



Opice

BLUM

Redefinindo os limites do possível.

cert.br nie.br egi.br



Guilherme Ochsendorf de Freitas



Especialista em Direito e Tecnologia da Informação pela POLI-USP, MBA em Gestão Estratégica em Tecnologia da Informação pela FEA-RP - USP.

Certificado em Cibersegurança pelo ISC², CISCO e Resposta a Incidente pela Carnegie Mellon University (CERT.br) e FGV.

Advogado do Time de Resposta a Incidentes no Opice Blum e Professor em Cursos de Pós-Graduação em Direito Digital.

Coautor dos livros "LGPD para Pequenas Empresas - Teoria e Prática" e "*Ransomware 360°* - Abordagens Multidisciplinares



<https://br.linkedin.com/in/guilhermeochsendorf>

Da Teoria à Prática: Um Panorama sobre Proteção de Dados Pessoais e Gestão de Incidentes de Segurança

Panorama sobre Proteção de Dados Pessoais:
Deveres do provedores de internet e administradores de redes



Objetivos deste Bloco

- Período de retenção
- Porta lógica
- Ação judicial para quebra de sigilo.
- Relatório de Impacto à Proteção de Dados Pessoais (RIPD)



Provedores de conexão obrigação retenção de dados por 1 (um) ano (art. 13);

Provedores de aplicação, obrigação retenção de dados por 6 (seis) meses (art. 15).

- A base legal para essa guarda, sob a ótica da LGPD, é o cumprimento de obrigação legal.

Podem guardar por mais tempo? **Sim**, os artigos determinam um **prazo mínimo de guarda**:

- refletir o plano de resposta a incidente, as melhores práticas em segurança da informação e obrigações regulatórias (BACEN, SUSEP etc).
- mediante requisição direta aos provedores, sem necessidade de ordem judicial, pela autoridade policial ou Ministério Público (§ 2º dos arts. 13 e 15 do MCI).

Período de retenção



Em Outubro de 2013, o LACNIC – órgão responsável em gerir os IP's na América Latina - anunciou o início das fases de esgotamento do IPv4, realizando alocações de endereços IPv4 de maneira restritiva. Em 19 de agosto de 2020, o LACNIC designou o último bloco disponível de endereços IPv4.

Solução definitiva: utilização do protocolo **IPv6**. Protocolo com capacidade de endereços muito superior.

Solução paliativa:

- a técnica de NAT (Network Address Translation - RFC 3022) foi usada para contornar o problema.
- A função CG-NAT (NAT44) faz tradução de endereços de rede e de portas permite que vários assinantes compartilhem um único endereço público IPv4 e amplia o uso de um espaço de endereços IPv4 limitado.

Porta Lógica | Esgotamento de estoques IPv4



STJ tem posicionamento consolidado:

*“De fato, apenas com as duas pontas da informação – conexão e aplicação – é possível resolver a questão da identidade de usuários na internet que estejam utilizando um compartilhamento da versão 4 do IP. Portanto, é inegável que **ambas as categorias de provedores de que dispõe o Marco Civil da Internet têm a obrigação de guarda e fornecimento das informações da porta lógica de origem associada ao endereço IP** (REsp n. 2.005.051/SP, Terceira Turma, DJe de 25/8/2022).*

*“Uma vez reconhecida a **necessidade de prévia informação por parte do provedor de aplicação sobre a porta lógica** para a exigência do cumprimento da obrigação da recorrente, fica à ela suspensa a aplicação das astreintes até o fornecimento da referida informação” (STJ, DJ 1º mar. 2024, REsp 2.111.290/SP, Rel. Min. Marco Aurélio Bellizze)*

Porta Lógica
| Impasse
Jurídico



- **Ambientes com Proxies e Load Balancers.**

Ajustar as configurações para que a porta de origem seja propagada corretamente (ex: via headers) em toda a cadeia de servidores.

- **Uso de Serviços Intermediários (Ex: Cloudflare, AWS, Google).**

Avaliar o custo-benefício de planos que ofereçam acesso aos logs completos. Buscar alternativas ou negociar com o provedor para garantir a visibilidade necessária.

- **Protocolos além do HTTP (FTP, SMTP, etc.)**

Implementar soluções de log customizadas ou utilizar softwares alternativos que suportem o registro desta informação por padrão.

