Q&A

COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA

Indo além da Resolução nº 15/24 - ANPD

Direito,
Inovação
& Tecnologia

www.vlklaw.com.br

Perguntas Frequentes

1. Qual é o prazo para comunicação de incidentes de segurança à ANPD e aos titulares?

A LGPD prevê que a comunicação à ANPD e aos titulares será feita em prazo razoável. A Resolução 15/ANPD (“Resolução”) trouxe o prazo de 3 dias úteis para ambas as situações, exceto em caso de lei específica ou regulação setorial que preveja outro prazo. Caso a comunicação à ANPD seja preliminar, deverá ser complementada no prazo de 20 dias úteis. Agentes de Tratamento de Pequeno Porte possuem prazos em dobro.

2. Quando tem início a contagem do prazo para comunicação de incidentes de segurança à ANPD e aos titulares?

De acordo com a Resolução, o prazo começa a ser contado do “conhecimento pelo controlador de que o incidente afetou dados pessoais”. Desde que devidamente documentado, esse marco inicial poderá ser diferente da data em que se tomou conhecimento do incidente e até em momento diverso de quando foi identificado o comprometimento de dados pessoais. Explicamos:

Veja exemplo a seguir: **(i)** organização tomou conhecimento de incidente de segurança no dia 05/01; **(ii)** no dia 11/01 a empresa identifica o comprometimento de dados cadastrais, que não trazem risco ou dano relevante; **(iii)** no dia 18/01 é confirmado que dados sensíveis e financeiros de crianças foram objeto do incidente podem trazer risco ou dano relevante. Nessa situação, apesar de o incidente ter sido identificado no início de janeiro e confirmado o comprometimento de dados pessoais no dia 11, desde que devidamente documentado, é possível sustentar que o prazo de 3 dias úteis para comunicação à ANPD e aos titulares se iniciará em 18/01.

Diante disso, recomendamos **elaborar/revisar o Plano de Resposta a Incidentes de Segurança da Informação**, deixando-o aderente à realidade da sua organização e à nova Resolução, testando-o na prática, por meio de **Simulações de Incidentes.**

3. Quais eventos devem ser comunicados?

A LGPD prevê que devem ser comunicados incidentes de segurança que possam acarretar risco ou dano relevante aos titulares. A Resolução esclareceu 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”.

Complementando esse conceito, o artigo 46 da LGPD especifica que “os agentes de tratamento 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”.

É importante diferenciar esses incidentes daqueles reportados por pesquisadores de falhas e bugs, que ao informarem vulnerabilidades para uma companhia ficam sujeitos a regras específicas dentro do **Programa de Recompensas** (“*Bug Bounty Program*”).

Essa iniciativa é vista como forma de elevar a segurança dos sistemas, pois permite a correção de falhas e traz impactos reduzidos aos titulares de dados e à organização, e, dependendo contexto, é possível sustentar tese de que não obrigam a comunicação à ANPD e aos titulares eventualmente afetados. Para tanto, é fundamental que a documentação do programa seja completa e coerente e inclua clara informação sobre a não divulgação de informações sobre os titulares e a vulnerabilidade.

Ainda, nestes casos, são comuns dúvidas sobre como efetivar a transferência dos valores ao Pesquisador, como identificar essas recompensas no Balanço da empresa, entre outros pontos específicos desse tipo de prática a serem definidos nas regras internas do Programa.

4. Como se faz a análise de risco ou dano potencial? O que representa risco ou dano relevante?

A Resolução, em seu art. 5º, trouxe critérios objetivos para a análise de risco ou dano relevante de um incidente de segurança. Em nossa visão, o primeiro ponto a se confirmar é se o incidente envolve pelo menos um dos seguintes tipos de dados:

- Sensíveis;
- De crianças, adolescentes ou idosos;
- Financeiros;
- De autenticação em sistemas;
- Credenciais de acesso ou de confirmação da identidade;
- Protegidos por sigilo legal, judicial ou profissional; **OU**
- Em larga escala - Importante observar a documentação da Consulta Pública sobre esse tema, que foi disponibilizada pela ANPD.

Em se estando diante de uma das situações acima, é preciso confirmar que o incidente afeta significativamente interesses e direitos fundamentais, isto é: **(i)** impede o exercício de direito ou o uso de um serviço; e/ou **(ii)** ocasiona danos morais ou materiais (discriminação, violação à integridade física ou à imagem; ou fraude financeira).

