L.O. BAPTISTA

BOAS PRÁTICAS
COMUNICAÇÃO DE INCIDENTES

2ª edição

QUAL É A DEFINIÇÃO DE INCIDENTE DE SEGURANÇA?

Conforme a Resolução CD/ANPD n. 15/24, um incidente de segurança é qualquer evento adverso confirmado, relacionado à violação das propriedades de **confidencialidade, integridade, disponibilidade e autenticidade** da segurança de dados pessoais.

Cabe ao **controlador** identificar as situações que caracterizam um incidente de segurança a afetar suas operações de tratamento de dados pessoais, levando-se em consideração os seguintes pontos indicados pela ANPD:

Incidentes que envolvam somente dados anonimizados ou que não estejam relacionados a pessoas naturais identificáveis não precisam ser comunicados à ANPD.

Pode decorrer de ações voluntárias (como a invasão de um sistema de informação ou o furto de um dispositivo de armazenamento de dados) ou de ações acidentais (como o envio de informações para o destinatário incorreto) que resultem em divulgação, alteração, perda indevidas ou acessos não autorizados a dados pessoais, independentemente do meio em que estão armazenados.

A mera existência de uma vulnerabilidade em um sistema de informação não constitui um incidente de segurança. Contudo, a exploração dessa vulnerabilidade, pode resultar em um incidente.

COMO COMUNICAR UM INCIDENTE À ANPD?

O encarregado pela proteção de dados (ou um representante legal constituído pelo controlador) comunica a autoridade através de um formulário próprio a ser protocolado eletronicamente na plataforma de Peticionamento Eletrônico do SUPER.BR (Sistema Único de Processo Eletrônico em Rede) gerando um Recibo Eletrônico de Protocolo.

A ANPD disponibiliza manuais e instruções específicos para que este cadastro seja realizado de maneira correta e eficiente.

Acesse o formulário aqui

QUAIS INCIDENTES DEVEM SER COMUNICADOS?

Os controladores devem informar à ANPD e aos titulares de dados qualquer incidente de segurança que possa acarretar risco ou dano relevante, que envolva o tratamento de, pelo menos, um desses tipos de dados pessoais:

- Dados pessoais sensíveis
- Dados de crianças, adolescentes ou idosos
- Dados financeiros
- Dados de autenticação em sistemas
- Dados protegidos por sigilo legal, judicial ou profissional
- Dados pessoais em larga escala

Isso inclui situações que possam impedir o exercício de direitos dos titulares ou causar danos materiais ou morais, como discriminação, violação à integridade física, fraudes financeiras ou roubo de identidade, conforme exemplos divulgados pela própria ANPD.

AVALIAÇÃO DE RISCO DE UM INCIDENTE COM DADOS PESSOAIS

A ANPD sinaliza alguns aspectos que devem ser levados em consideração para avaliação do risco (que possam causar danos materiais ou morais aos titulares):

- O contexto da atividade de tratamento de dados pessoais.
- As categorias e quantidades de titulares afetados.
- Os tipos e quantidade de dados pessoais violados.
- Os potenciais danos materiais, morais, reputacionais causados aos titulares.
- Os dados violados estavam protegidos impossibilitando a identificação dos titulares.
- As medidas de mitigação adotadas pelo controlador após o incidente.

Estes pontos destacam a postura proativa da ANPD em promover a segurança da informação e a proteção de dados pessoais, enfatizando a responsabilidade das organizações em adotar medidas de **compliance digital e cibersegurança** eficazes e uma comunicação transparente em caso de incidentes.

A ANPD poderá publicar orientações com o objetivo de auxiliar os agentes de tratamento na avaliação do incidente que possa acarretar risco ou dano relevante aos titulares.

e-Book

Compliance digital e Cibersegurança

DOWNLOAD

QUAL O PRAZO PARA COMUNICAÇÃO DO INCIDENTE?

