Comunicação de incidente de segurança

Publicado em 23/12/2022 10h34 Atualizado em 16/03/2023 19h04

A Comunicação de Incidente de Segurança se destina exclusivamente aos **controladores de dados pessoais**. Para noticiar a ocorrência de um incidente com seus dados pessoais ou de terceiros, utilize o canal de denúncia da ANPD.

Orientações Gerais

A Lei Geral de Proteção de Dados (LGPD) determina aos agentes de tratamento de dados pessoais (controladores e operadores) a adoção de medidas para prevenir a ocorrência de danos aos titulares em virtude de suas atividades.
Na eventualidade de um incidente de segurança, uma importante medida de mitigação de danos é a comunicação da ocorrência aos titulares dos dados pessoais violados. Dessa forma, eles poderão tomar conhecimento do ocorrido e adotar medidas de precaução para mitigar os riscos a que foram expostos em razão do incidente.

A LGPD impõe aos controladores, em seu art. 48, o dever de comunicar aos titulares e à ANPD a ocorrência de incidentes que possam causar **riscos ou danos relevantes** aos titulares. O cumprimento dessa obrigação junto à ANPD e aos titulares afetados, se dá no processo de Comunicação de Incidente de Segurança (CIS).

É a Coordenação-Geral de Fiscalização (CGF) da ANPD quem recebe as comunicações de incidente de segurança e dá a elas o tratamento necessário, bem como é a responsável por fiscalizar e aplicar as sanções administrativas cabíveis.

Cabe ao agente regulado solicitar à ANPD o sigilo de informações protocoladas nos processos relativas à sua atividade empresarial, como dados e informações técnicas, econômico-financeiras, contábeis, operacionais, cuja divulgação possa representar violação a segredo comercial ou a industrial, nos termos do §2º Art. 5º do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador.

Procedimento para Comunicação de Incidente à ANPD

A comunicação de incidentes de segurança à ANPD deve ser realizada pelo encarregado pela proteção de dados ou por um representante legalmente constituído do controlador, por meio do preenchimento do formulário disponibilizado abaixo.

O formulário deve ser protocolado eletronicamente por meio do Peticionamento Eletrônico do SUPER.BR (Sistema Único de Processo Eletrônico em Rede).

Durante o protocolo, selecione o tipo de processo "**ANPD – Comunicados de Incidentes à Autoridade Nacional de Proteção de Dados**". Junte ao processo o formulário preenchido, **preferencialmente em formato PDF**, os documentos complementares e a documentação comprobatória da legitimidade para representação do controlador junto à ANPD.

Se cabível, ato de designação do encarregado, procuração e atos constitutivos tais como contrato ou estatuto social.

O Portal de Assinatura Eletrônica da plataforma GOV.BR pode ser utilizado para assinatura do formulário eletrônico, caso o usuário possua nível de confiabilidade "prata" ou "ouro", sem prejuízo da possibilidade de utilização de qualquer outro meio previsto pela Lei Nº 14.063, de 23 de Setembro de 2020.

Após a finalização, um Recibo Eletrônico de Protocolo será gerado automaticamente pelo sistema e incluído no processo.

- Formulário de Comunicação de Incidente de Segurança
- Instruções para Cadastro e Acesso ao SUPER.BR
- Manual do Peticionamento Eletrônico
- Instruções para Assinatura Eletrônica GOV.BR

Em caso de dificuldade no cadastro no SUPER.BR, entre em contato com a Coordenação de Documentação da Secretaria Geral da Presidência da República por meio do e-mail codoc.protocolocentral@presidencia.gov.br.

Dúvidas a respeito do procedimento de comunicação de incidentes de segurança devem ser encaminhadas à CGF, por meio do e-mail fiscalizacao@anpd.gov.br.

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

Dúvidas Frequentes Sobre Incidentes de Segurança

O que é um incidente de segurança com dados pessoais?

É um evento adverso confirmado que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais. Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda indevidas ou acessos não autorizados a dados pessoais, independentemente do meio em que estão armazenados.

