Onde o **Direito**
impulsiona a **inovação**

E-BOOK

Comunicação de Incidentes de Segurança

2ª Edição Atualizada

- Infográficos interativos atualizados
- Q&A ampliado sobre a Resolução CD/ANPD nº 15/2024
- Novas orientações da ANPD: Notas Técnicas, fiscalização e sanções
- Checklist de sigilo e comunicações no SEI
- Documentos mais solicitados pela ANPD em incidentes
- Tendências regulatórias e jurisprudenciais em segurança da informação

Junho de 2026

VLK Direito, Inovação & Tecnologia

www.vlklaw.com.br

Onde o **Direito**
impulsiona a **inovação**

Sumário:

VLK Direito, Inovação & Tecnologia

1

Apresentação

Apresentação:

Este material, dinâmico e interativo, apresenta análise profunda e atual do tema, com o objetivo de orientar empresas na gestão de incidentes, garantindo conformidade, mitigando riscos aos titulares e fortalecendo as estratégias de governança em proteção de dados.

O E-book aborda os incidentes sob três perspectivas principais: dados pessoais/sensíveis, segredos de negócios internos e segredos de negócios de clientes. Recomendamos o download do material para facilitar a interação com os botões clicáveis, otimizando a leitura e o aprendizado. O conteúdo está dividido em três partes principais:

1. Infográficos: Incluem 5 fluxos detalhados que sintetizam aspectos relevantes do processo de resposta a incidentes de forma prática, visual e interativa (itens clicáveis) para esclarecimentos adicionais. Apresentamos as principais medidas técnicas e administrativas a serem adotadas antes, durante e após um incidente.

2. Perguntas e Respostas: Aborda questões cruciais como: prazo de comunicação; eventos que devem ser comunicados; análise de risco ou dano relevante; composição do Comitê de Crise/Sala de Guerra; responsável pela comunicação; conteúdo da comunicação à ANPD e aos titulares; e elementos do Relatório de registro do incidente, entre outros. Baseado na recente Resolução nº15 da ANPD, este conteúdo oferece insights técnicos e práticos para garantir a conformidade e segurança das operações.

3. Visão da ANPD: Apresenta as principais lições aprendidas a partir das Notas Técnicas da ANPD, incluindo a aplicação de sanções. Destacamos o entendimento da Autoridade sobre notificação aos titulares, sanções por não apresentação de documentos, necessidade de medidas de segurança robustas ao lidar com dados sensíveis, de crianças, adolescentes e idosos, e a relevância dos registros (logs). Explicamos como a ausência de um Plano de Resposta a Incidentes é vista como violação à legislação e que a comunicação individual aos titulares é indispensável, independentemente de danos concretos, focando na possibilidade de risco relevante.

Esperamos que este Guia seja uma ferramenta valiosa para aprimorar suas práticas de resposta a incidentes de segurança, reforçando a importância de uma atuação preventiva e uma resposta eficiente diante de violações.