Porta Lógica | Desafios Operacionais



Quando a identificação dos responsáveis por um incidente ou o rastreamento de atividades ilegais exige acesso a dados protegidos, pode ser necessário recorrer a medidas judiciais, como a quebra de sigilo.

Objetivo: possibilitar a obtenção de informações essenciais para a investigação e identificar autoria.

Fundamento legal:

- **O art. 10 do Marco Civil da Internet** prevê a proteção de dados pessoais, mas admite a quebra de sigilo em casos **devidamente fundamentados**.
- Somente autorizado a fornecer os registros por decisão judicial.

Ação judicial para quebra de sigilo



Marco Civil da Internet:

- Manter os registros (de conexão) **sob sigilo, em ambiente controlado e de segurança (Art. 10 e Art. 13/15).**
- É vedado **bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados**, salvo nas exceções técnicas ou de emergência previstas em regulamento (Art. 9º, § 3º).
- É vedado ao provedor de conexão guardar os registros de acesso a aplicações de internet (ou seja, os sites e aplicativos que o usuário acessou) (Art. 14).

Lei Geral de Proteção de Dados:

- Exige, entre outras obrigações, a adoção de medidas de segurança técnicas e administrativas para proteger os dados pessoais (Art. 46 - LGPD), a criação de um programa de governança em privacidade (Art. 50 - LGPD) e a nomeação de um Encarregado pela proteção de dados (DPO) (Art. 41 - LGPD).

Outros
deveres |
provedores
de conexão



1. O que é o Relatório de Impacto à Proteção de Dados Pessoais (RIPD)?

O RIPD é a documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados.

2. O que deve conter no Relatório de Impacto à Proteção de Dados Pessoais (RIPD)?

Deve conter, as medidas, salvaguardas e mecanismos de mitigação de risco, nos termos dos artigos 5º, inciso XVII, e 38 da LGPD.

3. Quem é o responsável pela elaboração do RIPD?

O controlador é o agente de tratamento responsável pela elaboração do RIPD, nos termos dos art. 5º, inciso XVII, e 38, da LGPD.

4. Quando elaborar o RIPD?

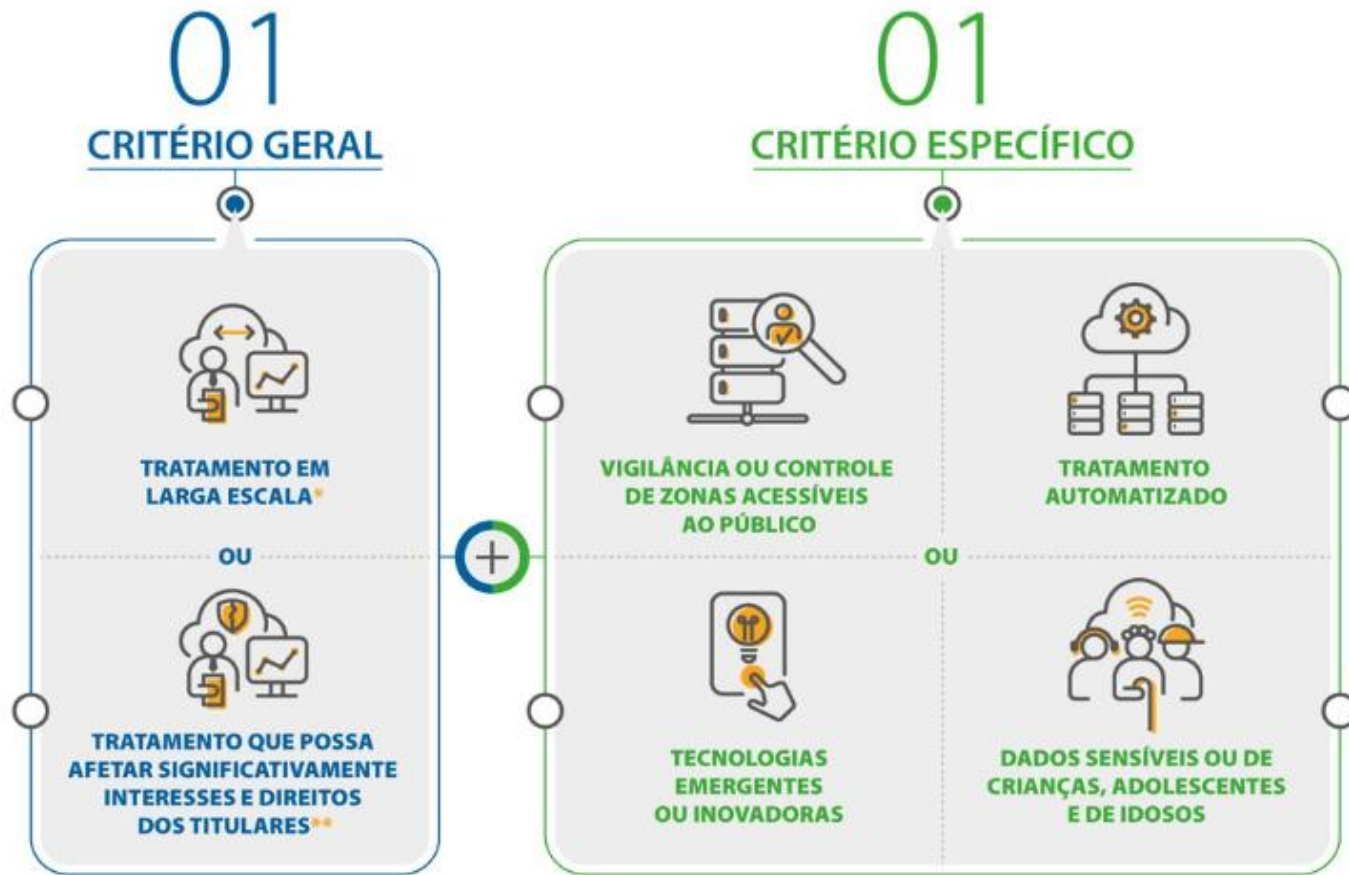
Assim que se identificar um tratamento que possa gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados.