Incidentes podem ocorrer de forma acidental, como o envio de informações para o destinatário incorreto, ou em decorrência de atos intencionais, como a invasão de um sistema de informação ou o furto de um dispositivo de armazenamento de dados.

Os incidentes de segurança não se restringem às violações da confidencialidade, abrangem também eventos de perda ou indisponibilidade dados pessoais. São exemplos de incidentes de segurança o sequestro de dados (ransomware), o acesso não autorizado a dados armazenados em sistemas de informação e a publicação não intencional de dados dos titulares.

Nem todo incidente de segurança da informação envolve dados pessoais. Incidentes que envolvam somente dados anonimizados ou que não estejam relacionados a pessoas naturais identificáveis não precisam ser comunicados à ANPD.

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

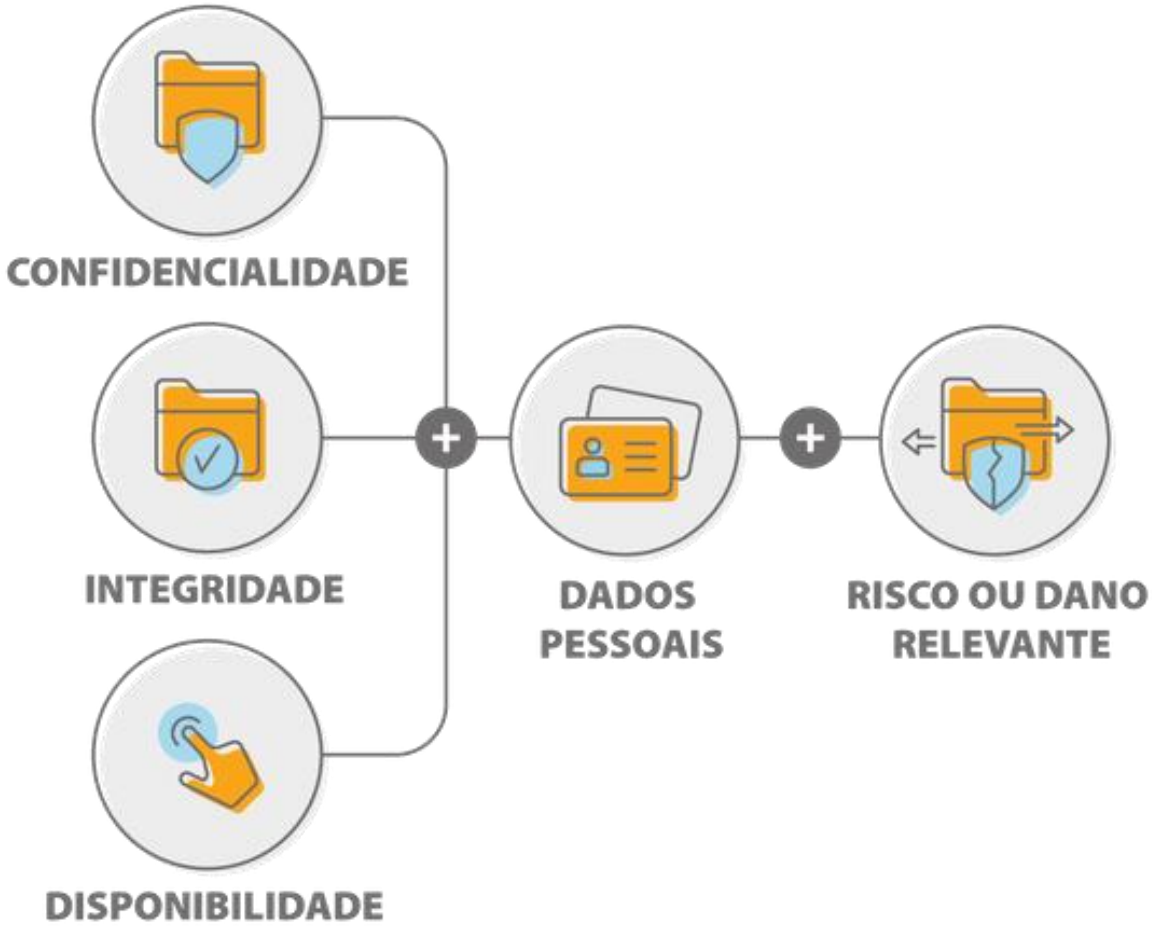
Cabe ao controlador identificar, tratar e avaliar o risco dos incidentes de segurança que afetem suas operações de tratamento de dados pessoais.