VLK Direito, Inovação & Tecnologia

www.vlklaw.com.br

2

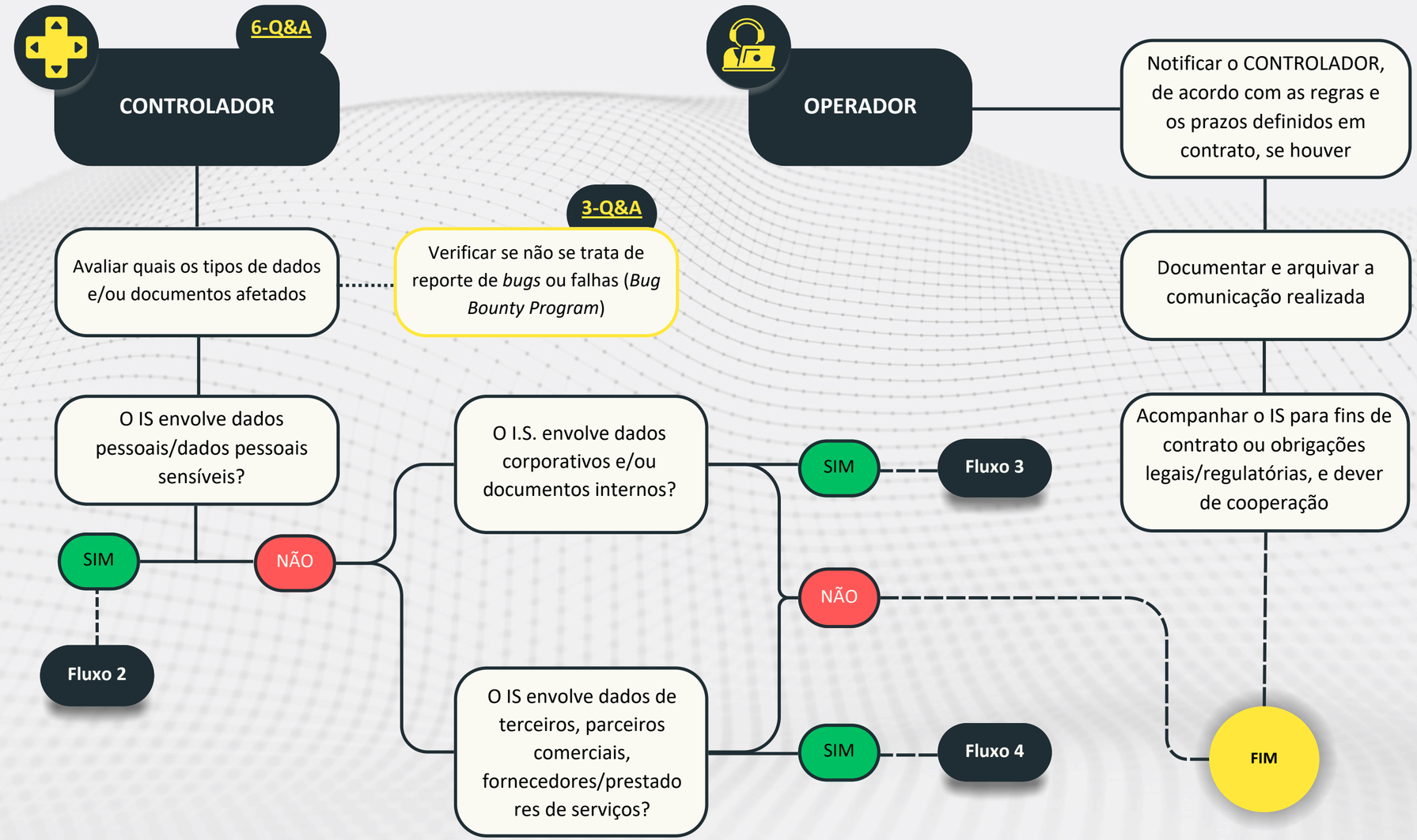
Infográficos Interativos

Itens clicáveis

Direito,
Inovação
& Tecnologia

Fluxo 1 - Identificando Incidentes de Segurança (“IS”) e as suas Consequências

3-Q&A

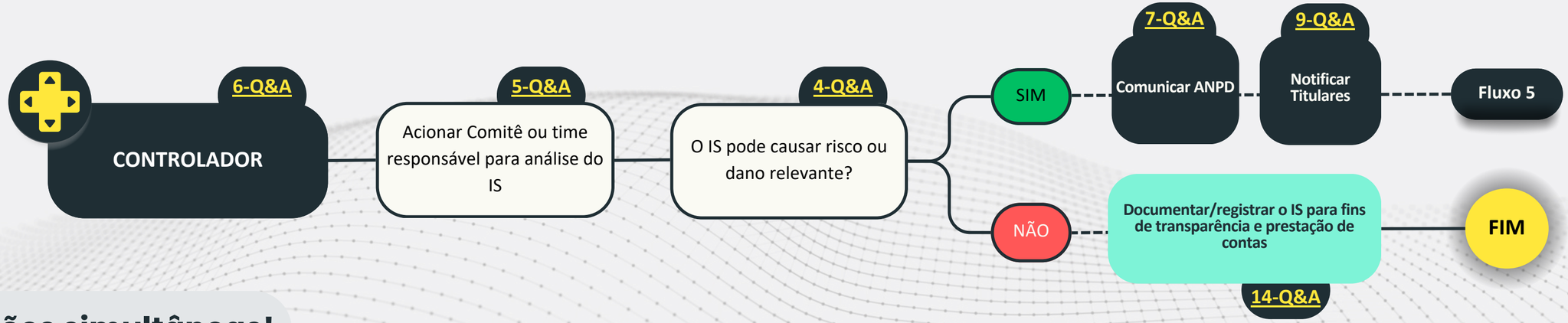


Direito, Inovação & Tecnologia

Clique nos botões de Q&A para ser direcionado à questão

Fluxo 2 - Respondendo Incidentes de Segurança com Dados Pessoais e Dados Pessoais Sensíveis

3-Q&A



Ações simultâneas!

Identificar/documentar a **causa-raiz** e demais ações realizadas para demonstrar a detecção e o estancamento da vulnerabilidade

Criar **Sala de Crise (*War Room*)** e Grupo de Trabalho, documentar ações e responsabilidades dos integrantes do time de resposta e gerar ata das reuniões com todos os pontos discutidos e debatidos, incluindo as conclusões

Entender **potenciais danos/riscos decorrentes do IS**: interrupção dos serviços; destruição de dados e/ou documentos; e/ou exfiltração de dados e/ou documentos; alterações/ modificações não autorizadas em documentos e/ou configurações de segurança internas

No caso de **solicitação de valores** para identificação ou correção de vulnerabilidades, acionar o Jurídico/*Compliance*, imediatamente, para avaliar a possibilidade e os riscos relacionados

Preservar e armazenar todas as evidências (incluindo logs de atividade dos sistemas, redes e aplicações relacionadas ao IS), utilizar mecanismos de cópia forense digital (hash) e elaborar Ata Notarial, se necessário

Avaliar **Plano de Continuidade de Negócios e/ou Plano de Recuperação de Desastres** para identificar medidas específicas para lidar com o IS

Avaliar **Comunicado ao Mercado/Fato Relevante** e para **Reguladores** (CVM, BACEN, ANS, SUSEP etc.)

Analisar os contratos de clientes afetados para verificar se há obrigações relacionadas

Analisar **legislação de outros países envolvidos**, caso o IS tenha abrangência internacional

Reuniões diárias, ou conforme necessidade, com o Grupo de Trabalho, para atualizações e gerenciamento da situação

Monitorar surface/*deep*/*dark* web e reportar ao Jurídico, imediatamente, caso seja identificado algum material da companhia

Avaliar e acionar o **seguro cibernético**, ainda que seja para comunicar expectativa de sinistro, se o caso

Na hipótese de envolvimento de fraudador, **confirmar veracidade de potencial vulnerabilidade ou amostra** dos dados disponibilizados, bem como se a amostra não é originada de incidentes em outras companhias

Analisar necessidade de adoção de medidas para remoção do conteúdo/material

Se o caso, **avaliar a interlocução com o atacante sobre o pedido de resgate**/recompensa e envolver o Jurídico/*Compliance* nas tratativas

Avaliar eventual **Boletim de Ocorrência** ou pedido de instauração de Inquérito Policial para preservação de direitos e utilização desse fato nas notas reativas

Analisar eventual elaboração de **Nota Reativa à Imprensa** e aos **clientes envolvidos**

Orientar o time atendimento e preparar documento com "Perguntas e Respostas", conforme caso concreto

Orientar os colaboradores internos que não se manifestem sobre o IS, em caso de questionamento por terceiros externos à companhia, bem como instrui-los a direcionar eventuais questionamentos para o ponto de contato adequado

