DEFENSORIA PÚBLICA
DO ESTADO DO RIO DE JANEIRO

Referência: Processo nº E-20/001.004338/2021

RESOLUÇÃO DPGERJ N° 1142 DE 25 DE ABRIL DE 2022

INSTITUI O PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA NO ÂMBITO DA DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO

O DEFENSOR PÚBLICO-GERAL DO ESTADO DO RIO DE JANEIRO, no uso das atribuições que lhe foram conferidas pelo art. 8o, I da Lei Complementar n° 06/77;

Considerando o disposto no art. 48 da Lei n° 13.709/18, que trata do incidente de segurança em matéria de proteção de dados pessoais;

Considerando o disposto no art. 50 , § 2º, da Lei n° 13.709/18, que trata das boas práticas em proteção de dados;

Considerando o disposto no art. 6º, VII e VIII, da Lei n° 13.709/18, que determina o tratamento de dados pessoais de acordo com os princípios da segurança e da prevenção;

Considerando a autonomia administrativa da Defensoria, consagrada no art. 134, § 4º, da CRFB/88;

Considerando o disposto nos arts. 3º, III, e 7º, IV, da Resolução n° 1090/2021;

Considerando o constante do Processo SEI E-020/001.004338/2021;

Considerando que o processo de adequação à LGPD deve se dar de forma continuada, sendo que a elaboração de plano preliminar não afasta a necessidade de aperfeiçoamento do plano;

Considerando a necessidade premente de criação de fluxo para eventual ocorrência de incidente de segurança envolvendo dados pessoais.

RESOLVE:

Art. 1º Aprovar o Plano de Resposta de Incidente de Segurança à Proteção de Dados Pessoais, na forma do anexo.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

Rio de Janeiro, 25 de abril de 2022.

RODRIGO BAPTISTA PACHECO

Defensor Público-Geral do Estado

ANEXO ÚNICO

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

Institui o Plano de Resposta a Incidentes de Segurança no âmbito da Defensoria Pública do Estado do Rio de Janeiro

DISPOSIÇÕES GERAIS

Art. 1º - O presente Plano de Resposta a Incidentes de Segurança contemplará um conjunto de diretrizes para a identificação e detecção de incidentes envolvendo dados pessoais no âmbito da Defensoria Pública do Estado do Rio de Janeiro e comunicação adequada às autoridades responsáveis pela proteção de dados e partes envolvidas.

§ 1o As diretrizes serão divididas em funções que expressem a gestão do risco organizacional e que permitam decisões adequadas para a identificação e detecção de ameaças e a melhor gestão de práticas e de metodologias existentes quanto a comunicação de incidentes.

§ 2o As diretrizes poderão ser adaptadas, incrementadas ou ajustadas considerando a realidade de cada incidente ocorrido e as orientações vindouras da Autoridade Nacional de Proteção de Dados (ANPD) sobre o tema.

Art.2º - Para os fins deste Plano, considera-se incidente de segurança com dados pessoais como qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita que possa ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

CAPÍTULO II

DA GESTÃO DE INCIDENTES DE SEGURANÇA

Art. 3º - A gestão de incidentes de segurança é realizada por meio de processo definido e constituído formalmente.

Art. 4º - Na fase de detecção, caso qualquer membro, servidor, aluno-residente ou estagiário da Defensoria Pública tenha ciência de evento que possa configurar um incidente de segurança, deverá comunicá-lo imediatamente ao órgão Encarregado de Proteção de Dados, endereçando e-mail ou processo administrativo próprio.

Art. 5º - Na fase de detecção, caso qualquer operador tenha ciência de evento que possa configurar um incidente de segurança, deverá comunicá-lo imediatamente à Defensoria Pública do Estado do Rio de Janeiro, enquanto órgão controlador, endereçando e-mail ou processo administrativo próprio.

Art. 6º - Na fase de detecção, caso qualquer interessado tenha ciência de evento que possa configurar um incidente de segurança, poderá comunicá-lo ao órgão Encarregado de Proteção de Dados, endereçando e-mail ou processo administrativo próprio.

Art. 7º - Nas hipóteses dos artigos 4º, 5º e 6º, o comunicante deverá fornecer as seguintes informações:

I – nome, telefone e e-mail;

II - descrição resumida do suposto incidente;

III - motivos pelos quais entende que o suposto incidente tenha relação com a gestão de dados Defensoria Pública;

IV – data do suposto incidente ou data provável, caso não tenha certeza da data;

V – caso o comunicado tenha sido feito somente após 2 (dois) dias a contar da data do suposto incidente, a justificativa pela qual a comunicação não se deu nas primeiras 48 (quarenta e oito) horas posteriores ao fato;

VI - apontamento de dados pessoais dos quais seja titular que o comunicante suspeita tenham sido atingidos pelo incidente, se houver;

VII – se possível for a identificação, o apontamento de dados pessoais de terceiros que o comunicante suspeita tenham sido atingidos pelo incidente, se houver;

VIII – se possível for a identificação, quantidade de titulares de dados pessoais que o comunicante estima tenham sido atingidos pelo incidente;

VIII – se possível for a identificação, a natureza da relação entre os titulares de dados supostamente atingidos com o controlador.

Art. 8º - Caso a comunicação não contenha todos os requisitos previstos no art. 7º desta Resolução, o órgão Encarregado de Proteção de Dados poderá solicitar ao comunicante a complementação das informações no prazo de 24 (vinte e quatro) horas.