Comunicação Completa ou Preliminar

A ANPD recomenda que a comunicação seja feita o mais breve possível, em até 3 dias úteis da ciência do fato com o intuito de preservar os direitos dos titulares e diminuir os prejuízos.

Comunicação Complementar

A comunicação preliminar poderá ser complementada em até 20 dias úteis, caso o controlador não disponha de informações completas a respeito do incidente ou não conseguir notificar a todos os titulares no prazo recomendado.

Prazo em dobro

Os agentes de tratamento de pequeno porte terão os prazos contados em dobro para realização do CIS.

A demora injustificada em comunicar o incidente será considerada um agravante!

Além disso, **o controlador deverá manter o registro do incidente de segurança, inclusive daquele não comunicado à ANPD e/ou aos titulares**, pelo prazo mínimo de cinco anos, contado a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

PAPEL DO OPERADOR NO PROCESSO DE COMUNICAÇÃO DE INCIDENTES

- Obrigação legal de comunicar o incidente de segurança aos titulares e à ANPD.
- Obrigação de adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais se estende a todos os agentes de tratamento de dados, inclusive aos operadores.

COMO COMUNICAR OS INCIDENTES AOS TITULARES

A ANPD enfatiza que a obrigação do art. 48 da LGPD não se cumpre com a mera comunicação do incidente de segurança à autoridade, sendo que na hipótese de risco ou dano relevante, o controlador deve, necessariamente, comunicar o ocorrido aos titulares dos dados pessoais violados no incidente.

Esta comunicação deve ser feita de forma individual e diretamente aos titulares por quaisquer meios (tais como e-mail, SMS, carta ou mensagem eletrônica), se não for possível individualizar os titulares afetados, pode ser necessário comunicar a todos cujos dados pessoais estejam presentes na base de dados violada e em alguns casos excepcionais por publicação em meios de comunicação. Informações mínimas podem ser encontradas na página ao lado.

Resumo e data da ocorrência do incidente

Descrição da natureza e categoria dos dados pessoais afetados

Riscos e consequências aos titulares de dados

Medidas técnicas e de segurança utilizadas pelo controlador para a proteção dos dados, observados os segredos comercial e industrial

Os motivos da demora, no caso de a comunicação não ter sido feita no prazo estabelecido pela ANPD

Medidas que foram ou serão utilizadas pelo controlador para reverter ou mitigar os efeitos do incidente aos titulares, se cabíveis

Dados de contato do encarregado do controlador para que os titulares possam solicitar informações adicionais a respeito do incidente.

O QUE ACONTECE APÓS A COMUNICAÇÃO DO INCIDENTE?

A Coordenação-Geral de Fiscalização (CGF) da ANPD recepciona a comunicação para avaliação da gravidade que poderá acarretar o arquivamento ou a aplicação de sanções administrativas previstas na LGPD.

Além disso a CGF poderá aplicar medidas preventivas e sanções se constatar que o controlador não cumpriu os seguintes passos:

- Não comunicar o incidente à ANPD e aos titulares em tempo razoável;
- Não comunicar o incidente aos titulares de dados pessoais afetados;
- Não adotar medidas de segurança técnicas e administrativas compatíveis aos riscos de suas atividades de tratamento de dados pessoais.

> A equipe de Privacidade e Proteção de Dados de L.O. Baptista Advogados está preparada para atender empresas na assessoria jurídica a novos negócios digitais, privacidade de dados pessoais, segurança da informação, startups, mídias, entretenimento e propriedade intelectual, sempre oferecendo excelência e soluções inovadoras a seus clientes. Estamos à disposição!

Autoria de: Denise de Araujo Berzin Reupke e Carolina Britski Puga

CONTATO

Esther Jerussalmy Cunha
Sócia
ejc@baptista.com.br

Fabrício B. Pasquot Polido
Sócio
fbp@baptista.com.br

L.O. BAPTISTA

Avenida Paulista, 1294 - 8° andar
São Paulo - SP | Brasil | +55 3147 0800

São Paulo, maio de 2024