Atuar para **restauração do ambiente afetado**

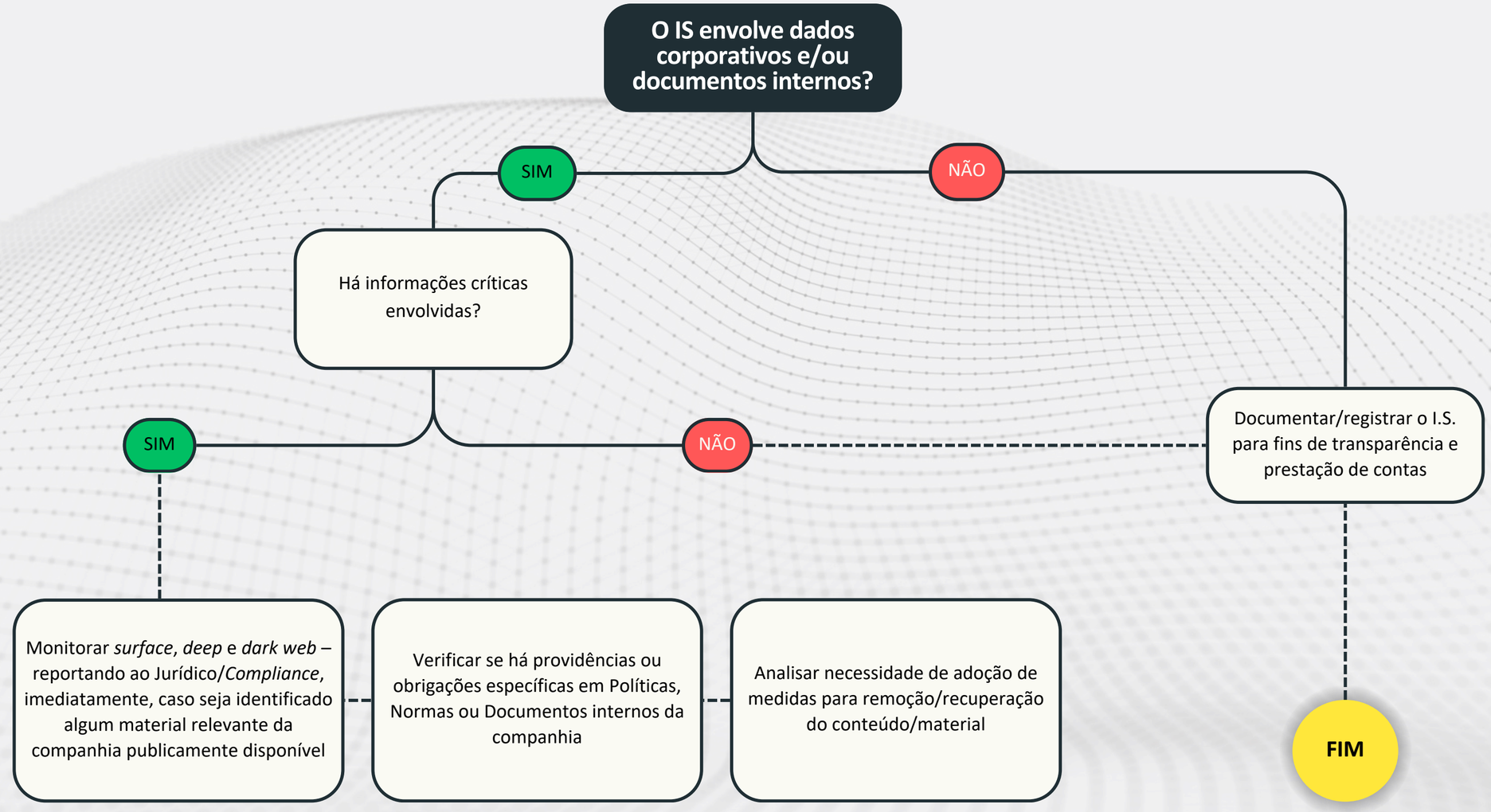
Avaliar **obrigação de comunicação a terceiros**

Entender o risco dos dados expostos e **atuar para eventual remoção**, caso venha a ser disponibilizado publicamente algum material

Voltar ao Fluxo 1

Fluxo 3 - Respondendo Incidentes de Segurança com Dados Corporativos e Documentos internos

3-Q&A

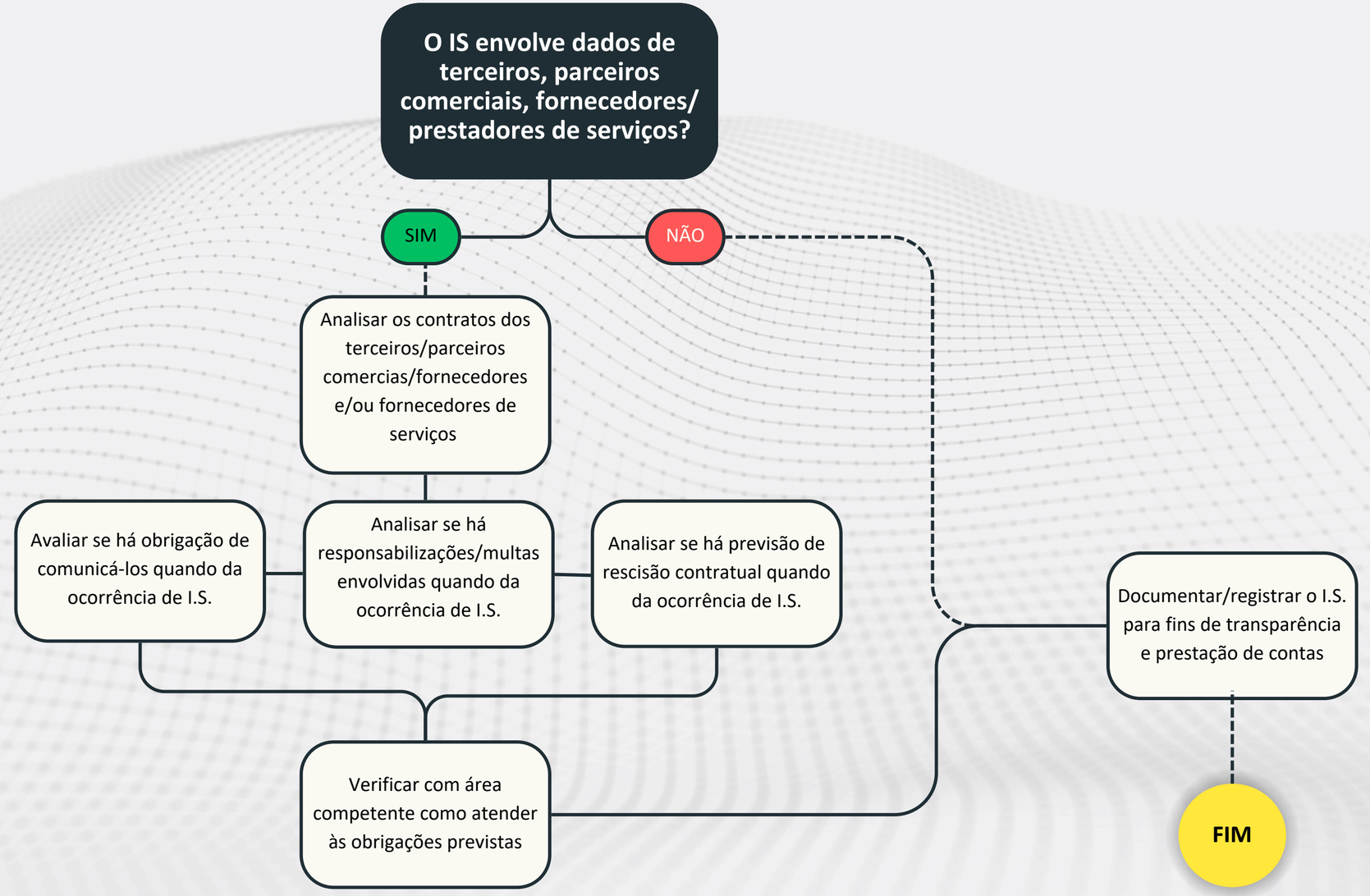


VLK Direito, Inovação & Tecnologia

Voltar ao Fluxo 1

Fluxo 4 - Respondendo Incidentes de Segurança com Dados de Terceiros

3-Q&A



Direito, Inovação & Tecnologia

Voltar ao Fluxo 1

Fluxo 5 - Prazos de Comunicação (Titulares e ANPD)

