, com o objetivo de promover a compreensão da legislação, regulamentação vigente e boas práticas relacionadas ao tema, permitindo sua aplicação no dia a dia de trabalho;
§ **2º.** Deve ser implementado um programa permanente de treinamento em Proteção de Dados Pessoais, abrangendo todos os colaboradores envolvidos no tratamento de dados pessoais, para garantir o cumprimento eficaz de suas competências e responsabilidades relacionadas ao tema;
§ **4º.** Deve ser estabelecido um programa permanente de formação de profissionais especializados em Proteção de Dados Pessoais, com o objetivo de oferecer suporte ao Programa Municipal de Proteção de Dados Pessoais.

CAPÍTULO III
DAS ATRIBUIÇÕES

Art. 16º. São atribuições da direção da IplanRio:

I. Buscar os recursos necessários para a implementação desta política;

II. Dirigir, avaliar e monitorar as ações de suporte à implementação desta política em seu âmbito de atuação.

Art. 17º. São atribuições das gerências da IplanRio:

I. Planejar, executar e controlar as ações de implementação desta política em seu âmbito de atuação;

II. Monitorar o grau de conformidade das áreas sob sua liderança, levando em consideração e gerenciando as ações de resposta para corrigir eventuais desconformidades identificadas;

III. Avaliar e revisar a alocação, eficiência e eficácia dos recursos utilizados em atividades relacionadas à proteção de dados pessoais, reportando às respectivas lideranças as necessidades de suporte identificadas.

Art. 18º. São atribuições do(s) encarregado(s):

I. Fornecer orientações e acompanhar as ações de gerenciamento de riscos de privacidade;

II. Prover orientações quanto à identificação dos riscos de privacidade no tratamento de dados pessoais, bem como na indicação das boas práticas para o seu tratamento;

III. Propor uma regulamentação interna de proteção de dados pessoais;

IV. Coordenar os programas internos de conformidade à legislação e regulamentos vigentes em proteção de dados pessoais;

V. Monitorar continuamente a conformidade da IplanRio à legislação e regulamentação aplicáveis à proteção de dados pessoais;

VI. Promover a cultura de proteção de dados pessoais, prestando assessoramento e suporte às ações de sensibilização, conscientização e treinamento;

VII. Atuar como canal de comunicação junto aos controladores, operadores, titulares dos dados, autoridades municipais e à Autoridade Nacional de Proteção de Dados - ANPD.

Art. 19º. São atribuições dos colaboradores:

I. Executar suas atividades funcionais em conformidade com todas as políticas, normas e procedimentos relacionados à proteção de dados pessoais;

II. Observar desvios das políticas, normas e procedimentos estabelecidos e informar tais desvios ao superior imediatamente.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 20º. Aplica-se aos dados pessoais todas as disposições da Política de Segurança da Informação e suas normas complementares.

Art. 21º. Os colaboradores que violarem esta política estarão sujeitos às sanções administrativas previstas legislação vigente.