GUIA DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

iab brasil

Índice

Prefácio

A segurança da informação tem se tornado uma preocupação central em um mundo cada vez mais digital e interconectado. A Lei Geral de Proteção de Dados (LGPD) trouxe diretrizes fundamentais para a proteção dos dados pessoais, impondo às organizações a necessidade de implementar medidas robustas para garantir a confidencialidade, integridade e disponibilidade dessas informações.

Neste contexto, a gestão de incidentes de segurança da informação é um pilar essencial para a conformidade e a proteção dos direitos dos titulares de dados. Um incidente mal gerenciado pode resultar em penalidades legais e financeiras, além de impactos reputacionais severos para as organizações envolvidas.

Este **Guia de Incidente de Segurança com Dados Pessoais** foi elaborado com o objetivo de oferecer um framework prático e estruturado para auxiliar empresas e profissionais a compreenderem, identificarem e responderem de forma eficiente a incidentes de segurança. O documento apresenta conceitos fundamentais da LGPD, explica as responsabilidades de cada agente no tratamento de dados, detalha o processo de avaliação de riscos e estabelece diretrizes para comunicação de incidentes, garantindo transparência e mitigação de danos.

Ao seguir as diretrizes aqui apresentadas, as organizações poderão atender aos requisitos regulatórios e adotar práticas eficazes de governança e segurança, assegurando maior proteção aos dados e confiança dos stakeholders.

Boa leitura!

Marcel Leonardi
(Leonardi Advogados)
Membro do Conselho Executivo 2025 do IAB Brasil

O que é a LGPD?

A Lei Geral de Proteção de Dados Pessoais ("LGPD" – Lei Federal n.º 13.709/2018) é a legislação brasileira que regula as atividades de tratamento de dados pessoais, visando proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A LGPD estabelece diretrizes claras sobre como as organizações devem coletar, armazenar, processar e compartilhar dados pessoais, sejam eles de clientes, colaboradores ou parceiros. A lei também define penalidades para o descumprimento, que podem incluir multas significativas e até a suspensão das atividades de tratamento de dados. Neste contexto, a Autoridade Nacional de Proteção de Dados (ANPD) é responsável por fiscalizar e garantir o cumprimento da LGPD no Brasil.

A importância da LGPD se dá sob dois aspectos: de um lado, a LGPD busca garantir aos titulares mais **direitos e garantias** em relação aos seus dados pessoais. De outro, a LGPD garante aos agentes de tratamento (entidades que tratam estes dados) regras claras e maior **segurança jurídica** em suas atividades.

Em relação à segurança dos dados pessoais, a LGPD determina que as empresas 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. Adotar medidas preventivas, além de ser uma obrigação legal, ajuda a evitar o risco de vazamento ou outras falhas internas que possam gerar danos aos titulares destes dados.

1. Definições

Dado pessoal é qualquer informação relacionada a uma pessoa identificada ou identificável (por exemplo: nome, RG, CPF, e-mail, telefone, endereço, histórico de navegação, endereço IP, score de crédito).

Pessoa "identificada" e "identificável"?

O conceito de 'dado pessoal' é bastante amplo: ele engloba dados que *identificam* diretamente uma pessoa — como seu nome completo, seu RG, CPF — e dados que identificam *indiretamente* uma pessoa — dados que por si só não identificam alguém, mas que podem fazê-lo a depender do contexto, como geolocalização, endereço IP, IMEI, dentre outros.

Dado pessoal sensível é qualquer informação sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