**Relatório de
Impacto à
Proteção de
Dados Pessoais
(RIPD)**



TRATAMENTO DE ALTO RISCO

ART 4º, RES. CD/ANPD Nº2/2022



* LARGA ESCALA

Quando o tratamento abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.

** AFETAR SIGNIFICATIVAMENTE INTERESSES E DIREITOS

Quando o tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

Da Teoria à Prática: Um Panorama sobre Proteção de Dados Pessoais e Gestão de Incidentes de Segurança

Gestão de Incidentes de Segurança



- Compreender o conceito de incidente de segurança para ANPD.
- Avaliação de risco para o titular de dados pessoais
- Comunicação do incidente à ANPD e aos titulares de dados
- Registro de incidente e medidas adicionais
- Entender a importância de uma resposta rápida para mitigar consequências de incidentes.

Objetivos deste Bloco



Da Teoria à Prática: Um Panorama sobre Proteção de Dados Pessoais e Gestão de Incidentes de Segurança

Gestão de Incidentes de Segurança:
Contextualização e dados relevantes



Dados relevantes

- Brasil ocupa o primeiro lugar no ranking de ataques cibernéticos na América Latina.
- **Custo médio de um IS no Brasil:** Brasil é o país com a maior taxa de crescimento nos prejuízos ano a ano. Cerca de R\$ 7 milhões. Custos envolvem: gastos com contenção, recuperação, investigações técnicas, consultorias especializadas, comunicação dos afetados etc.
- **Ciclo de vida do incidente:** 207 dias para identificar e 70 dias para conter. Empresas com maior maturidade (isso inclui plano de respostas) tem um gasto consideravelmente menor (R\$ 3,4 milhões) e ciclo de vida reduzido.