Art. 9º - Após verificar o preenchimento dos requisitos do art. 7º desta Resolução, o Encarregado de Proteção de Dados deverá avaliar a veracidade e confirmação da relevância do incidente, e, caso entenda que há elementos suficientes que possam comprovar a possibilidade de vazamento de dados, enviará o procedimento à Secretaria de Tecnologia da Informação e Comunicação, para confirmação do possível vazamento e início da fase triagem, análise e resposta.

Parágrafo único – Caso os fatos não envolvam ataques cibernéticos a sistemas, ativos, dados e a recursos de tecnologia da informação e comunicação, o órgão encarregado encaminhará o procedimento ao Controle Interno para adoção de providências e elaboração de relatório, aplicando-se, no que couber, o artigo 10 desta Resolução.

Art. 10 - A Secretaria de Tecnologia da Informação e Comunicação apresentará parecer sobre a possibilidade de comprovação do incidente reportado, e em caso de confirmação, apresentará relatório do incidente ao órgão Encarregado de Proteção de Dados, no qual deverão constar:

I – a data e hora da detecção do incidente;

II – a data e hora do incidente e sua duração;

III – as circunstâncias em que ocorreu a violação de segurança de dados pessoais (e.g., perda, roubo, cópia, vazamento);

IV – descrição dos dados pessoais e informações afetadas, tais como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados;

V – resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento;

VI - possíveis consequências e efeitos negativos sobre os titulares dos dados afetados;

VI - medidas técnicas de segurança preventivas tomadas;

VII - resumo das medidas técnicas implementadas até o momento para controlar os possíveis danos;

VIII - possíveis problemas de natureza transfronteiriça;

IX - outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

Parágrafo único. A Secretaria de Tecnologia da Informação e Comunicação deverá apresentar relatório com a maior brevidade possível e, de preferência, no prazo indicativo de 1 (um) dia útil, contados da data do conhecimento do incidente, sem prejuízo de posterior complementação.

Art. 11 – Recebido o relatório da Secretaria de Tecnologia da Informação e Comunicação e coletada as demais informações necessárias, o órgão Encarregado de Proteção de Dados comunicará à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante.

§ 1º - A avaliação acerca da relevância do risco ou dano será feita com cautela e em atenção aos princípios da prevenção, responsabilização e prestação de contas, de modo que, em caso de dúvida, a comunicação à ANPD deverá ser realizada.

§ 2º - A comunicação será feita com a maior brevidade possível e, de preferência, no prazo indicativo de 2 (dois) dias úteis, contados da data do conhecimento do incidente, sem prejuízo de posterior complementação.

§ 3º - A comunicação deverá conter as informações exigidas no art. 48, § 1º, da Lei n° 13.709/18 e no formulário de informe de incidentes de segurança da ANPD, incluindo:

I - Identificação e dados de contato da Defensoria Pública do Estado do Rio de Janeiro enquanto entidade controladora e do órgão Encarregado de Proteção de Dados;

II - Indicação se a notificação é completa ou parcial e, em caso de comunicação parcial, indicação se se trata de uma comunicação preliminar ou de uma comunicação complementar;

III - Data e hora da detecção do incidente;

IV - Data e hora do incidente e sua duração;

V - Circunstâncias em que ocorreu a violação de segurança de dados pessoais (e.g., perda, roubo, cópia, vazamento);

VI - Descrição dos dados pessoais e informações afetadas, tais como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados;

VII - Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento;

VIII - Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados;

IX - Medidas de segurança, técnicas e administrativas preventivas tomadas;

X - Resumo das medidas implementadas até o momento para controlar os possíveis danos;

XI - Possíveis problemas de natureza transfronteiriça;

XII - Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

Art. 12 - O órgão Encarregado de Proteção de Dados comunicará aos titulares a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante.

§ 1º - Quando da avaliação da relevância do risco ou dano, deverão ser considerados com maior peso as situações em que o incidente:

I – envolver dados sensíveis ou de pessoas em situação de vulnerabilidade, como crianças e adolescentes; e

II - tiver potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade.

§ 2º - Ainda quando da avaliação da relevância do risco ou dano, deverá ser considerado o volume de dados envolvidos, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados.

§ 3º - A comunicação aos titulares será realizada em prazo razoável e de acordo com as orientações vindouras da Autoridade Nacional de Proteção de Dados (ANPD).

§ 4º - A depender da gravidade do incidente e do número de titulares afetados, o órgão Encarregado de Proteção de Dados poderá recomendar a divulgação do fato no sítio eletrônico, nas redes sociais e em outros meios de comunicação oficiais da Defensoria Pública, bem como a articulação junto à Ouvidoria Externa para informe à sociedade civil.

Art. 13 – Quando cabível, o órgão Encarregado de Proteção de Dados elaborará relatório de impacto sobre o incidente de segurança.

Art. 14 – O resultado da apuração será informado aos titulares dos dados pessoais atingidos pelo incidente.

CAPÍTULO III

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 15 – No prazo de 3 meses a contar da publicação da presente Resolução, a Secretaria de Tecnologia da Informação e Comunicação elaborará protocolos técnicos específicos de prevenção e resposta a incidentes de segurança.

Art. 14 – Os casos omissos serão decididos pelo Defensor Público-Geral.

Art. 16 – A presente Resolução entra em vigor na data da sua publicação.

Documento assinado eletronicamente por **RODRIGO BAPTISTA PACHECO**, **Defensor Público Geral do Estado**, em 26/04/2022, às 13:17, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.rj.def.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0831515** e o código CRC **6C204892**.