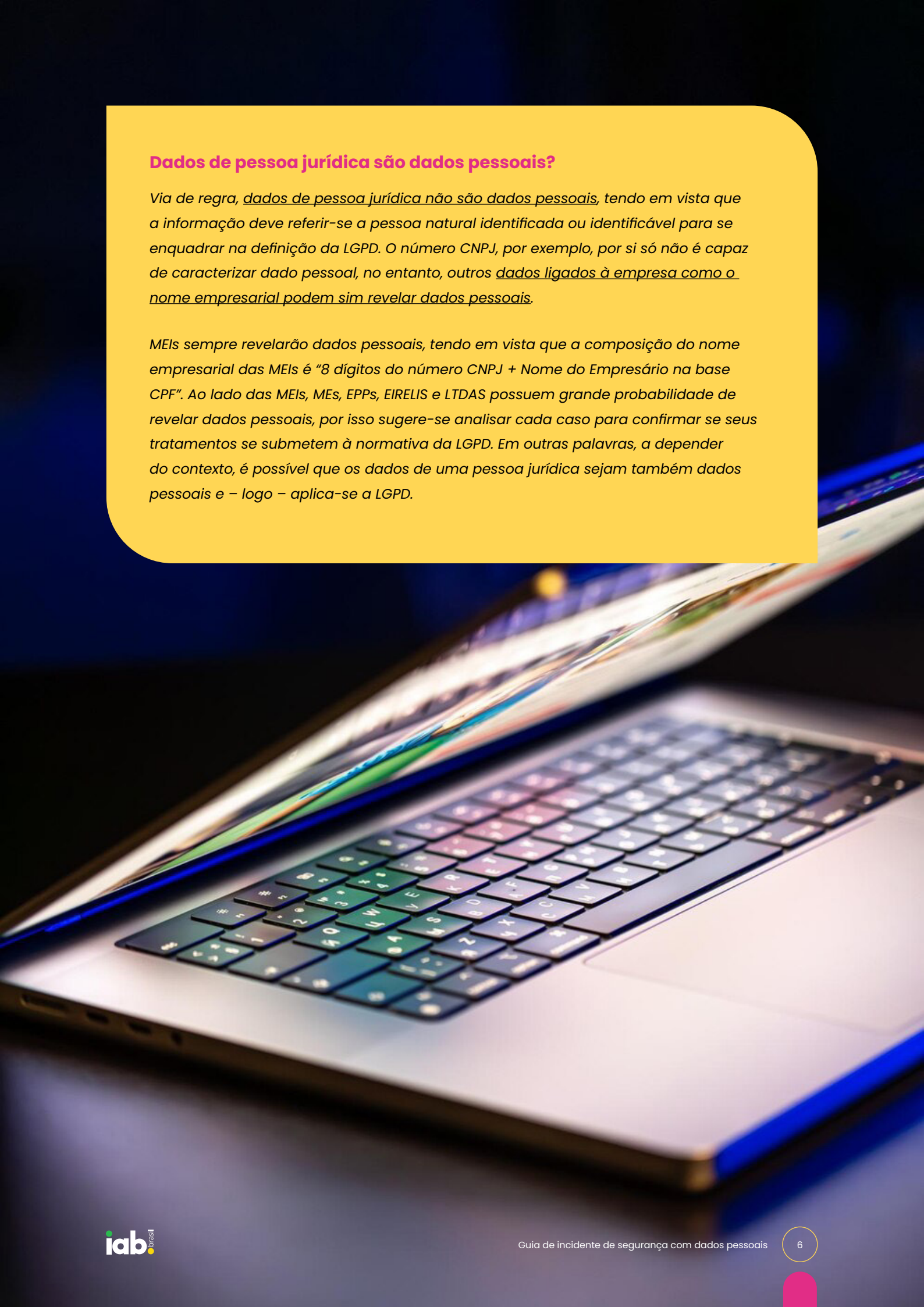
Tratamento de dados pessoais é toda operação realizada com dados pessoais, como a coleta, produção, recepção, classificação, utilização, dentre outras. Em outras palavras, tratamento é basicamente qualquer uso de um dado pessoal, desde o mero armazenamento até análises aprofundadas. Assim como com 'dados pessoais', a LGPD também dá uma definição ampla para 'tratamento de dados'.

Anonimização e pseudonimização: dados anonimizados são dados que passaram por um processo de descaracterização de forma que não seja possível relacioná-los a um titular, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Como não é possível chegar direta ou indiretamente a um Titular via dados anonimizados, eles não são considerados dados pessoais — logo, não há aplicação da LGPD. Note, porém, que se os dados apenas foram mascarados e ainda puderem permitir a identificação de pessoas quando combinados com outras informações, estaremos falando de dados pseudonimizados, aos quais a lei se aplica normalmente.