Fonte: IBM



Dados relevantes



COORDENAÇÃO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA - TIS
COORDENAÇÃO-GERAL DE FISCALIZAÇÃO - CGF

NÚMERO DE INCIDENTES DE SEGURANÇA RECEBIDOS
2021 - 2025

Última Atualização

Atualizado em 09/09/2025 às 14h

Ano, Trimestre, Mês

Todos

UF

Todos

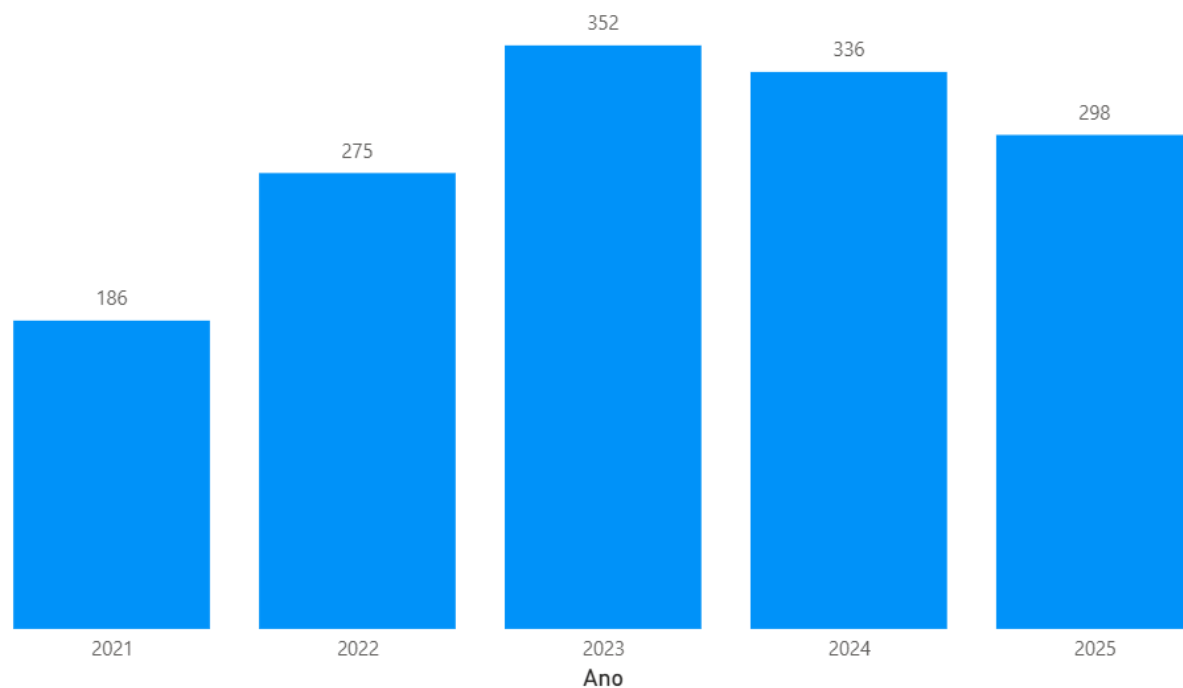
Setor

Todos

Incidentes Reportados

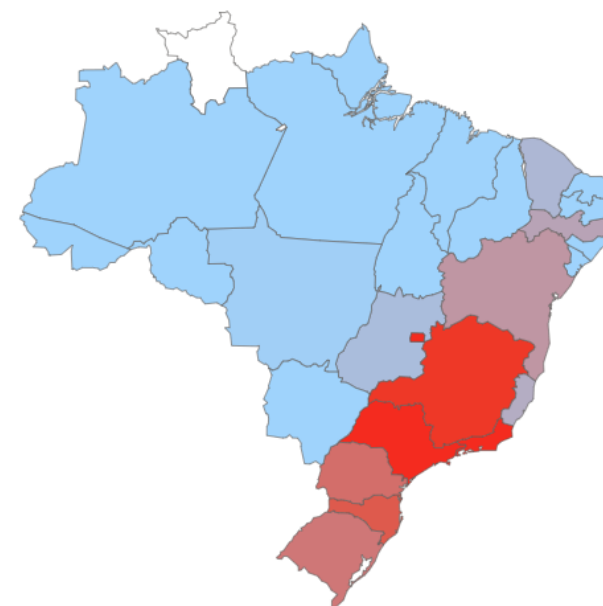
1,447 Mil

Incidentes x Ano



Incidentes por UF

2021 - 2025



Dados relevantes



COORDENAÇÃO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA - TIS
COORDENAÇÃO-GERAL DE FISCALIZAÇÃO - CGF

Última Atualização

Atualizado em 09/09/2025 às 14h

Ano

2021

2025

TIPOS DE INCIDENTES DE SEGURANÇA RECEBIDOS
2021 - 2025

Tipo de Incidente



UF	Total
Sao Paulo	491
Distrito Federal	209
Rio de Janeiro	135
Minas Gerais	94
Santa Catarina	76
Estrangeira	73
Parana	65
Rio Grande do Sul	60
Bahia	43
Pernambuco	36
Espirito Santo	31
Ceara	25
Goias	22
Mato Grosso	12
N/A	11
Alagoas	9
Mato Grosso do Sul	9
Para	8
Sergipe	7
Piaui	6
Rio Grande do Norte	6
Rondonia	5
Paraiba	4
Amazonas	3
Amapa	2
Maranhao	2
Tocantins	2
Total	1447

Da Teoria à Prática: Um Panorama sobre Proteção de Dados Pessoais e Gestão de Incidentes de Segurança

Gestão de Incidentes de Segurança:
Conceitos e leis aplicáveis



Definição

Um incidente de segurança é um evento que coloca em risco a confidencialidade, integridade e disponibilidade de um sistema de informação ou das informações (dados) que o sistema processa, armazena ou transmite, ou que constitui uma violação ou ameaça iminente de violação das políticas ou procedimentos de segurança (NIST).

Diferenças conceituais

- **Incidente cibernético:** evento adverso que compromete a segurança de um sistema ou de informações armazenadas em um sistema tecnológico.
- **Incidente de segurança com dados pessoais:** afeta informações associadas a uma pessoa (identificada ou identificável).

O que é um
incidente de
segurança da
informação?



- Envio de um e-mail para destinatário incorreto, contendo planilha com nomes e salários de colaboradores.
- Arquivos expostos em um diretório aberto na Internet, com acesso sem necessidade de identificação, contendo currículos de candidatos a uma vaga.