COMUNICAR ANPD — 7-Q&A

Formulário CIS

PRAZO
03 DIAS ÚTEIS
contados do conhecimento do I.S. envolvendo dados pessoais — 1 /2-Q&A

PRAZO
06 DIAS ÚTEIS
contados do conhecimento do I.S. envolvendo dados pessoais, apenas para Agentes de Tratamento de Pequeno Porte (ATPP) — 1 /2-Q&A

Comunicação completa

Comunicação preliminar

Comunicação complementar — 8-Q&A

PRAZO
20 DIAS ÚTEIS
contados do comunicado preliminar

7-Q&A

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 afetados pelo incidente;
Motivos da demora, caso a comunicação não tenha sido realizada no prazo; e
Medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares, quando cabíveis.

Acompanhar andamento CIS

7-Q&A

Pedido de sigilo no SEI
Antes de protocolar a comunicação e anexos, verificar se há informações confidenciais ou estratégicas e solicitar sigilo de forma específica e fundamentada.

NOTIFICAR TITULARES — 9-Q&A

Comunicação direta e individualizada (se possível)

Utilizar linguagem simples e de fácil entendimento ao titular

O conteúdo da notificação deve conter:
Descrição da natureza e categoria dos dados afetados;
Medidas técnicas de segurança utilizadas (antes, durante e após o incidente);
Riscos do incidente e possíveis impactos aos titulares;
Motivos da demora, caso a comunicação não tenha sido realizada no prazo previsto de três dias úteis;
Medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares, quando cabíveis;
Data de conhecimento do incidente;
Contato para obtenção de informações;
Dados de contato do encarregado.

10-Q&A

Documentos Adicionais
A ANPD poderá requisitar:
Mapeamento das Atividades (RoPA);
Relatório de Impacto à Proteção de Dados Pessoais (RIPD);
Testes de Balanceamento (LIAs);
Relatório de Tratamento do Incidente; e
Quaisquer documentos que sejam relevantes para a investigação.

Medidas Técnicas e Administrativas Preventivas

MEDIDAS TÉCNICAS

PENETRATION TESTS
Executar *penetration tests* nos sistemas, redes e aplicações corporativas, gerando relatório com as análises e descobertas

LOGS/REGISTROS
Investigar *logs*/registros de acesso em redes, sistemas e aplicações corporativas, visando detectar acessos (ou tentativas) que fujam a normalidade

NÍVEIS DE PRIVILÉGIO
Verificar os níveis de privilégio das credenciais dos colaboradores (*need to know e least privilege*) para avaliar se estão de acordo com cada função exercida

MÚLTIPLOS FATORES DE AUTENTICAÇÃO
Verificar a existência de recursos de Múltiplos Fatores de Autenticação para acesso aos sistemas, redes e aplicações críticos

CRIPTOGRAFIA E OUTRAS TECNOLOGIAS
Verificar a existência de criptografia e/ou recursos de mascaramento em bancos de dados que armazenam dados pessoais

CONFIGURAÇÕES
Verificar se as configurações padrão de sistemas, redes e aplicações corporativas estão dentro do previamente especificado pela organização (*baseline configuration*)

BACKUPS
Verificar se *backups*, testes e análises de segurança da informação da organização estão em dia (incluindo, por exemplo, atualizações de programas anti-malwares, realização de patches de segurança em aplicações e programas, dentre outros)

MEDIDAS ADMINISTRATIVAS

PROGRAMA DE RECOMPENSAS
Avaliar a criação de Programa de Recompensas (*Bug Bounty*), privado e interno, para fins de governança

TREINAMENTO COLABORADORES
Implementar cronograma de treinamento dos colaboradores sobre os atuais riscos de segurança da informação

CONSCIENTIZAÇÃO
Reforçar ações de conscientização em proteção de dados e segurança da informação

MATRIZ DE RISCOS
Atualizar com frequência a matriz de risco corporativa para refletir as novas ameaças de segurança da informação/proteção de dados, acompanhando a implementação dos controles mitigatórios

TREINAMENTO DE *SPEAKERS*
Treinar porta-vozes da companhia e estruturar *talking points* para conversas com executivos de outros clientes impactados, incluindo comunicações à imprensa/mídia sobre o incidente

SIMULAÇÃO DE INCIDENTE
Simular incidente de segurança e atualizar o plano de resposta a incidentes, de acordo com as oportunidades de melhoria documentadas

POLÍTICAS INTERNAS
Elaborar e/ou revisar Política de Segurança da Informação, Política de Classificação de Dados, Plano de Continuidade de Negócios e/ou Plano de Recuperação de Desastres para identificar medidas específicas para lidar com o IS

LIÇÕES APRENDIDAS
Documento final com lições aprendidas para mitigação do risco de reincidência

GOVERNANÇA E MÉTRICAS
Implementar indicadores de resposta a incidentes, incluindo tempos de detecção, contenção, confirmação de dados pessoais afetados, análise de risco, aprovação de comunicações, titulares afetados por categoria, comunicações bem-sucedidas, conclusão do relatório final e status das ações corretivas.

3

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.

Atenção a conflito de interesses do Encarregado
Quando o DPO/Encarregado cumular essa função com outras posições, especialmente de liderança, é fundamental avaliar se há conflito de interesses e, se necessário, acionar o Encarregado substituto ou representante legal para condução do processo de resposta ao incidente, incluindo a comunicação à ANPD e aos titulares.

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 dentro do sistema SEI 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 realizada 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.

Checklist de Sigilo e Anexos no SEI

Antes de protocolar a comunicação:

- ☐ Separar anexos sigilosos e não sigilosos.
- ☐ Fundamentar o sigilo por documento e, se necessário, por parágrafo, item ou tópico.
- ☐ Evitar anexar credenciais, chaves, IOCs sensíveis, arquitetura de rede ou amostras de dados sem necessidade.
- ☐ Preparar versão redigida para eventual publicidade.

Exemplos de hipóteses e fundamentos a considerar:

- Segredo de negócio, segredo comercial ou industrial: fundamentar na competência da ANPD de zelar pela observância de segredos comercial e industrial e de informações protegidas por lei. A Nota Técnica nº 22/2024 da ANPD menciona o art. 55-J, II, da LGPD e a necessidade de balancear transparência com proteção de informações restritas sob custódia da Autoridade.