Dados de pessoa jurídica são dados pessoais?

Via de regra, dados de pessoa jurídica não são dados pessoais, tendo em vista que a informação deve referir-se a pessoa natural identificada ou identificável para se enquadrar na definição da LGPD. O número CNPJ, por exemplo, por si só não é capaz de caracterizar dado pessoal, no entanto, outros dados ligados à empresa como o nome empresarial podem sim revelar dados pessoais.

MEIs sempre revelarão dados pessoais, tendo em vista que a composição do nome empresarial das MEIs é "8 dígitos do número CNPJ + Nome do Empresário na base CPF". Ao lado das MEIs, MEs, EPPs, EIRELIS e LTDAS possuem grande probabilidade de revelar dados pessoais, por isso sugere-se analisar cada caso para confirmar se seus tratamentos se submetem à normativa da LGPD. Em outras palavras, a depender do contexto, é possível que os dados de uma pessoa jurídica sejam também dados pessoais e – logo – aplica-se a LGPD.



2. Quem é quem no tratamento de dados pessoais?

A principal parte nas atividades de tratamento de dados pessoais é o **titular dos dados** ("titular"). Ele é a pessoa natural a quem se referem os dados pessoais que são objeto do tratamento e, logo, a pessoa que é ou pode ser identificada por eles.

Em relação às partes que realizam o tratamento dos dados pessoais do Titular, temos duas figuras centrais que são definidos como agentes de tratamento:

- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento dos dados pessoais. Em outras palavras, é o agente responsável por definir como, quando e para quê os dados pessoais serão tratados.

Exemplo: *a empresa "X" atua como controladora dos dados pessoais de seus próprios funcionários em atividades de RH, como contratação, avaliação periódica e de desenvolvimento, concessão de benefícios, entre outras.*

- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais em nome do Controlador. Ou seja, o agente que executa o tratamento dos dados conforme as definições do Controlador. Ainda que por vezes tenha um grau de expertise no serviço ou fornecimento, o Operador não tem autonomia para decidir, determinar ou gerenciar qualquer aspecto relativo ao tratamento dos dados pessoais, principalmente as finalidades do tratamento.

Exemplo: *caso a empresa "X" contrate a Empresa "Y" para digitalizar planilhas que contêm dados pessoais de terceiros, a Empresa "Y" estará atuando como operadora destes dados, enquanto a Empresa "X" será a controladora.*

Temos, ainda, o(a) Encarregado(a) ou Data Protection Officer ("DPO"), que é a pessoa indicada pelo agente de tratamento para atuar como canal de comunicação entre a empresa, os titulares dos dados e a ANPD.

Uma empresa contrata atores de uma agência para a realização de uma campanha de marketing. A agência é apenas operadora dos dados pessoais dos modelos ou também pode ser considerada controladora?

No caso, ambas as empresas serão controladoras destes dados pessoais. Ainda que a empresa tenha contratado uma agência terceirizada para a seleção de modelos para uma campanha, todas as decisões referentes à seleção e escolha dos modelos serão da agência terceirizada. Não há qualquer problema ou incompatibilidade com a LGPD no fato de duas empresas serem controladoras de dados pessoais, principalmente quando cada empresa tem suas próprias finalidades específicas para o tratamento destes dados.

Por fim, temos a **ANPD** - Autoridade Nacional de Proteção de Dados, órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

3. O que é um incidente de segurança com dados pessoais?

Um incidente de segurança refere-se a qualquer evento adverso confirmado que compromete a confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais. Incidentes **confirmados** devem ser imediatamente avaliados pelos times competentes para definir se é ou não o caso de comunicação à ANPD e aos titulares.

- **Confidencialidade:** propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, empresas, sistemas, órgãos ou entidades não autorizados.

Exemplo: um colaborador de uma empresa de marketing envia, acidentalmente, informações de clientes para um destinatário externo não autorizado, expondo dados pessoais como endereços e histórico de compras.

- **Integridade:** propriedade pela qual se assegura que o dado pessoal não foi modificado ou destruído de maneira não autorizada ou acidental.