- Ataque DDoS que causa perda, temporária ou permanente, da disponibilidade de dados pessoais.
- Alteração não autorizada de dados cadastrais de colaboradores.
- Perda de documentos físicos, como fichas médicas de funcionários.

Exemplos de incidentes de segurança envolvendo dados pessoais



Resolução nº 15/2024 ANPD

Em 26 de abril de 2024, a ANPD publicou a **Resolução CD/ANPD nº 15/2024**, para regulamentar o processo de comunicação de incidentes de segurança, previsto no artigo 48 da Lei Geral de Proteção de Dados (LGPD).

O texto, que passou por consulta pública, estabelece várias regras como prazo para comunicação, insumos para classificação do que vem a ser risco ou dano relevante, medidas preventivas a serem adotadas pela ANPD no curso do processo, obrigação legal de registro de incidente, dentre outras.



Da Teoria à Prática: Um Panorama sobre Proteção de Dados Pessoais e Gestão de Incidentes de Segurança

Gestão de Incidentes de Segurança:
Avaliação de risco para os titulares



O que é avaliação de risco?

Processo de análise para identificar e mensurar o impacto potencial de um incidente de segurança sobre os direitos e interesses dos titulares de dados pessoais.

- **Importância:** auxilia na tomada de decisão sobre a necessidade de comunicar a ANPD e os titulares, bem como nas estratégias de mitigação do incidente.

Base legal

- Art. 48 da LGPD e detalhada na Resolução 15/2024 da ANPD (art. 4º e art. 5º).

Avaliação de risco para o titular de dados pessoais



Avaliação de risco

Nem todo incidente de segurança precisa ou deve ser comunicado à ANPD.

Art. 48 LGPD. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

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

- Tenha a ocorrência confirmada pelo agente.
- Envolver **dados pessoais**.
- Possa acarretar **risco ou dano relevante** aos titulares dos dados.



De que forma o incidente afeta dados pessoais?

- **Confidencialidade:** houve acesso não autorizado aos dados, violando seu sigilo.
- **Integridade:** houve alteração ou destruição de dados de maneira não autorizada ou acidental.
- **Disponibilidade:** houve perda ou dificuldade de acesso aos dados por período significativo.
- **Autenticidade:** houve impacto ao processo de garantia de que os dados são autênticos.

