Procedimento interno para comunicação de incidentes de segurança envolvendo dados pessoais

I. INTRODUÇÃO

A Secretaria Estadual de Saúde de Pernambuco (SES/PE), por meio da Diretoria Geral de Controle Interno (DGCI), vem orientar acerca das medidas a serem adotadas nos casos de incidente de segurança relacionados a dados pessoais, salientando a possibilidade de responsabilização pela inobservância das normas e procedimentos destinados à proteção dessas informações.

II. DO INCIDENTE DE SEGURANÇA

A Resolução CD/ANPD n° 15/2024, em seu art. 3°, inciso XII, dispõe que incidente de segurança é **"qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais".**

Portanto, um incidente de segurança acontece quando os dados pessoais sofrem violação, como nos casos de vazamento de informações, acessos não autorizados, perda de equipamentos, alteração indevida de registros ou ataques virtuais.

Nesses casos, consoante art. 48 da Lei n° 13.709/2018 (LGPD), quando a ocorrência do incidente de segurança resultar em risco ou dano relevante, é dever do controlador comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados.

Assim, a seção I, da Resolução CD/ANPD n° 15/2024, estabelece critérios que definem a obrigatoriedade de comunicar o incidente, considerando especialmente situações que envolvam dados pessoais sensíveis, dados de crianças e idosos, informações financeiras, dados de autenticação em sistemas, informações protegidas por sigilo legal ou em larga escala.

Desse modo, é fundamental que o órgão registre todos os incidentes detectados, avalie sua gravidade, verifique a necessidade de comunicação do evento e adote as medidas corretivas e mitigadoras cabíveis.

Além disso, nos termos do art. 10 da referida resolução, é dever do controlador manter o registro dos incidentes, inclusive daqueles não comunicados à ANPD e aos titulares de dados.

Nesse contexto, a seguir, explica-se o procedimento interno de comunicação de incidentes, o qual deve ser observado para garantir a conformidade da SES/PE com as normas de proteção de dados pessoais.

III. PROCEDIMENTO INTERNO DE COMUNICAÇÃO DO INCIDENTE

O procedimento interno de comunicação de incidentes visa garantir que tanto o controlador quanto o encarregado sejam cientificados da ocorrência do incidente de segurança, uma vez que são os agentes responsáveis por avaliar a gravidade do evento e propor a adoção das medidas legais cabíveis.

Para melhor compreensão, o fluxograma do procedimento encontra-se no Anexo I deste boletim, devendo ser utilizado como referência prática no cumprimento das etapas descritas.

Assim, o trâmite é iniciado com o gestor da unidade de saúde ou do setor administrativo, que, ao tomar conhecimento do incidente, deve comunicar imediatamente o fato à Diretoria Geral de Controle Interno (DGCI).

A unidade ou setor demandante, ao formalizar a comunicação, deverá apresentar, juntamente com os documentos que considerar pertinentes, **no mínimo, as seguintes informações:**

- Descrição do incidente;
- Identificação dos dados e titulares envolvidos;
- Detalhamento das medidas de segurança já adotadas;
- Indicação de eventual violação de segurança aos sistemas;
- Informação sobre comunicação prévia ao titular, se houver.

Recebida a comunicação, a DGCI procederá ao registro e encaminhará o processo para análise da Coordenação Geral de Proteção de Dados (CGPD). Esta, por sua vez, poderá solicitar informações complementares para a devida apuração do evento.

Concluída a análise, a CGPD elaborará relatório com base nos requisitos da Resolução CD/ANPD nº 15/2024, e que será submetido ao Comitê Técnico de Estudos e Acompanhamento da Política de Proteção de Dados Pessoais Local (CTEA-PPDPL), para apreciação e validação.

Esta fase poderá resultar nos seguintes direcionamentos:

1) Inexistência de incidente: o processo será arquivado e a decisão comunicada à área demandante;

2) Confirmação da ocorrência de incidente: o CTEA validará a conclusão e submeterá para análise da Controladora de Dados, responsável por ratificar a decisão.

Quando necessário, o CTEA poderá encaminhar o caso ao Comitê Gestor de Segurança da Informação (CGSI), para manifestação e eventuais recomendações.

Após validação pela Controladora, o processo retornará à CGPD, que adotará as seguintes providências:

1) **Nos casos em que não haja necessidade de comunicação à ANPD,** o relatório conclusivo será encaminhado à unidade solicitante para ciência e adoção das providências cabíveis, sendo arquivado na CGPD;

2) **Quando houver necessidade de comunicação à ANPD**, além das medidas anteriores, a CGPD, por intermédio do Encarregado, realizará a comunicação à ANPD e aos titulares de dados afetados.

Ressalta-se que, a partir da confirmação da ocorrência de incidente envolvendo dados pessoais, **terá início a contagem do prazo de três dias úteis para conclusão do procedimento e decisão quanto à comunicação ou não do evento à ANPD,** em consonância com os arts. 6º e 9º da Resolução CD/ANPD nº 15/2024.

Portanto, o cumprimento do procedimento exposto possibilita a adequada apuração dos fatos, a adoção de medidas corretivas, bem como a comunicação tempestiva à ANPD e aos titulares de dados, quando for o caso.

III. RESPONSABILIZAÇÃO

A comunicação de incidentes de segurança relacionados a dados pessoais constitui obrigação legal prevista na LGPD e em normas complementares que regulamentam a proteção de dados pessoais.

Nos termos do art. 17, § 1°, da Resolução CD/ANPD nº 15/2024, a Autoridade Nacional de Proteção de Dados poderá instaurar processo administrativo sancionador em face do controlador para apurar eventual falha no cumprimento da obrigação de comunicação.

No âmbito da SES/PE, para mitigar tais falhas, implementou-se a Política de Proteção de Dados Pessoais Local (PPDPL), que tem por finalidade estabelecer princípios, diretrizes e responsabilidades mínimas para a proteção dessas informações.

Nesse sentido, a PPDPL dispõe, em seu art. 2°, que todas as pessoas que realizam algum tratamento de dados pessoais sob a tutela da Secretaria — inclusive operadores atuando em seu nome — devem observar rigorosamente a política, bem como as normas complementares, manuais e procedimentos internos.

Ademais, os arts. 11 e 22 da referida política reforçam esse dever, atribuindo aos gestores de processos e aos operadores a responsabilidade de cumprir as orientações emitidas por esta Secretaria.

Sendo assim, a omissão ou o descumprimento do procedimento de comunicação de incidentes configura infração normativa, podendo ocasionar a responsabilização dos agentes nas esferas cível, penal e administrativa, além de comprometer a conformidade do órgão perante à LGPD.

IV. CONCLUSÃO

Em suma, a adoção do procedimento interno de comunicação de incidentes fortalece a governança de proteção de dados pessoais da SES/PE, assegura a conformidade com a LGPD e contribui para mitigar riscos de responsabilização e danos reputacionais.

Assim, é essencial que todos os envolvidos no tratamento de dados pessoais observem o procedimento descrito neste boletim **e no fluxograma constante do Anexo I.**

Por fim, em caso de dúvidas, sugestões ou outros comentários, a Diretoria Geral de Controle Interno está à disposição pelo e-mail: encarregado.lgpd@saude.pe.gov.br.

Anexo I – Fluxograma do Procedimento Interno de Comunicação do Incidente de Segurança