Exemplo: um erro no sistema de CRM corrompe os dados de contato de clientes, causando alterações incorretas e prejudicando o envio de campanhas de marketing.

- **Disponibilidade:** propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa natural ou determinado sistema, órgão ou entidade devidamente autorizados.

Exemplo: um ataque de ransomware bloqueia o acesso a uma base de dados com informações de clientes, impedindo que a empresa utilize esses dados para campanhas e dê suporte aos clientes.

- **Autenticidade:** propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

Exemplo: a falsificação de documentos oficiais, como RG ou carteira de trabalho, para fins como obtenção de crédito, benefícios sociais ou usurpação de identidade.

Nem todo incidente de segurança envolve Dados Pessoais. Incidentes relacionados a dados operacionais, comerciais ou técnicos – ou seja, que não envolvem dados pessoais – bem como relativos a dados anonimizados não estão sujeitos à LGPD e, portanto, não geram obrigações legais como a notificação à Autoridade Nacional de Proteção de Dados (ANPD) ou aos titulares.

Além disso, a mera existência de uma vulnerabilidade em um sistema de informação não necessariamente constitui um incidente de segurança. A exploração da referida vulnerabilidade, no entanto, pode resultar em um incidente.

4. Como identificar o grau de risco do incidente?

A identificação do nível de risco do incidente auxiliará na sua gestão, na definição dos próximos passos e no entendimento de pontos críticos da resposta ao incidente, bem como a necessidade ou não de comunicação à ANPD e aos titulares.

A tabela abaixo foi desenvolvida para auxiliar na classificação dos incidentes com base no nível de risco envolvido. Ela fornece critérios objetivos que permitem a identificação de um incidente de baixo, médio ou alto risco, considerando fatores como categoria de dado afetado, volume e impacto.

PERGUNTA	RESPOSTA
O incidente envolveu algum dos dados descritos na coluna ao lado?	☐ Dados pessoais sensíveis *(dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico)*. ☐ Dados de crianças, de adolescentes ou de idosos. ☐ Dados financeiros. ☐ Dados de autenticação em sistemas. ☐ Dados protegidos por sigilo legal, judicial ou profissional.
O incidente envolveu dados em larga escala? ***[Larga escala: O incidente envolveu 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].*** ***Observação: esta é uma questão subjetiva que deve ser analisada caso a caso, levando em consideração a realidade da empresa, pois o conceito e requisitos característicos do que é entendido como larga escala ainda não foram estabelecidos no Brasil.***	☐ Sim ☐ Não Justifique: _____

PERGUNTA	RESPOSTA
O incidente pode afetar significativamente interesses e direitos fundamentais dos titulares?	☐ A atividade de tratamento de dados pode impedir o exercício de direitos. ☐ A atividade de tratamento de dados pode impedir a utilização de um serviço. ☐ A atividade de tratamento de dados pode ocasionar danos materiais ou morais aos indivíduos *(ex: tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade)*.

5. Quando devo comunicar um incidente de segurança envolvendo dados pessoais?

Nem todo incidente de segurança deve ser comunicado à ANPD. Um incidente precisa ser comunicado se atender, cumulativamente, aos seguintes critérios: (i) envolver dados pessoais; e (ii) acarretar risco ou dano relevante aos titulares dos dados.

A comunicação, portanto, deve ocorrer sempre que um incidente, após confirmado, envolver dados pessoais e possa causar risco ou dano relevante aos titulares. Um incidente será considerado causador de risco ou dano relevante quando afetar significativamente os interesses ou direitos fundamentais dos titulares e, cumulativamente, envolver um ou mais dos seguintes critérios:

i. Tratamento de dados pessoais sensíveis;

ii. Tratamento de dados de crianças, de adolescentes ou de idosos;

iii. Tratamento de dados financeiros;

iv. Tratamento de dados de autenticação em sistemas;

v. Tratamento de dados protegidos por sigilo legal, judicial ou profissional; ou

vi. Tratamento de dados em larga escala.