Avaliação de risco
para o titular de
dados pessoais



Exemplos de dados pessoais com alta criticidade

- **Dados sensíveis:** LGPD, art. 5º, II (racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização religiosa, filosófica ou política, saúde ou vida sexual, genético ou biométrico).
- **Cópia de documentos oficiais:** RH, CNH, Carteira de trabalho.
- **Informações financeiras:** cartão de crédito; histórico de crédito; informações de fatura; extratos bancários.
- **Dados de acesso e autenticação:** senhas (de contas pessoais); tokens de autenticação (incluindo autenticação de dois fatores); dados de login (usuário e senha).
- *E os dados do negócio da empresa, estão sujeitos à LGPD?*

Avaliação de risco para o titular de dados pessoais



Como saber se o incidente pode acarretar risco ou dano relevante?

- O contexto da atividade de tratamento de dados;
- As categorias e quantidades de titulares afetados;
- As naturezas, as categorias e a 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.

Avaliação de risco
para o titular de dados
pessoais



Art. 5º O incidente de segurança pode acarretar risco ou dano relevante aos titulares quando puder afetar significativamente interesses e direitos fundamentais dos titulares 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.

Avaliação de risco para o titular de dados pessoais

(continua)



§ 1º O incidente de segurança que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, **naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares**, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

- De acordo com o Art. 5º da Res. 15/2024 da ANPD, temos 2 etapas para avaliar o risco.

Avaliação de risco para o titular de dados pessoais



Avaliação de risco para o titular de dados pessoais

Primeira etapa

Critérios	Impacto
I - Dados pessoais sensíveis	☐ Sim ☐ Não
II - Dados de crianças, de adolescentes ou de idosos	☐ Sim ☐ Não
III - Dados financeiros	☐ Sim ☐ Não
IV - Dados de autenticação em sistemas	☐ Sim ☐ Não
V - Dados protegidos por sigilo legal, judicial ou profissional	☐ Sim ☐ Não
VI - Dados em larga escala	☐ Sim ☐ Não

Essa tabela pode ser utilizada como checklist durante a **avaliação de risco** para verificar se os critérios definidos na **Resolução 15/2024** da ANPD são aplicáveis ao incidente identificado.



Avaliação de risco para o titular de dados pessoais

Segunda etapa

Essa tabela facilita a identificação e documentação das consequências potenciais em um incidente de segurança, conforme exigido pela Resolução 15/2024 da ANPD e LGPD.



Consequência	Possibilidade
Danos morais	☐ Sim ☐ Não
Danos materiais	☐ Sim ☐ Não
Danos reputacionais	☐ Sim ☐ Não
Discriminação social	☐ Sim ☐ Não
Roubo de identidade	☐ Sim ☐ Não
Engenharia social / fraudes	☐ Sim ☐ Não
Restrições de direitos	☐ Sim ☐ Não
Violação à integridade física	☐ Sim ☐ Não
Limitação de acesso a um serviço	☐ Sim ☐ Não
Exposição de dados protegidos por sigilo profissional/legal	☐ Sim ☐ Não
Perda de acesso a dados pessoais	☐ Sim ☐ Não

Da Teoria à Prática: Um Panorama sobre Proteção de Dados Pessoais e Gestão de Incidentes de Segurança

Gestão de Incidentes de Segurança: Comunicação do incidente para ANPD



Comunicação para ANPD

Se for o operador:



Quem deve comunicar?

O próprio controlador.

Quem deve ser comunicado?

Autoridade Nacional de Proteção de Dados e Titulares impactados.

O que deve ser comunicado?

A ocorrência do incidente que pode acarretar risco ou dano relevante aos titulares.

Em qual prazo?

Em até 3 dias úteis do conhecimento de que o IS afetou dados pessoais.



Comunicação de incidente para a ANPD

Processo de notificação à Autoridade Nacional de Proteção de Dados (ANPD) sobre um incidente que afete dados pessoais e represente risco relevante aos titulares.

Demonstra transparência, conformidade com a lei e evidência compromisso com a proteção de dados pessoais.

Base legal: art. 6º da Res. n. 15/2024.

Art. 6º A comunicação de incidente de segurança à ANPD deverá ser realizada pelo controlador no prazo de três dias úteis, ressalvada a existência de prazo para comunicação previsto em legislação específica.

§ 1º O prazo a que se refere o caput será contado do conhecimento pelo controlador de que o incidente afetou dados pessoais.