Quais incidentes de segurança precisam ser comunicados aos titulares e à ANPD?

Somente os controladores sujeitos à Lei Geral de Proteção de Dados têm obrigação de comunicar os incidentes à ANPD.

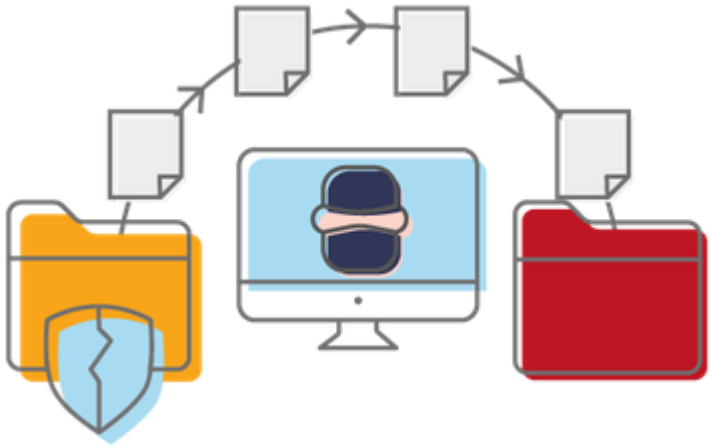
Um incidente precisa ser comunicado se atender, cumulativamente, aos seguintes critérios:

1. Tenha a ocorrência confirmada pelo agente.
2. Envolva dados pessoais sujeitos à LGPD.
3. Acarrete risco ou dano relevante aos titulares dos dados.



A figura mostra os aspectos (confidencialidade, integridade, disponibilidade + Dados Pessoais + Risco ou Dano relevante aos titulares) que devem ser analisados na avaliação da necessidade de comunicação do incidente.

Veja exemplos de incidentes capazes de gerar risco ou dano relevante aos titulares:



A invasão de uma rede de computadores de uma instituição financeira por um agente malicioso que realize a cópia não autorizada de uma base de dados contendo dados pessoais dos correntistas, tais como extratos bancários, números de cartões de crédito e senhas viola o sigilo bancário dos titulares e os expõe a risco de fraudes e danos morais e materiais.

A indisponibilidade prolongada de um sistema utilizado por uma rede hospitalar em razão de um incidente de sequestro de dados, impedindo o acesso aos dados dos pacientes ou a realização de procedimentos médicos, pode expor dados pessoais sensíveis dos titulares e causar-lhes riscos ou danos à saúde.

A perda ou roubo de documentos ou dispositivos de armazenamento de dados que contenham dados pessoais protegidos por sigilo profissional, cópia de documentos de identificação oficial e dados de contato dos titulares pode expô-los a riscos reputacionais e de sofrer fraudes financeiras.

Nem todo incidente de segurança deve ser comunicado à ANPD. Cabe ao controlador avaliar os riscos e impactos aos titulares decorrentes do incidente, e verificar a necessidade de realizar a comunicação.

O que deve ser considerado na avalição de risco de um incidente com dados pessoais?

Na avaliação de risco do incidente, devem ser considerados, dentre outros aspectos:

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

Um mesmo tipo incidente pode ou não ser considerado capaz de causar risco ou dano relevante em função da combinação desses critérios.