- **Dados pessoais, dados sensíveis ou informações que possam afetar privacidade, intimidade, honra, imagem ou autodeterminação informativa dos titulares:** embasar na LGPD, especialmente nos fundamentos do art. 2º, também mencionados pela ANPD na Nota Técnica nº 22/2024 ao tratar de restrição de acesso.

- **Informações técnicas sensíveis de segurança, como arquitetura de rede, logs detalhados, vulnerabilidades exploradas, IOCs sensíveis, evidências forenses ou detalhes de contenção:** fundamentar na necessidade de evitar ampliação de risco ao ambiente, aos titulares e à própria apuração, podendo haver suporte adicional na LAI quando a divulgação puder comprometer segurança, sistemas, bens, instalações, atividades de investigação ou fiscalização em andamento.

- **Documentos parcialmente sigilosos:** privilegiar ocultação apenas dos trechos sensíveis, e não do documento inteiro, quando viável. A Nota Técnica nº 22/2024 da ANPD indica que, em vez de restringir documentos em sua integralidade, deve-se ocultar apenas os trechos sigilosos, preservando a primariedade da informação e o interesse público na publicidade de entendimentos regulatórios.

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 social.

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 contato 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.

Caso o incidente envolva públicos vulneráveis, como crianças, adolescentes ou idosos, recomenda-se avaliar a elaboração de modelos de comunicação segmentados, considerando as características do público afetado e os canais mais adequados para assegurar compreensão e efetividade.

A depender do caso, podem ser preparados modelos distintos para titulares em geral, titulares vulneráveis, responsáveis legais por crianças e adolescentes e/ou outros representantes legalmente autorizados.

Além do conteúdo da mensagem, é recomendável preservar evidências sobre a efetividade da comunicação, incluindo: versão final da comunicação enviada; canal utilizado; data e horário de envio; logs, comprovantes ou screenshots de disparo; taxa de entrega; registros de falha ou devolução; medidas de reenvio; percentual de titulares comunicados com sucesso; volume e natureza das dúvidas recebidas; respostas fornecidas; e versão final da FAQ ou roteiro utilizado pelo time de atendimento.

Esses elementos podem ser relevantes caso a ANPD questione a suficiência, a clareza ou a efetividade da comunicação aos titulares.

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 analisa 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 não ter adotado medidas técnicas e organizacionais preventivas compatíveis com o risco que o tratamento de dados representa, incluindo controles de segurança, governança, políticas, procedimentos, registros, monitoramento e mecanismos de resposta adequados ao contexto do tratamento, 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.

Quando houver dúvida sobre comunicar ou não, é possível preencher o formulário no formato preliminar da ANPD e depois de 20 dias úteis complementar com a conclusão

Quando eventuais informações fornecidas à ANPD envolverem segredo de negócio, a empresa deverá solicitar sigilo para os trechos específicos e caberá 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.

4

A Visão da ANPD

Lições Aprendidas a partir das Sanções Aplicadas

Direito,
Inovação
& Tecnologia

A comunicação de incidentes de segurança a ANPD sem que haja a notificação concomitante aos titulares pode gerar sanções. Em casos envolvendo elementos de risco mais evidentes, como o envolvimento de dados sensíveis, a ANPD considerou a notificação aos titulares após a comunicação preliminar à ANPD como notificação tardia.

A não apresentação de documentos solicitados pela ANPD é considerada violação à LGPD e foi sancionada em mais de um caso. Diante das sanções pela falta de apresentação de documentos no prazo solicitado pela ANPD, é recomendável preparar os documentos relevantes sobre o tratamento de dados com antecedência (especialmente: mapeamento; Testes de Balanceamento; Relatório de Impacto; contratos; formalização da nomeação do Encarregado; *due diligence* em fornecedores), e não somente mediante o acontecimento de incidente de segurança ou solicitação da ANPD.

O tratamento de dados pessoais sensíveis ou de categorias especiais de titulares como crianças, adolescentes e idosos implica a necessidade de medidas mais robustas de segurança. Em casos específicos em que falhas de segurança causaram os incidentes, a ANPD ressaltou que a violação se dá especialmente diante do tratamento de dados que apresentam maiores riscos aos titulares.

A ausência de registros (logs) foi considerada falha:

a ANPD entendeu que não é razoável que a falha no dever de proteger os dados, e consequente incapacidade de demonstrar que tais dados não foram acessados e de determinar quantas vezes a vulnerabilidade foi explorada, que essa incerteza, provocada por falha em cumprir dever legal, seja aproveitada em favor daquele que deixou de cumprir seu dever. Esse entendimento foi baseado no princípio da responsabilização e prestação de contas da LGPD, que determina que o agente de tratamento deve ser capaz de demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Documentos normalmente solicitados pela ANPD em incidentes de segurança.

A ANPD tem utilizado seus poderes de fiscalização para solicitar documentos que permitam avaliar com profundidade os incidentes, a suficiência das medidas técnicas e organizacionais adotadas, verificar a comunicação aos titulares e confirmar a implementação de medidas corretivas. Em casos que avançam para análise mais aprofundada, é comum que a Agência envie ofícios requisitando documentos e esclarecimentos específicos.

Documento / informação	Base ou fundamento indicado	Grau de recorrência sugerido
Relatório técnico do incidente	Art. 8º da Resolução CD/ANPD nº 15/2024	Comumente solicitado
RoPA / mapeamento das atividades de tratamento	Art. 8º da Resolução CD/ANPD nº 15/2024	Comumente solicitado
RIPD / DPIA	Art. 8º da Resolução CD/ANPD nº 15/2024 e art. 38 da LGPD	Comumente solicitado

Documento / informação	Base ou fundamento indicado	Grau de recorrência sugerido
LIA / teste de balanceamento	Poderes gerais de fiscalização da ANPD	Comumente solicitado
Logs, trilhas de auditoria e registros de acesso	Logs, trilhas de auditoria e registros de acesso	Comumente solicitado
Evidências de comunicação aos titulares	Obrigação legal do controlador de comunicar os titulares, quando cabível	Comumente solicitado
Obrigação legal do controlador de comunicar os titulares, quando cabível	Obrigação legal do controlador, quando a divulgação pública for adotada ou determinada	Comumente solicitado
Documentação de remediação e medidas de não recorrência	Art. 48 da LGPD; dever de mitigar ou reverter os efeitos do incidente	Comumente solicitado