Comunicação do incidente para ANPD



Conteúdo da comunicação

O conteúdo da comunicação à ANPD é regulado pelo Art. 6º da Resolução 15/2024, que estabelece os elementos mínimos que devem constar na notificação.

I - a descrição da natureza e da categoria de dados pessoais afetados;

II - o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;

III - as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;

(continua)

Comunicação do incidente para ANPD e para titulares de dados



IV - os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;

V - os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto no caput deste artigo;

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;

(continua)

Comunicação do
incidente para ANPD e
para titulares de
dados



VII - a data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo controlador;

VIII - os dados do encarregado ou de quem represente o controlador;

IX - a identificação do controlador e, se for o caso, declaração de que se trata de agente de tratamento de pequeno porte;

(continua)

Comunicação do incidente para ANPD



X - a identificação do operador, quando aplicável;

XI - a descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e

XII - o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

§ 3º As informações poderão ser complementadas, de maneira fundamentada, no prazo de 20 (vinte) dias úteis, a contar da data da comunicação.

Comunicação do incidente para ANPD



Forma da comunicação

A comunicação de incidente de segurança deverá ocorrer por meio de formulário eletrônico disponibilizado pela própria ANPD.

Atenção às formalidades:

- Formulário próprio;
- Sistema exclusivo – necessidade de cadastro prévio e com validação de informações;
- Anexar documentação comprobatória de Nomeação do DPO ou do Representante Legal.

Comunicação do incidente para ANPD



Formulário de Comunicação de Incidente de Segurança



Formulário de Comunicação de Incidente de Segurança com Dados Pessoais

Dados do Controlador

Razão Social / Nome:		
CNPJ/CPF:		
Endereço:		
Cidade:	Estado:	
CEP:		
Telefone:	E-mail:	
Declara ser Microempresa ou Empresa de Pequeno Porte:	☐ Sim	☐ Não
Declara ser Agente de Tratamento de Pequeno Porte ¹ :	☐ Sim	☐ Não
Informe o número aproximado de titulares cujos dados são tratados por sua organização:		

Dados do Encarregado

Possui um encarregado pela proteção de dados pessoais?	☐ Sim	☐ Não
Nome:		
CNPJ/CPF:		
Telefone:	E-mail:	

Dados do Notificante / Representante Legal

☐ O próprio encarregado pela proteção de dados.

☐ Outros (especifique):

Nome:

CNPJ/CPF:

Telefone:

E-mail:

A documentação comprobatória da legitimidade para representação do controlador junto à ANPD deve ser protocolada em conjunto com o formulário de comunicação de incidente.

- *Encarregado*: ato de designação/nomeação/procuração.
- *Representante*: contrato social e procuração, se cabível.

Tipo de Comunicação

☐ Completa

Todas as informações a respeito do incidente estão disponíveis e a comunicação aos titulares já foi realizada.

☐ Preliminar

Nem todas as informações sobre o incidente estão disponíveis, justificadamente, ou a comunicação aos titulares ainda não foi realizada.

A complementação deverá ser encaminhada no prazo de 20 dias úteis a contar da data da comunicação – Art. 6º § 3º do Regulamento de Comunicação de Incidentes.

☐ Complementar

Complementação de informações prestadas em comunicação preliminar.

A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar.

- 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.

Formulário de Comunicação de Incidente de Segurança

Avaliação do Risco do Incidente	
☐	O incidente de segurança pode acarretar risco ou dano relevante aos titulares.
☐	O incidente não acarretou risco ou dano relevante aos titulares. (Comunicação Complementar)
☐	O risco do incidente aos titulares ainda está sendo apurado. (Comunicação Preliminar)
Justifique, se cabível, a avaliação do risco do incidente:	
Da Ciência da Ocorrência do Incidente	
Por qual meio se tomou conhecimento do incidente?	
☐	Identificado pelo próprio controlador.
☐	Notificação do operador de dados.
☐	Denúncia de titulares/terceiros.
☐	Notícias ou redes sociais.
☐	Notificação da ANPD.
☐	Outros. (especifique)
Descreva, resumidamente, de que forma a ocorrência do incidente foi conhecida:	
Caso o incidente tenha sido comunicado ao controlador por um operador, informe:	
Dados do Operador	
Razão Social / Nome:	
CNPJ/CPF:	
E-mail:	
Cabe ao controlador solicitar ao operador as informações necessárias à comunicação do incidente.	