Situações que podem configurar riscos relevantes e/ou danos relevantes incluem, a título exemplificativo:

- Impedimento ao exercício de direitos fundamentais ou a utilização de serviços essenciais;
- Acesso à base de dados sensíveis, como informações de saúde, religião ou orientação sexual;
- Discriminação;
- Violação à integridade física;
- Possibilidade de fraudes, como roubo de identidade ou informações financeiras detalhadas, ocasionando danos materiais; e
- Impacto concreto sobre a honra, imagem, ou reputação dos titulares.

Em hipótese alguma um colaborador deve fazer a comunicação do incidente diretamente para a ANPD. Assim que for identificado um possível incidente, o colaborador deve acionar a equipe de privacidade ou o encarregado pelo tratamento de dados pessoais na empresa.

A **construção da comunicação do incidente para a ANPD é um trabalho multidisciplinar.** Conforme o porte da empresa, é essencial que outras equipes, além do time de privacidade, estejam envolvidas no processo de construção da comunicação do incidente, como Segurança ou Tecnologia da informação, Compliance e o Jurídico. É importante contar também com o apoio de escritórios externos especializados no assunto, de forma a tirar dúvidas e confirmar a abordagem.

A tabela abaixo ajudará a entender melhor o incidente investigado e o mapeamento da necessidade, ou não, de comunicação:

PERGUNTA	RESPOSTA
De quem são os dados pessoais envolvidos no incidente?	☐ Colaboradores ☐ Prestadores de serviços ☐ Clientes ☐ Outros: _____
Quais as categorias das titulares afetadas pelo incidente?	☐ Adultos ☐ Crianças e/ou adolescentes ☐ Idosos ☐ Outros: _____
Qual a quantidade aproximada de titulares afetadas pelo incidente?	

PERGUNTA	RESPOSTA
Quais dados pessoais estão envolvidos no incidente?	☐ Dados básicos de identificação *(ex: nome, sobrenome, data de nascimento, matrícula)*. ☐ Dados de contato *(ex: telefone, endereço, e-mail)*. ☐ Número de documentos de identificação oficial *(ex: RG, CPF, CNH, passaporte)*. ☐ Cópias de documentos de identificação oficial *(ex: cópia do RG, cópia do CPF, cópia da CNH)*. ☐ Dados de meios de pagamento *(ex: cartão de crédito/débito)*. ☐ Dado financeiro ou econômico *(ex: dados de salário)*. ☐ Dados protegidos por sigilo profissional/legal. ☐ Nomes de usuário de sistemas de informação. ☐ Dado de autenticação de sistema *(ex: senhas, PIN ou tokens)*. ☐ Imagens / áudio / vídeo ☐ Dado de geolocalização *(ex: coordenadas geográficas)*. ☐ Outros: _____
Quais dados pessoais sensíveis estão envolvidos no incidente? ***[Os dados pessoais sensíveis estão restritos às categorias listadas ao lado. Qualquer dado que não se enquadre nessas categorias é considerado dado pessoal comum].***	☐ Origem racial ou étnica *(ex: declaração de raça ou etnia)*. ☐ Convicção religiosa. ☐ Opinião política. ☐ Referente à saúde *(ex: resultados de exames médicos, diagnósticos de condições de saúde)*. ☐ Biométrico *(ex: impressões digitais, reconhecimento facial)*. ☐ Genético *(ex: testes de DNA, dados de sequenciamento genético)*. ☐ Referente à vida sexual. ☐ Filiação a organização sindical, religiosa, filosófica ou política *(ex: associação a sindicatos, filiação partidária)*.
Quais as prováveis consequências para os titulares decorrentes do incidente?	☐ Danos morais ☐ Danos materiais. ☐ Violação à integridade física. ☐ Discriminação social. ☐ Danos reputacionais. ☐ Roubo de identidade. ☐ Engenharia social / fraudes. ☐ Limitação de acesso a um serviço. ☐ Exposição de dados protegidos por sigilo profissional/legal.