Documento / informação	Base ou fundamento indicado	Grau de recorrência sugerido
Plano de resposta a incidentes e políticas internas de segurança	Poderes gerais de fiscalização da ANPD; arts. 46 e 49 da LGPD	Comumente solicitado
Notas de ransomware / comunicações com atacante	Poderes gerais de fiscalização da ANPD, especialmente para avaliação da ameaça, eventual exfiltração e decisões de negociação	Comumente solicitado
Contratos com operadores e terceiros envolvidos	Poderes gerais de fiscalização da ANPD; dever de governança e prestação de contas	Solicitado em casos específicos
Comunicações com atacantes	Troca de mensagens com o atacante (sobretudo mensagens de solicitação de resgate por dados)	Solicitado em casos específicos

Documento / informação	Base ou fundamento indicado	Grau de recorrência sugerido
Relatórios forenses	Poderes gerais de fiscalização da ANPD	Solicitado em casos específicos
Atas de war room / comitê de crise	Poderes gerais de fiscalização da ANPD; documentação da tomada de decisão	Solicitado em casos específicos
Ata notarial ou outras evidências formais de preservação	Poderes gerais de fiscalização da ANPD; preservação de evidências	Solicitado em casos específicos

Atenção aos primeiros 30 a 60 dias após a comunicação.

Esse período tende a ser crítico para demonstrar cooperação, transparência e capacidade de resposta perante a ANPD. É recomendável que o controlador esteja preparado para apresentar rapidamente relatórios técnicos, logs, cronologia do incidente, evidências de comunicação aos titulares, RoPA, RIPD/DPIA, medidas de contenção e plano de remediação. Respostas completas e bem documentadas nessa fase podem reduzir o risco de aprofundamento da análise ou instauração de procedimento sancionador.

Jurisprudência em Incidentes de Segurança

Além da atuação administrativa da ANPD, incidentes de segurança também têm sido objeto de crescente análise pelo Poder Judiciário, especialmente em discussões sobre responsabilidade civil, dano moral, tratamento de dados bancários, ataques cibernéticos, dados sensíveis e ônus de demonstrar a adoção de medidas adequadas de segurança.

A jurisprudência recente indica que o vazamento de dados pessoais comuns não necessariamente gera dano moral presumido, exigindo-se, em determinados casos, prova de prejuízo efetivo pelo titular. Contudo, o entendimento pode ser distinto quando o incidente envolve dados sensíveis, hipótese em que há maior tendência de reconhecimento de dano moral presumido.

Em incidentes envolvendo dados bancários, financeiros ou operacionais sigilosos, a exposição judicial tende a ser maior quando houver elementos de que as informações foram obtidas a partir da instituição ou de sua cadeia de tratamento e utilizadas para viabilizar fraude contra o titular.

Em relações de consumo, a aplicação conjunta da LGPD e do CDC pode reforçar o regime de responsabilidade objetiva do fornecedor, sobretudo em casos de fraude ou falha na prestação do serviço. Da mesma forma, falhas na demonstração de boas práticas de segurança e governança podem dificultar a defesa do agente de tratamento e reforçar a imputação de responsabilidade, especialmente em ataques cibernéticos, mas não configuram, isoladamente, hipótese automática de dano moral in re ipsa.

Nesse contexto, o acompanhamento de precedentes judiciais é relevante para calibrar a estratégia de resposta a incidentes, a documentação das medidas adotadas, comunicação aos titulares e preparação de evidências que demonstrem diligência, prevenção, segurança e prestação de contas.

Tendências gerais em casos de incidentes de segurança

Tema	Tendência identificada	Impacto prático para incidentes
Responsabilidade e ressarcimento de danos	As decisões sobre incidentes de segurança têm mencionado de forma recorrente os arts. 42, 43, 44 e 45 da LGPD, indicando que a discussão judicial costuma se concentrar na responsabilidade civil e no dever de reparação.	A resposta ao incidente deve ser estruturada também como preparação probatória para eventual litígio. **Isso significa registrar, desde o início, a linha do tempo do incidente, as medidas técnicas existentes antes do evento, as ações de contenção e mitigação, os critérios usados na análise de risco, os fundamentos para comunicar ou não comunicar titulares e ANPD, e os elementos que demonstrem inexistência de dano indenizável ou ausência de nexo causal.**
Setores mais afetados	O Painel identifica maior concentração de decisões em incidentes envolvendo setor financeiro, bancos de dados e cadastros de consumidores e setor público.	Organizações desses setores devem tratar incidentes como eventos de exposição regulatória e judicial ampliada. Em especial, recomenda-se reforçar controles antifraude, trilhas de auditoria, governança de terceiros, bases de consulta e mecanismos de autenticação, **pois a discussão judicial tende a conectar o incidente a riscos concretos de fraude, uso indevido de dados e falha na prestação do serviço.**

Tema	Tendência identificada	Impacto prático para incidentes
Fraudes, boletos falsos e phishing	Casos de golpe de boleto, phishing e uso indevido de dados financeiros aparecem de forma expressiva, com discussões sobre falhas em medidas de segurança e autenticação.	Em incidentes com potencial de fraude financeira, a organização deve priorizar a preservação de evidências sobre origem do dado utilizado no golpe, canais de comunicação com o titular, mecanismos de autenticação, alertas antifraude, bloqueios, reenvios, contestação de transações e medidas de contenção. **A estratégia deve considerar não apenas o vazamento em si, mas se os dados expostos viabilizaram ou facilitaram a fraude alegada.**
Culpa exclusiva de terceiros	A alegação de ataque externo ou fraude de terceiros não tem sido suficiente, por si só, para afastar responsabilidade; os tribunais tendem a exigir demonstração de medidas robustas de segurança.	**A tese de ato exclusivo de terceiro somente tende a ser sustentável se acompanhada de documentação robusta sobre controles preventivos, monitoramento, resposta ao incidente e mitigação**. Por isso, é recomendável manter evidências de governança, testes de segurança, logs, gestão de vulnerabilidades, gestão de acessos, análise forense, atuação do comitê de crise e decisões tomadas para reduzir o impacto aos titulares.

