

Comunicação de incidentes de segurança: o passo a passo definitivo de acordo com o regulamento da ANPD

27.04.2024 4 minutos de leitura

Autores

Felipe Palhares

Fernanda Villela

Quando se trata de segurança da informação, a máxima popular reflete uma realidade incontornável: um incidente de segurança não é uma questão de “se” acontecerá, mas sim de “quando” acontecerá.

Áreas relacionadas

Proteção de Dados e
Cybersecurity

Das violações mais simples – como o envio de um e-mail ao destinatário errado – às mais desafiadoras – como um ataque de ransomware com exfiltração de dados pessoais – fato é que organizações ao redor do mundo sofrem incidentes de segurança todos os dias indiferentemente das medidas de segurança que tenham sido implementadas previamente.

Assuntos

Proteção de Dados e
Cybersecurity

COMO SE PROTEGER DE ATAQUES CIBERNÉTICOS?

Por melhores que sejam as ferramentas tecnológicas adotadas por uma organização, sejam de hardware ou de software, ou as medidas administrativas e organizacionais tomadas, como o treinamento constante de seus empregados, não há como garantir que um incidente de segurança nunca ocorrerá, especialmente no atual cenário global, com a propagação de grupos criminosos focados única e exclusivamente na prática de delitos virtuais.

Em 2024, ataques cibernéticos sofisticados não são mais atos perpetrados somente por criminosos altamente especializados e com conhecimentos técnicos profundos. Modelos de negócio como o de *ransomware-as-a-service*, no qual o malware é desenvolvido por um criminoso e depois ofertado para ser utilizado por terceiros, inclusive por pessoas sem qualquer conhecimento prévio, ampliam exponencialmente a probabilidade de incidentes de segurança ocorrerem.

Um dos pontos centrais normalmente previsto em leis de privacidade e proteção de dados é justamente o estabelecimento de obrigações de comunicação de incidentes de segurança a órgãos reguladores e aos titulares de dados afetados. Com a Lei Geral de Proteção de Dados Pessoais (LGPD) não foi diferente.

AS LACUNAS DA LGPD E A RESOLUÇÃO CD/ANPD 15/2024

Contudo, a LGPD deixou diversas lacunas a respeito da comunicação de incidentes de segurança, provocando insegurança jurídica a controladores de

dados pessoais que sofreram incidentes desde a sua entrada em vigor, em 18 de setembro de 2020.

A partir de agora, com a edição da Resolução CD/ANPD nº 15/2024 e a aprovação do Regulamento de Comunicação de Incidentes de Segurança (Regulamento), esses vazios passam a ser preenchidos com mais clareza, com a definição de prazos de comunicação, critérios para identificação de incidentes relevantes e estipulação de obrigações acessórias aos controladores de dados em aspectos de governança e prestação de contas.

Este e-book traz tudo que você precisa saber sobre a comunicação de incidentes de segurança de acordo com as disposições do Regulamento, em detalhes, de forma prática, com um passo a passo do que fazer na hora da resposta a um incidente.

CONFIRA OS PONTOS ABORDADOS NA PUBLICAÇÃO:

- Incidentes de segurança com dados pessoais envolvem a quebra de um (ou mais) dos pilares de segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade.
- Devem ser comunicados, tanto à ANPD quanto aos titulares afetados, os incidentes de segurança envolvendo dados pessoais que possam resultar em risco ou dano relevante aos titulares.
- A comunicação deve ser realizada em até 3 dias úteis, contados da data do conhecimento de que o incidente afetou dados pessoais. O prazo é aplicável tanto para a comunicação à ANPD, quanto para a comunicação aos titulares. Agentes de tratamento de pequeno porte possuem este prazo em dobro.
- A comunicação aos titulares deve ocorrer de forma direta e individualizada.
- A comunicação pode ser complementada com informações adicionais no prazo de 20 dias úteis, contados da data da comunicação anterior, de maneira fundamentada.
- Além da comunicação espontânea, a ANPD poderá instaurar procedimento de apuração de incidente de segurança quando tomar conhecimento de incidente não comunicado pelo controlador.
- Como regra geral, a comunicação não é coberta por sigilo, cabendo ao controlador realizar essa solicitação à ANPD, de maneira fundamentada.
- Ainda que um determinado incidente de segurança não seja comunicado, em razão de não ser verificado risco ou dano relevante aos titulares, é obrigação do controlador manter um registro de todos os incidentes sofridos pelo prazo de 5 anos.
- O controlador deve gerar evidências sobre o tratamento que foi conferido ao incidente de segurança, documentando os trabalhos realizados e as decisões tomadas na resposta ao evento adverso.
- A ANPD poderá divulgar, em seu sítio eletrônico, informações relativas a incidentes de segurança reportados.

Profissionais que aliam visão jurídica e visão de mercado



Felipe Palhares



Fernanda Villela