PERGUNTA	RESPOSTA
	☐ Restrições de direitos. ☐ Perda de acesso a dados pessoais. ☐ Outros: _____
O incidente pode gerar consequências específicas para crianças, adolescentes ou idosos? ***[As consequências do incidente são específicas ou amplificadas devido ao fato de os indivíduos serem crianças, adolescentes ou idosos?]***	☐ Sim ☐ Não Caso "Sim", explique quais consequências do incidente serão específicas ou amplificadas em virtude de os indivíduos afetados serem crianças, adolescentes ou idosos: _____ _____ _____

6. Como fazer a comunicação de um incidente envolvendo dados pessoais?

Como regra, a comunicação de um incidente deve ser feita à **ANPD** e aos **titulares** no **prazo de até três dias úteis** após a confirmação do incidente e de seus riscos e/ou danos, ou seja, a constatação de que o incidente ocorreu e que há riscos relevantes e/ou danos relevantes aos titulares. É possível a realização de uma comunicação preliminar, caso a empresa não tenha todas as informações necessárias dentro desse prazo.

Além disso, a comunicação aos titulares deve ser feita de maneira clara, direta e com linguagem simples.

Comunicação à ANPD:

Meios: a comunicação à ANPD deve ser realizada pelo sistema SEI (Sistema Eletrônico de Informações[1]) utilizado pela Autoridade para peticionamento eletrônico. Esse sistema é a principal via para formalizar notificações de incidentes de segurança.

Conteúdo: segundo o art. 48 da LGPD e a Resolução CD/ANPD nº 15 de 2024, a comunicação deve conter:

- **Descrição da natureza do incidente:** detalhamento sobre o que ocorreu, como por exemplo se houve vazamento de dados, ataque cibernético ou outra forma de comprometimento.
- **Dados afetados:** quais categorias de informações pessoais foram expostas ou comprometidas no incidente. As categorias devem ser informadas nos termos do artigo 3º, inciso III da Resolução e, portanto, definidas de acordo com o contexto de sua utilização: dados de identificação pessoal, dados de autenticação em sistemas, dados financeiros.
- **Número de titulares impactados:** Estimativa ou número exato de pessoas afetadas pelo incidente, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos.
- **Medidas adotadas para mitigar os danos:** ações corretivas ou preventivas adotadas para minimizar os riscos e danos aos titulares, como por exemplo bloqueio de acessos indevidos, troca de senhas, reembolso de valores, cancelamento de credenciais e melhoria de processos de segurança após o incidente, observados os segredos comercial e industrial.

[1] https://www.gov.br/anpd/pt-br/canais_atendimento/peticionamento-eletronico-anpd

- **Avaliações de riscos:** os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares.
- **Prazos:** a data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pela empresa. No caso de a comunicação nã o ter sido realizada no prazo previsto de 3 (três) dias úteis, os motivos da demora.

Além disso, a ANPD poderá solicitar documentos e informações mais detalhadas a partir do recebimento da comunicação.

A ANPD oferece em seu site um Formulário para Comunicação de Incidente de Segurança[2], o qual deve ser utilizado em sua versão mais recente, que deverá ser preenchido e anexado no sistema SEI no momento da comunicação pela empresa. Por este motivo, é essencial que as empresas sempre utilizem a versão vigente no momento da submissão da comunicação no sistema.

Importante reforçar que as informações compartilhadas com a ANPD podem ser tidas como sigilosas, mas não de forma automática. A Resolução 15/2014 reforça que a empresa deve solicitar o sigilo à ANPD de maneira fundamentada.

Comunicação aos titulares:

Meios: a comunicação com os titulares deve ser feita de forma direta e individualizada, sempre que possível. Os meios preferenciais incluem:

- **Os canais usualmente utilizados para contatar o titular, como e-mail** ou **telefone:** para os casos em que a identificação individual e, logo, o contato com os titulares individualmente é possível.

- **Ampla divulgação:** Caso não seja possível identificar individualmente os titulares afetados, a comunicação pode ser feita por meio de avisos públicos, como no site ou em redes sociais da empresa, seus aplicativos ou por meios de comunicação amplos, garantindo que todos os potenciais afetados venham a ter conhecimento do incidente.

Caso a comunicação direta e individualizada mostre-se inviável ou não seja possível identificar, parcial ou integralmente, os titulares afetados, a empresa deverá comunicar a ocorrência do incidente pelos meios de divulgação disponíveis, tais como: seu site, aplicativos, mídias sociais e canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, três meses.