Um incidente de roubo de um dispositivo eletrônico, por exemplo, pode ou não ser capaz de causar um risco relevante aos titulares de dados. A avaliação vai depender do tipo de dado armazenado, do contexto da atividade de tratamento e do fato de os dados estarem ou não protegidos por criptografia.

São considerados incidentes capazes de causar risco ou dano relevante aqueles que possam causar aos titulares danos materiais ou morais, expô-los a situações de discriminação ou de roubo de identidade, especialmente se envolverem dados em larga escala, sensíveis e de grupos vulneráveis como crianças e adolescentes ou idosos.

Qual o prazo para comunicar um incidente de segurança?

A lei determina que os incidentes de segurança devem ser comunicados aos titulares de dados e à Autoridade em prazo razoável, que será definido futuramente pela ANPD em um regulamento próprio.

Para preservar os direitos dos titulares e tentar diminuir os possíveis prejuízos que um incidente de segurança possa causar, recomenda-se que a comunicação seja feita o mais breve possível, em **até 2 (dois) dias úteis** da ciência do fato.

A comunicação voluntária do incidente pelo controlador é demonstração de transparência, cooperação e boa-fé do agente e será considerada em eventual ação de fiscalização da ANPD.

A demora injustificada na comunicação de incidente de segurança que possa causar risco ou dano relevante aos titulares pode sujeitar os agentes às sanções administrativas previstas na LGPD.

Como proceder se informações sobre o incidente não estiverem disponíveis no prazo recomendado pela ANPD?

Excepcionalmente, na hipótese de o controlador não dispor de informações completas a respeito do incidente **ou não conseguir notificar a todos os titulares no prazo recomendado**, a comunicação à ANPD poderá ser realizada em etapas: **preliminar e complementar**.

A impossibilidade de realizar a comunicação completa deve ser devidamente justificada pelo controlador. A complementação deverá ser encaminhada o mais breve possível e, no mais tardar, em 30 dias corridos contados da comunicação preliminar.

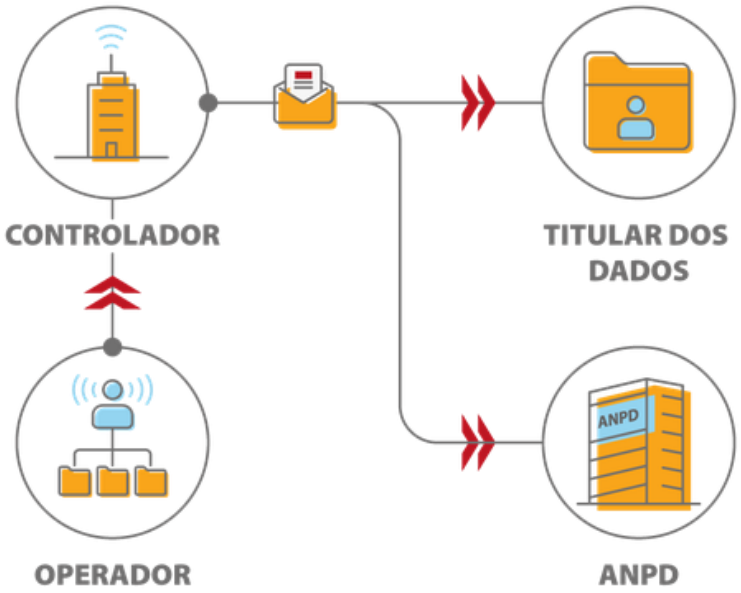
A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar, por meio de petição intercorrente.

A comunicação preliminar é insuficiente para o cumprimento da obrigação estabelecida pelo art. 48 da LGPD e deve ser complementada pelo controlador no prazo estabelecido.

Qual o papel do operador no processo de comunicação de incidentes de segurança?

A obrigação legal de comunicar o incidente de segurança aos titulares e à ANPD é do controlador, nos termos do art. 48 da LGPD. No entanto, a obrigação de adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais se estende a todos os agentes de tratamento de dados, inclusive aos operadores.