Tema	Tendência identificada	Impacto prático para incidentes
Dano moral	O reconhecimento de dano moral em incidentes de segurança ainda não é uniforme: há decisões que exigem comprovação de prejuízo e outras que reconhecem reparação diante da violação à privacidade, especialmente quando há falha de segurança, dados sensíveis, dados bancários, financeiros ou operacionais sigilosos, quando houver elementos de que foram obtidos a partir da instituição ou de sua cadeia de tratamento e utilizados para viabilizar fraude contra o titular ou titulares vulneráveis.	**A classificação dos dados afetados deve orientar a estratégia jurídica desde o início.** Dados comuns podem permitir linha defensiva baseada na necessidade de comprovação de dano concreto; já dados sensíveis, financeiros, de autenticação, de crianças, adolescentes, idosos ou titulares em situação de vulnerabilidade exigem tratamento de risco elevado, com comunicação mais cuidadosa, mitigação reforçada e documentação específica sobre potenciais danos materiais, morais, discriminatórios, reputacionais ou de fraude.
Medidas de segurança adequadas	O Painel aponta que ainda há subjetividade judicial sobre quais medidas técnicas e administrativas são consideradas suficientes, embora decisões venham valorizando evidências de monitoramento, autenticação, controles antifraude e políticas de segurança.	**Como não há um checklist judicial único sobre suficiência de segurança, a organização deve conseguir demonstrar proporcionalidade entre risco e controles adotados**. Para isso, recomenda-se documentar baseline de segurança, MFA, criptografia, segregação de acessos, monitoramento, backups, testes, gestão de patches, políticas internas, treinamentos, simulações de incidente e plano de melhoria pós-incidente, conectando cada medida ao risco específico do tratamento afetado.

Fonte: Relatório Painel LGPD nos Tribunais, 5ª edição.

Tendências gerais em casos de incidentes de segurança

Dano moral presumido em vazamento de dados sensíveis	Responsabilidade proativa e ataque hacker	Dados pessoais comuns - ausência de dano moral presumido	Dados pessoais não sensíveis em bancos de dados - dano moral presumido	Dados pessoais não sensíveis - necessidade de comprovação do dano
STJ, REsp nº 2.121.904/SP, Rel. Min. Nancy Andrighi, 3ª Turma, julgado em 11/02/2025, DJe 17/02/2025, Informativo de Jurisprudência nº 842)	**STJ, REsp nº 2.147.374/SP, Rel. Min. Ricardo Villas Bôas Cueva, 3ª Turma, julgado em 03/12/2024, DJe 06/12/2024, Informativo de Jurisprudência nº 838.**	**STJ, AREsp nº 2.130.619/SP, Rel. Min. Francisco Falcão, 2ª Turma, julgado em 07/03/2023. DJe 10/3/2023, Informativo de Jurisprudência nº 766.**	**STJ, REsp nº 2.201.694/SP, Rel. Min. Ricardo Villas Bôas Cueva, Rel. p/ Acórdão Min. Nancy Andrighi, 3ª Turma, julgado em 05/08/2025, DJe 15/08/2025.**	**STJ, REsp nº 2.221.650/SP, Rel. Min. Maria Isabel Gallotti, 4ª Turma, julgado em 04/11/2025, DJe 14/11/2025.**
Entendimento: em contrato de seguro de vida, o vazamento de dados pessoais sensíveis fornecidos pelo segurado enseja responsabilidade objetiva da seguradora e caracteriza dano moral presumido.	**Entendimento:** mesmo quando o vazamento decorrer de ataque hacker, o agente de tratamento permanece sujeito aos deveres da LGPD, especialmente aos deveres de transparência, segurança e demonstração de medidas adequadas. A alegação de ato ilícito de terceiro não afasta, por si só, as obrigações do controlador.	**Entendimento:** o vazamento de dados pessoais comuns, embora constitua falha indesejável no tratamento de dados, não gera automaticamente dano moral indenizável. O titular deve comprovar prejuízo efetivo decorrente da exposição. O STJ destacou que o entendimento poderia ser diferente se o caso envolvesse dados pessoais sensíveis. Entretanto, esse entendimento pode vir a ser revisitado por decisões recentes do STJ que versam sobre incidentes envolvendo dados pessoais não sensíveis e bancos de dados de proteção ao crédito.	**Entendimento:** a 3ª Turma entendeu, por maioria, que o gestor de banco de dados regido pela Lei nº 12.414/2011 não pode disponibilizar a terceiros consulentes informações cadastrais e de adimplemento que somente poderiam ser compartilhadas entre bancos de dados. Nessa hipótese, a disponibilização indevida gera responsabilidade objetiva e dano moral presumido ao titular.	**Entendimento:** a 4ª Turma entendeu que, embora gestores de bancos de dados não estejam autorizados a disponibilizar dados pessoais e histórico de crédito sem consentimento prévio, a disponibilização de dados pessoais não sensíveis, por si só, não configura dano moral presumido. É necessária a comprovação de abalo significativo aos direitos da personalidade.

A Visão da ANPD sobre a Comunicação de Incidentes: Lições Aprendidas a partir das Sanções Aplicadas

Dano moral presumido em vazamento de dados sensíveis	Responsabilidade proativa e ataque hacker	Dados pessoais comuns - ausência de dano moral presumido	Dados pessoais não sensíveis em bancos de dados - dano moral presumido	Dados pessoais não sensíveis - necessidade de comprovação do dano
Impacto prático: incidentes envolvendo dados sensíveis, como dados de saúde, biométricos ou informações íntimas, devem ser tratados como cenários de maior risco jurídico, com reforço na análise de risco, comunicação aos titulares, mitigação, preservação de evidências e documentação das medidas adotadas.	**Impacto prático:** a organização deve ser capaz de demonstrar responsabilidade proativa, com evidências de governança, controles técnicos, logs, monitoramento, resposta ao incidente, mitigação e boas práticas de segurança, inclusive para sustentar eventual excludente ou redução de responsabilidade.	**Impacto prático:** em incidentes envolvendo apenas dados pessoais comuns, a organização pode estruturar sua estratégia a partir da distinção entre exposição indesejada e dano indenizável, documentando a natureza dos dados, a ausência de dados sensíveis, a inexistência de indícios de fraude ou uso indevido e as medidas de mitigação adotadas. No entanto, diante da evolução jurisprudencial, essa tese deve ser utilizada com cautela.	**Impacto prático:** agentes que atuam como gestores de bancos de dados, bureaus de crédito ou empresas que disponibilizam dados a terceiros devem revisar fluxos de compartilhamento, bases legais, controles de acesso e contratos com consulentes. Mesmo quando os dados não forem sensíveis, a disponibilização indevida a terceiros pode ser tratada como violação apta a gerar dano moral presumido, especialmente quando houver descumprimento dos limites da Lei do Cadastro Positivo e da LGPD.	**Impacto prático**: a decisão preserva espaço para defesa baseada na ausência de dano concreto, especialmente quando não houver prova de efetiva disponibilização dos dados, de acesso por terceiros ou de abalo relevante aos direitos da personalidade. Ainda assim, a organização deve documentar a licitude do tratamento, a finalidade de proteção ao crédito, a comunicação ou consentimento quando aplicável e os elementos probatórios que afastem dano, nexo causal e uso indevido.