[2] https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis

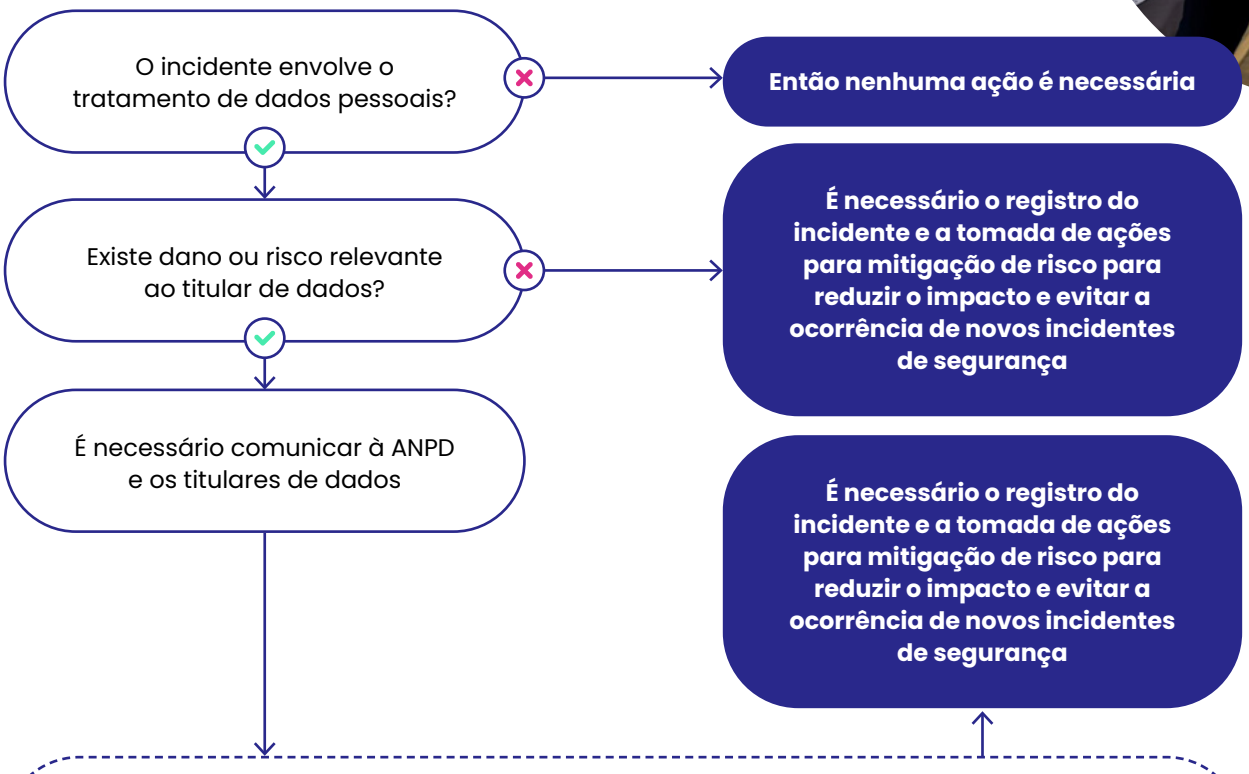
Conteúdo: a comunicação aos titulares deve incluir, minimamente:

a. Descrição do incidente: o que e quando aconteceu, qual a extensão do incidente e quais categorias de dados foram afetadas.

b. Medidas de técnicas e de segurança adotadas: quais ações foram tomadas para controlar a situação e evitar ou reverter o problema, observados os segredos comercial e industrial.

c. Orientações aos titulares: informações sobre como os titulares podem se proteger e reduzir potenciais danos, como mudança de senhas ou uso de serviços de monitoramento, e contato da empresa para maiores informações.

d. Data: quando o controlador tomou conhecimento do incidente de segurança. No caso de a comunicação não ter sido feita no prazo três dias úteis contados do conhecimento pela empresa, os motivos da demora.