Se preenchidos esses 2 blocos (tipos de dados **E** direitos fundamentais), então se estará diante de alto risco ou dano relevante, que demandará a comunicação à ANPD e aos titulares. É fundamental, portanto, estruturar **metodologia** fundamentada para **calcular o risco**, documentando o resultado em Relatório.

Quando puder afetar **significativamente** interesses e direitos fundamentais dos titulares:

(i) A atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço;
OU
(ii) Ocasionar danos materiais ou morais aos titulares (tais como a discriminação, violação à reputação, fraudes financeiras ou roubo de identidade).

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 (tabela ANPD - valor do nº de titulares, volume médio dos dados, duração do tratamento em anos, frequência do tratamento, extensão geográfica).

Além desses critérios, é uma boa prática conduzir essa análise por meio de matriz de impacto e probabilidade dos riscos envolvidos, sendo importante destacar que a análise deve ser realizada caso a caso, levando em consideração as circunstâncias do incidente, pois a mudança em uma característica pode afetar toda a análise de risco.

5. Na prática, quem a organização deve reunir para a análise do risco ou dano potencial?

Cada incidente possui características únicas e poderá envolver áreas diferentes na organização, além do próprio Encarregado, de acordo com as necessidades específicas. Em linhas gerais, estas áreas são envolvidas:

- Segurança/Tecnologia da Informação;
- Jurídico/Compliance;
- Relações Públicas/Comunicação;
- Recursos Humanos (se envolver dados de funcionários); e
- Atendimento ao Consumidor (se envolver clientes).

Adicionalmente, é relevante contar com assessorias técnicas externas, especialmente peritos forenses e consultorias especializadas em incidentes de segurança com dados pessoais. Tudo isso deve constar do **Plano de Resposta a Incidentes,** que deve ser atualizado com frequência, reproduzindo a realidade da companhia.

6. Quem deve comunicar incidentes de segurança?

O controlador, por meio de representante legal ou do Encarregado, nas situações de incidente de segurança da informação confirmado, em que houver risco ou dano relevante aos titulares. Essa comunicação à ANPD, quando feita pelo **Encarregado**, deverá **demonstrar a existência de vínculo contratual, empregatício ou funcional**. Se por meio de representante legal, mediante procuração – a documentação comprobatória deve ser apresentada.

Assim, é relevante revisar **contratos com terceiros** que estejam envolvidos em tratamentos de dados relevantes em nome da sua organização ou conjuntamente com ela para garantir a inclusão de cláusulas que regulem o processo de reporte de incidente de segurança, caso ocorra.

Grande parte dos incidentes, contudo, ocorre no âmbito do tratamento de dados por terceiros, seja em nome do controlador ou conjuntamente com ele. Assim, fazer a ***due diligence*** **desses terceiros,** antes da contratação é medida altamente recomendável para mitigar riscos e o impacto de incidentes de segurança, bem como para demonstrar responsabilidade e prestação de contas perante a ANPD.

7. O que deve conter na comunicação de um incidente de segurança a ANPD?

A comunicação deverá ser feita por meio de formulário disponibilizado pela ANPD e deverá conter, no mínimo o(a)(s):

- **Descrição da natureza** e categoria dos dados afetados;
- **Número de titulares afetados** (especificando os vulneráveis);
- Medidas **técnicas de segurança utilizadas** (antes, durante e após o incidente);
- Riscos do incidente e possíveis impactos aos titulares;
- **Data da ocorrência;**
- Dados do Encarregado;
- Identificação do **controlador e do operador**;
- Descrição do incidente e **causa principal**;
- **Total de titulares** cujos dados são tratados nas atividades de tratamento afetadas pelo incidente;
- **Motivos da demora**, caso a comunicação não tenha sido realizado no prazo previsto de três dias úteis; e
- **Medidas** que foram ou serão adotadas **para reverter ou mitigar os efeitos do incidente** sobre os titulares, quando cabíveis.

8. E se a empresa não tiver ciência de todos os elementos para a comunicação inicial completa à Autoridade?

Deve ser apresentada comunicação preliminar, a ser complementada, de maneira fundamentada, no prazo de 20 dias úteis, a contar da data da comunicação inicial.

Assim, se, após os 3 dias iniciais, ainda houver dúvida sobre o risco do incidente, é possível realizar comunicação preliminar à ANPD para garantir relação de transparência e confiança com a autoridade.

9. O que deve conter na comunicação aos titulares?

A comunicação deve conter basicamente as mesmas informações constantes na questão 7 acima, com alguns ajustes específicos. Adicionalmente, deve ser informada a data de conhecimento do incidente e deve ser indicado o contato para obtenção de informações e, quando aplicável, os dados de contado do Encarregado.