Quando um incidente de segurança ocorre, o operador deverá informar o fato, sem demora injustificada, ao controlador dos dados. Todas as informações necessárias à comunicação do incidente de segurança à ANPD e aos titulares deverão ser fornecidas pelo operador ao controlador.



Recomenda-se que as obrigações referentes à comunicação de incidentes entre controladores e operadores sejam estabelecidas em contrato, para que possam agilizar o procedimento e minimizar os riscos aos titulares de dados pessoais.

Como comunicar um incidente de segurança aos titulares de dados?

A comunicação deve ser realizada o mais rápido possível, uma vez que o controlador constate que o incidente pode causar risco ou dano relevante aos titulares. Isso permite aos titulares mitigarem eventuais impactos negativos decorrentes do incidente.

A comunicação deve ser feita de forma individual e diretamente aos titulares, sempre que possível. Pode ser realizada por quaisquer meios tais como e-mail, SMS, carta ou mensagem eletrônica e, preferencialmente, através do canal já habitualmente utilizado pelo agente para se comunicar com o titular.

Se, apesar de confirmada a ocorrência do incidente, não foi possível individualizar os titulares afetados, pode ser necessário comunicar a todos cujos dados estejam presentes na base de dados violada.

Excepcionalmente, e de forma justificada, pode ser feita a comunicação indireta por meio de publicação em meios de comunicação. O meio utilizado deve ser capaz de alcançar o maior número possível de titulares, e deve ser dado o devido destaque à divulgação.

O comunicado aos titulares deve fazer uso de linguagem clara e conter, ao menos, as seguintes informações:

1. resumo e data da ocorrência do incidente;
2. descrição dos dados pessoais afetados;
3. riscos e consequências aos titulares de dados;
4. medidas tomadas pelo controlador e as recomendadas aos titulares para mitigar os efeitos do incidente, se cabíveis;
5. dados de contato do encarregado do controlador para que os titulares possam solicitar informações adicionais a respeito do incidente.

A ANPD poderá solicitar ao controlador, a qualquer tempo, a apresentação de cópia do comunicado aos titulares para fins de fiscalização.
Não é necessário encaminhar à ANPD a lista de titulares afetados, ou seus dados de contato para comprovação da comunicação.

O que ocorre após a comunicação de incidente à ANPD?

As comunicações de incidente de segurança são recebidas e tratadas pela Coordenação-Geral de Fiscalização (CGF) da ANPD. A gravidade do incidente será considerada na priorização da análise dos comunicados recebidos.

Caso o controlador já tenha comunicado a ocorrência do incidente aos titulares de dados e, após análise, a CGF não identificar infração à LGPD e nem a necessidade de adoção de medidas adicionais, o processo será arquivado.

Se a comunicação aos titulares não tiver sido realizada ou for considerada inadequada, pode ser determinada a sua realização ou correção em sua forma ou conteúdo. Se necessário, poderá ser determinado ao controlador a adoção de medidas adicionais para mitigação dos efeitos do incidente, como sua ampla divulgação.

Além disso, a CGF avaliará a possível ocorrência de infrações à LGPD e aplicará, se cabível, as sanções administrativas previstas no art. 52 da LGPD, em procedimento administrativo que possibilite a ampla defesa e o contraditório às partes.
Poderão ser aplicadas medidas preventivas e sanções, dentre outras situações, nos casos em que o controlador:

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

FISCALIZAÇÃO RESPONSIVA

A ANPD adota um modelo de fiscalização responsivo, como previsto no

Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador.

Isso permite que a fiscalização não apenas aplique sanções, mas também adote medidas orientativas e preventivas para reconduzir os agentes à conformidade com a lei e remediar situações que acarretem risco aos titulares. O não atendimento às medidas preventivas pode agravar a sanção aplicada ao agente em eventual processo administrativo sancionador.

Busca-se, dessa maneira, gerar posturas de colaboração entre a ANPD e os agentes de tratamento de dados e a solução.

Transcrição na integra de publicação de 23/12/2022 10h34 em:
https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis