GUIA SOBRE INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS PARA O MINISTÉRIO PÚBLICO BRASILEIRO

1. A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece que os agentes de tratamento de dados pessoais (controladores e operadores) devem adotar "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (art. 46).

2. O incidente de segurança com dados pessoais é um evento adverso confirmado que compromete os atributos de confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais, independentemente do meio em que estão armazenados (físico ou digital).

3. Esses incidentes podem ocorrer de forma **acidental**, como no envio de informações a destinatário incorreto e na divulgação não intencional de dados de titulares, ou por **atos intencionais**, como a invasão de sistema de informação por pessoa não autorizada, o sequestro de dados (*ransomware*) ou o furto de um dispositivo de armazenamento de dados.

4. A simples existência de uma vulnerabilidade em sistemas não configura, por si só, um incidente de segurança. No entanto, a exploração dessa vulnerabilidade pode gerar um incidente, o que impõe ao agente de tratamento o dever de identificar, avaliar e tratar riscos de incidentes em suas operações. Além disso, nem todo incidente de segurança da informação envolve dados pessoais. Incidentes que afetem apenas dados anonimizados ou não vinculados a pessoas naturais identificadas ou identificáveis não estão sujeitos às normas de proteção de dados pessoais.

5. Nos casos em que o incidente de segurança com dados pessoais puder acarretar "**risco ou dano relevante aos titulares**", a LGPD estabelece que o controlador deverá comunicar a ocorrência do incidente à autoridade nacional e aos titulares afetados (art. 48). Se o incidente envolve ramos e unidades do Ministério Público, a comunicação deve ser feita à Unidade Especial de Proteção de Dados Pessoais do Conselho Nacional do Ministério Público (UEPDAP/CNMP), conforme prevê o art. 148 da Resolução CNMP n. 281, de 12 de dezembro de 2023.

6. Essa comunicação deve ser realizada pelo Encarregado ou por um representante do controlador, sempre que possível, no **prazo de até 72 (setenta e duas) horas** a partir de quando tomou conhecimento do incidente, por meio do formulário eletrônico disponível na página da UEPDAP/CNMP na internet.

7. Excepcionalmente, caso as informações completas do incidente ainda não estejam disponíveis nesse prazo, a comunicação à UEPDAP/CNMP poderá ser realizada em duas etapas: **preliminar**, no prazo de 72 horas, e **complementar**, no prazo de 20 (vinte) dias úteis, a contar da data da comunicação preliminar.[1]

8. A comunicação voluntária do incidente demonstra transparência, cooperação e boa-fé por parte do agente e será considerada em eventual ação de fiscalização da UEPDAP/CNMP. Por outro lado, a omissão ou atraso injustificado na comunicação pode sujeitar os agentes às sanções previstas na legislação.

9. A fim de avaliar se o incidente representa risco ou dano relevante para fins de comunicação à UEPDAP/CNMP e aos titulares, devem ser considerados os elementos previstos no art. 5º do Regulamento de Comunicação de Incidente de Segurança da ANPD. De acordo com essa norma, o risco ou dano é considerado relevante quando "puder afetar significativamente interesses e direitos fundamentais dos titulares", conforme definição do §1º,[2] 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.[3]

10. Um mesmo tipo de incidente pode ou não ser considerado capaz de causar risco ou dano relevante em função da combinação desses critérios. Por exemplo, no roubo de um dispositivo eletrônico, a avaliação de relevância vai depender do tipo de dado armazenado, do contexto da atividade de tratamento e do fato de os dados estarem ou não protegidos por criptografia. Da mesma forma, a relevância de incidentes com credenciais (dados de autenticação em sistemas) dependerá de fatores como o tempo de

---

[1] Art. 6º, §3º do Regulamento de Comunicação de Incidente de Segurança da ANPD, aprovado pela Resolução CD/ANPD nº 15, de 24 de abril de 2024, aplicável subsidiariamente à Resolução CNMP n. 281, de 12 de dezembro de 2023, conforme deliberação adotada em reunião da UEPDAP/CNMP realizada em 29/08/2024 (ATA n° 05/2024/UEPDAP).

[2] § 1º 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.

[3] § 2º Considera-se incidente com dados em larga escala aquele que abranger número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares.

validade das credenciais, se houve efetivo acesso ao sistema pelo usuário naquele período e os tipos de dados acessados, conforme registros disponíveis (*logs*).

11. Para facilitar a análise de relevância do incidente, na forma do art. 5º do Regulamento de Comunicação de Incidente de Segurança da ANPD, a UEPDAP/CNMP disponibiliza essa planilha.

12. A comunicação aos titulares, quando cabível, deve ser realizada o mais breve possível, para que eles possam mitigar eventuais impactos negativos decorrentes do incidente. A comunicação deve ser feita em linguagem simples e de fácil entendimento e, sempre que possível, de forma individual e diretamente aos titulares por quaisquer meios disponíveis, tais como e-mail, SMS, carta ou mensagem eletrônica e, preferencialmente, através do canal já habitualmente utilizado pelo agente para se comunicar com o titular. Excepcionalmente, e de forma justificada, admite-se a comunicação indireta, por meio de publicações na internet ou outros canais amplos, com o devido destaque.

13. A UEPDAP/CNMP espera que estas orientações contribuam para maior clareza e segurança no processo de gestão e comunicação de incidentes com dados pessoais, a fim de que se tenha uma análise mais precisa da eficácia das medidas de segurança adotadas para proteção de dados pessoais nos ramos e unidades do Ministério Público brasileiro.