Comunicado à ANPD:

- **Meios:** O sistema SEI deve ser utilizado para peticionamento eletrônico do comunicado
- **Conteúdo:** Descrição da natureza do incidente, dados afetados, número de titulares impactados e as medidas adotadas para mitigar os danos.

Comunicado aos titulares:

- **Meios:** A comunicação deve ser direta (via e-mail, telefone) ou, caso não seja possível identificar os titulares, por meio de ampla divulgação (como no site da empresa).
- **Conteúdo:** Descrição do incidente, medidas de segurança adotadas, e orientações sobre como os titulares podem se proteger.

7. Dicas e boas práticas

O que fazer

- Ao identificar um incidente de segurança, comunique imediatamente ao DPO/Encarregado da empresa.
- Consulte e siga as orientações da equipe responsável por tratamento de dados.
- Assegure que as pessoas adequadas/necessárias estejam envolvidas em todo o momento ao identificar um incidente.
- Coopere com o time de privacidade ou área responsável e demais áreas envolvidas para investigação do incidente e a elaboração de comunicado à ANPD e aos titulares afetados, sempre que o time de privacidade julgar a comunicação necessária.
- Coopere com a investigação para confirmação da origem do incidente de segurança e os responsáveis pela sua ocorrência - se houver. Elabore um relatório minucioso com os fatos, histórico e conclusões da investigação.
- Reúna informações sobre o incidente de diversas fontes.
- Implemente medidas para mitigar os danos causados pelo incidente de segurança, como o isolamento de sistemas comprometidos ou a correção de vulnerabilidades.
- Quando aplicável, colete dados voláteis e arquivos de log pré-determinados. Também colete logs baseados na rede para análise futura.
- Mantenha, por no mínimo 5 anos, um registro descrevendo o modo que cada incidente de segurança ocorreu, incluindo a data e horário da descoberta, os dados e os titulares afetados, a avaliação do risco e os possíveis danos aos titulares, as medidas de mitigação e a forma de comunicação ou justificativa para sua ausência.
- Revise e reforce políticas e práticas de segurança para prevenir a ocorrência de novos incidentes de segurança.

O que não fazer

- Não deixe de se manifestar quando identificar um incidente de segurança! Comunique imediatamente ao DPO/Encarregado da empresa, mesmo que o problema ainda não tenha sido resolvido.
- Não deixe de registrar a ocorrência de incidentes de segurança conforme suas políticas internas.
- Não adie o processo de avaliação e mitigação dos riscos causados pelo incidente de segurança. A ação deve ser iniciada imediatamente após a descoberta do incidente.
- Não investigue o incidente por conta própria, envolva o time de Privacidade e demais necessários considerando a governança e procedimento(s) interno(s) da sua empresa.
- Não aja de forma impulsiva sem um planejamento prévio.
- Não discuta o incidente com outros colaboradores ou quaisquer terceiros, não autorizados, a menos que devidamente instruído.
- Não desligue, encerre ou faça o backup dos sistemas afetados, a menos que devidamente instruído.
- Não instale ou execute softwares desconhecidos.
- Não mantenha contato com pessoas que se apresentem como perpetradores de um ataque ou inicie negociações de “resgates” ou compensações financeiras, busque auxílio de um especialista.

Agradecimentos

Redação

Leonardi Advogados

Revisão

Grupo de Trabalho

Bernardo Araujo *(Publicis)*

Cecília Coutinho *(Pinheiro Neto)*

Fernanda Maia *(Leonardi Advogados)*

Mariana Bonelli *(TikTok)*

Natália Kuchar *(Google)*

Nathalia Silva *(AD Digital)*

Uhala Guedes da Silva *(Rakuten)*

Projeto Gráfico e Diagramação

Marcelo Vila Nova

IAB Brasil

Denise Porto Hruby - CEO

Cristiane Duarte - Diretora de Produtos

Jovanka de Genova - Gerente de Conteúdo e Educação

Beatriz Falcão - Gerente de Relações Governamentais

Cristina de Paula - Coordenadora de Conteúdo

Talita Nunes - Community Manager

Este material foi relevante para sua rotina de trabalho?
Responda nossa pesquisa e nos ajude a melhorar cada vez mais nossos conteúdos.

iabbrasil.com.br