As sanções reforçam os poderes de fiscalização da ANPD e os deveres dos agentes no âmbito desse processo. Os agentes devem estar preparados para as seguintes exigências da ANPD no âmbito de processos de fiscalização:

Fornecer cópias de documentos relevantes para a avaliação das atividades de tratamento pela ANPD (mapeamento, LIAs, DPIAs, contratos e *due dilligence* em operadores)

Permitir acesso às instalações, aos aplicativos, ferramentas e recursos tecnológicos, documentos para avaliação das atividades de tratamento, em seu poder ou de terceiros - ou seja, eventuais subcontratados

Possibilitar que a ANPD tenha acesso aos sistemas de informação e a aspectos relacionados à rastreabilidade e atualização

Submeter-se a auditorias, especialmente no caso de não atendimento de solicitações da ANPD

Manter os documentos durante os prazos estabelecidos em lei ou regulamentação e durante o processo administrativo em curso

Disponibilizar representante apto a oferecer suporte à atuação da ANPD, com autonomia, independência e informações claras e suficientes

Painel de Incidentes Comunicados da ANPD

A ANPD disponibiliza painel interativo com dados agregados sobre Comunicações de Incidentes de Segurança, permitindo acompanhar tendências, volumes, categorias e andamento dos procedimentos. Boas práticas:

Consultar periodicamente o painel

Usar os dados para atualizar treinamentos, planos de resposta e matrizes de risco;

Avaliar tendências sobre tipos de incidentes, dados afetados e setores mais expostos; e

cruzar os dados públicos com lições extraídas de sanções, notas técnicas e pedidos de complementação da ANPD.

Procedimentos parados podem ser retomados pela ANPD.

A falta de movimentação em uma Comunicação de Incidente de Segurança não significa arquivamento. A ANPD pode retomar o caso posteriormente, sobretudo diante de pendências documentais, inconsistências, ausência de evidências de mitigação, falhas na comunicação aos titulares ou risco relevante. Esse ponto ganha relevância adicional diante do fortalecimento institucional da Agência, especialmente após a Lei nº 15.352/2026, que transformou a ANPD em agência reguladora, com autonomia funcional, técnica, decisória, administrativa e financeira, criou a carreira de Regulação e Fiscalização de Proteção de Dados e previu cargos de Especialista em Regulação de Proteção de Dados; do Decreto nº 12.881/2026, que aprovou sua nova Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e Funções de Confiança; e da Resolução CD/ANPD nº 33/2026, que aprovou a nova estrutura institucional da Agência. Com estrutura mais robusta, incluindo Superintendência de Fiscalização, áreas especializadas e cargos técnicos dedicados, aumenta a capacidade da ANPD de revisar comunicações antigas, pedir complementações e priorizar casos de maior risco. Por isso, recomenda-se manter o dossiê do incidente completo e atualizado, com histórico das comunicações, evidências de envio, logs, relatórios técnicos, análise de risco, medidas corretivas e status de implementação.

A falta de Plano de Resposta a Incidentes é considerada violação ao artigo 5, I da LGPD do Regulamento de Fiscalização. A não apresentação do plano foi considerada obstrução à atividade de fiscalização, nos termos do art. 6º do Regulamento de Fiscalização, já que impediu avaliar as medidas técnicas adequadas e suficientes para prevenir e mitigar os efeitos do incidente.

A comunicação geral aos titulares não substitui a comunicação individual. Independentemente de a comunicação geral cumprir eventuais requisitos do art. 48, § 1º, da LGPD, a comunicação individual foi determinada considerado que o quantitativo de titulares é definido e limitado, de forma que não seria desproporcional e os endereços e e-mails dos titulares estavam disponíveis.

O dever de comunicação não depende da ocorrência de danos aos titulares, mas da possibilidade de risco relevante. A ANPD reforça que a obrigação de comunicação de incidentes à ANPD independe da concretização de danos aos titulares decorrentes do incidente, bastando que possa acarreta a eles risco ou dano relevante.

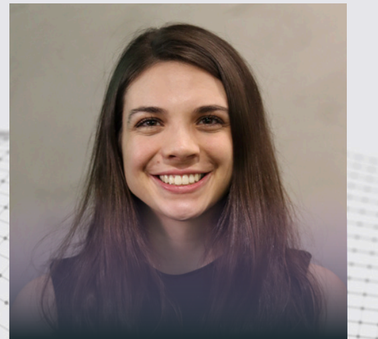
Os sistemas devem ser estruturados para conformidade com a LGPD. A ANPD identificou violação ao art. 49 da LGPD diante de que não estavam estruturados de modo a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD.

Exemplo de tipo de incidente e identificação de riscos pela ANPD: Considerando incidente que envolve dados de identificação utilizados comumente em cadastros (tais como: número de documento de identificação; foto do cartão de beneficiário, dados de crianças e adolescentes e dados de saúde), a ANPD vislumbrou os riscos de discriminação, violação à imagem, perturbações por ligações indevidas e fraudes em processos de autenticação ou validação de identidade em serviços específicos.

Autores

Caio Lima
caio@vlklaw.com.br

Bruna Bigas
bruna.bigas
@vlklaw.com.br



Giovanna Milanese
giovanna.milanese
@vlklaw.com.br

Paulo Sarmento
paulo.sarmento
@vlklaw.com.br

Jean Santana
jean.santana
@vlklaw.com.br

Emílio Loures
emilio.loures
@vlklaw.com.br

Direito,
Inovação
& Tecnologia

2026, VLK Advogados. Todos os direitos reservados.

Para mais informações ou para questões relacionadas à publicação, entre em contato conosco atráves do e-mail contato@vlklaw.com.br.

CC BY-ND - Esta licença permite cópia e distribuição do material em qualquer meio ou formato apenas de forma não adaptada e apenas desde que a atribuição seja dada ao criador. A licença permite o uso comercial.

contato@vlklaw.com.br

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

www.vlklaw.com.br

SOBRE NÓS

No VLK, **o Direito não é barreira**. É impulso para **inovar, viabilizar negócios** e construir uma sociedade mais próspera e justa.

Somos uma **boutique de Direito Digital** movida por **entregas que fazem a diferença**.

Conciliamos:

» Riscos e oportunidade;

» Complexidade e clareza; e

» Proteção e progresso.

Não importa o quão ousado seja o projeto: **faremos acontecer**, com segurança e **quebrando formalismos desnecessários**, nas seguintes áreas:

» Proteção de Dados Pessoais

» Governança Ética e Responsável de IA

» Cibersegurança e Resposta a Incidentes

» Legal Marketing e Propriedade Intelectual

» Regulação de Tecnologia

» Contencioso Estratégico

contato@vlklaw.com.br

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

www.vlklaw.com.br