Essa comunicação deve ocorrer de forma direta e individualizada e usar linguagem simples e de fácil entendimento, caso seja possível identificar os titulares. Assim, a aplicação de técnicas de ***legal design*** **e** ***visual law*** são recomendáveis a depender do caso.

10. Quais documentos a ANPD pode solicitar?

Além dos documentos comprobatórios, a ANPD poderá requisitar: Mapeamento das Atividade de Tratamento de Dados; e Relatório de Impacto à Proteção de Dados Pessoais e o Relatório de Tratamento do Incidente. De acordo com a Resolução sobre o Processo de Fiscalização e do Processo Administrativo Sancionador (CD/ANPD nº 01/2021), a ANPD ainda poderá requisitar quaisquer documentos que sejam relevantes para a investigação.

11. Como deve ocorrer a atuação pela ANPD?

A ANPD poderá iniciar o processo de fiscalização do incidente de segurança, a partir da comunicação do incidente por iniciativa do agente de tratamento ou de ofício.

Após receber a comunicação, a ANPD poderá determinar a ampla divulgação do incidente às expensas do controlador (que não se confunde com a sanção de publicização); e medidas para reverter ou mitigar os efeitos do incidente. A ANPD também poderá determinar a adoção de medidas imediatas de prevenção, mitigação ou reversão de riscos do incidente, mesmo sem a manifestação do controlador.

A ANPD analisar os incidentes comunicados de forma agregada, ou seja, não específica, com providências padronizadas, conforme os planejamentos da Autoridade para a fiscalização.

12. Quais são as possíveis sanções?

Todas as sanções administrativas da LGPD podem ser aplicadas pela ANPD, sem prejuízo de eventual responsabilização na esfera judicial, por agências reguladoras setoriais ou entidades do sistema de defesa do consumidor.

13. Quais são as hipóteses de extinção do processo de comunicação de incidente de segurança?

De acordo com o a Resolução, o processo será declarado extinto pela ANPD se:

- **(i)** não houver evidências suficientes da ocorrência do incidente;
- **(ii)** se a ANPD entender que o incidente não pode causar risco ou dano relevante;
- **(iii)** o incidente não envolver dados pessoais;
- **(iv)** se tiverem sido tomadas as medidas de mitigação e reversão; ou
- **(v)** se os titulares tiverem sido comunicados e todas as providências necessárias tiverem sido realizadas.

14. O que é o registro do incidente?

O registro do incidente de segurança deverá conter, no mínimo o(a)(s):

- **(i)** Data de conhecimento do incidente;
- **(ii)** Descrição geral das circunstâncias em que o incidente ocorreu;
- **(iii)** Natureza e a categoria de dados afetados;
- **(iv)** Número de titulares afetados;
- **(v)** Avaliação do risco e os possíveis danos aos titulares;
- **(vi)** Medidas de correção e mitigação dos efeitos do incidente, quando aplicável;
- **(vii)** Forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e
- **(viii)** Motivos da ausência de comunicação, quando for o caso.

Esse registro deve ser mantido pelo controlador, pelo prazo mínimo de 5

anos, contados a partir da data do registro, independentemente de ter sido considerada necessária a comunicação à ANPD e aos titulares.

Para fins de transparência e prestação de contas, mesmo nos casos em que a comunicação não é necessária, o registro deve ser realizado para formalizar a ocorrência e quais medidas foram adotadas pela companhia.

15. Quais ações são recomendadas para tornar o processo de comunicação o mais efetivo e menos custoso possível?

Medida essencial é realizar simulações de crises cibernéticas: ao simular incidentes e avaliar o processo de resposta já em vigor, as empresas fortalecem significativamente sua capacidade de lidar de maneira eficaz com situações reais. De acordo com dados da IBM (2023), organizações com alto nível de maturidade em resposta a incidentes economizaram, em média, US$ 1,49 milhão em comparação com as que apresentam baixo nível.

Os colaboradores da empresa devem ser treinados para lidar com essas situações, o que pode ser realizado por meio da simulação de incidentes, para maior efetividade.

Além disso, é recomendável preparar os documentos que podem ser solicitados pela ANPD, a começar: pelo **registro dos tratamentos de dados pessoais** (mapeamento dos dados), bem conduzido e atualizado; eventuais **Testes de Balanceamento** para embasar o uso da base legal do legítimo interesse; e **Relatórios de Impacto à Proteção de Dados.**

16. Quais são os principais pontos de atenção que a ANPD tem visto na comunicação de incidentes e que podem causar medidas repressivas?

Pelo que temos observado de representantes da ANPD, os seguintes pontos principais devem ser observados na comunicação de incidentes de segurança:

- **(i)** Entender a causa raiz do incidente;
- **(ii)** Levar informações completas e de forma proativa, com o máximo de transparência possível; e
- **(iii)** Apresentar todos os detalhes técnicos, incluindo ativos e dados afetados, registro de logs, documentos e políticas, relatórios forenses e medidas implementadas após o incidente.

Assim, é fundamental possuir maturidade que leve à obtenção de todas essas informações com rapidez e eficiência, permitindo fornecer dados mais detalhados e com segurança à ANPD, caso um incidente ocorra.

17. Para além da comunicação à ANPD e aos titulares, quais outras medidas a organização tenderá a tomar em um cenário de incidente de segurança?

A depender do incidente e do tipo de indústria envolvidos, algumas medidas deverão ser tomadas e servirão de apoio tanto para a comunicação à ANPD,

quanto para atividades futuras. Dentre elas, podemos ressaltar a preservação de evidências; a verificação da apólice de seguro e notificação de sinistro; análise de contratos estratégicos e prazos de comunicação entre clientes; contratação de ferramentas de monitoramento da *surface*, *deep* e *dark web;* comunicado reativo à imprensa. Como boa prática, todas medidas devem ser alinhadas em comitê específico que trate do incidente, com participação e colaboração de todos os envolvidos.

Lembretes!

A ANPD já esclareceu que o incidente por si só não gera penalidades. O que pode gerar sanção é a empresa estar com sistema de segurança inadequado em relação ao risco que o tratamento de dados representa ou a falta de comunicação quando o incidente se enquadra nos requisitos da Resolução. Assim, nem todo incidente gera sanção!

Se o incidente envolver dados pessoais com aplicabilidade de leis de outros países ou regiões, o alinhamento de estratégia com profissionais daqueles locais é fundamental.

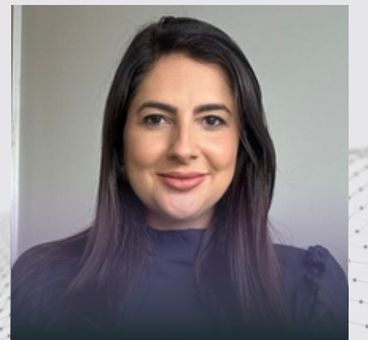
Não existe comunicação excessiva à ANPD. Na dúvida, é recomendável comunicar!

Informações fornecidas à ANPD podem incluir segredos de negócio, mas se transfere à ANPD a responsabilidade de proteger essas informações. Assim, será necessário solicitar o sigilo para os trechos específicos, fundamentando com os motivos que o caracteriza como parte do segredo de negócio da empresa.

Nem todo incidente ocorre no ambiente digital! Exemplo é a perda de pasta física contendo documentos médicos de aluno em uma escola.

Autores

Caio Lima
caio@vlklaw.com.br

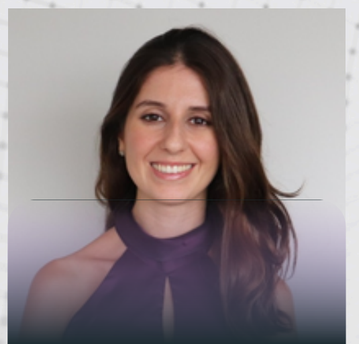


Alexandra Krastins
alexandra.lopes
@vlklaw.com.br

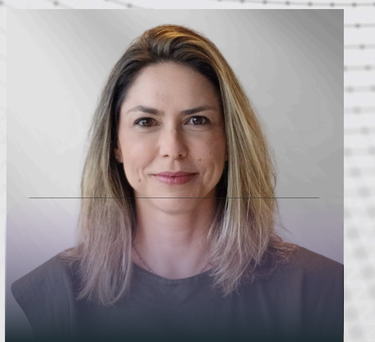
Bruna Bigas
bruna.bigas
@vlklaw.com.br

Jean Santana
jean.santana
@vlklaw.com.br

Mateus Lamonica
mateus.lamonica
@vlklaw.com.br



Nuria Baxauli
nuria.baxauli
@vlklaw.com.br



Verônica Barros
veronica.barros
@vlklaw.com.br

Direito,
Inovação
& Tecnologia

Avenida Paulista, 2073, 22º andar
Conjunto Nacional, Horsa 1
Tel.: (11) 3171-0089
www.vlklaw.com.br