Da Tempestividade da Comunicação do Incidente	
Informe as seguintes datas, sobre o incidente:	
Quando ocorreu	
Quando tomou ciência	
Quando comunicou à ANPD	
Quando comunicou aos titulares	
Justifique, se cabível, a não realização da comunicação à ANPD e aos titulares de dados afetados no prazo de 3 (três) dias úteis conforme prevê o Art. 6º da Resolução CD/ANPD nº 15, de 24 de abril de 2024 que aprova o Regulamento de Comunicação de Incidente de Segurança.	
Se cabível, informe quando e a quais outras autoridades o incidente foi comunicado:	

Formulário de Comunicação de Incidente de Segurança

Da Comunicação do Incidente aos Titulares dos Dados

Os titulares dos dados afetados foram comunicados sobre o incidente?

- ☐ Sim. ☐ Não, por não haver risco ou dano relevante a eles.
- ☐ Não, mas o processo de comunicação está em andamento. ☐ Não, vez que o risco do incidente ainda está sendo apurado. (**comunicação preliminar**)

Se cabível, quando os titulares serão comunicados sobre o incidente?

De que forma a ocorrência do incidente foi comunicada aos titulares?

- ☐ Comunicado individual por escrito. ☐ Anúncio público no sítio eletrônico, mídias sociais ou aplicativos do controlador.
(mensagem eletrônica / carta / e-mail / etc.)
- ☐ Comunicado individual por escrito com confirmação de recebimento. ☐ Ampla divulgação do fato em meios de comunicação, por iniciativa do controlador.
(mensagem eletrônica / carta / e-mail / etc.) (especifique abaixo)
- ☐ Outros. (especifique abaixo) ☐ Não se aplica.

Descreva como ocorreu a comunicação:

Quantos titulares foram comunicados individualmente sobre o incidente?

Justifique, se cabível, o que motivou a não realização da comunicação individual aos titulares:

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

1. resumo e data de ocorrência do incidente;
2. descrição dos dados pessoais afetados;
3. riscos e consequências aos titulares de dados;
4. medidas tomadas e recomendadas para mitigar seus efeitos, se cabíveis;
5. dados de contato do controlador para obtenção de informações adicionais sobre o incidente.

O comunicado aos titulares atendeu os requisitos acima?

- ☐ Sim ☐ Não

- Se não atendidos os requisitos, o comunicado aos titulares deverá ser devidamente retificado.
- Poderá ser solicitada pela ANPD, a qualquer tempo, cópia do comunicado aos titulares para fins de fiscalização.

Formulário de Comunicação de Incidente de Segurança

Descrição do Incidente

Qual o tipo de incidente? (Informe o tipo mais específico)

- | | |
|---|---|
| ☐ Sequestro de Dados (<i>ransomware</i>) sem transferência de informações. | ☐ Sequestro de dados (<i>ransomware</i>) com transferência e/ou publicação de informações. |
| ☐ Exploração de vulnerabilidade em sistemas de informação. | ☐ Vírus de Computador / <i>Malware</i> . |
| ☐ Roubo de credenciais / Engenharia Social. | ☐ Violação de credencial por força bruta. |
| ☐ Publicação não intencional de dados pessoais. | ☐ Divulgação indevida de dados pessoais. |
| ☐ Envio de dados a destinatário incorreto. | ☐ Acesso não autorizado a sistemas de informação. |
| ☐ Negação de Serviço (<i>DoS</i>). | ☐ Alteração/exclusão não autorizada de dados. |
| ☐ Perda/roubo de documentos ou dispositivos eletrônicos. | ☐ Descarte incorreto de documentos ou dispositivos eletrônicos. |
| ☐ Falha em equipamento (<i>hardware</i>). | ☐ Falha em sistema de informação (<i>software</i>). |
| ☐ Outro tipo de incidente cibernético. (especifique abaixo) | ☐ Outro tipo de incidente não cibernético. (especifique abaixo) |

Descreva, resumidamente, como ocorreu o incidente:

Explique, resumidamente, por que o incidente ocorreu (identifique a causa raiz, se conhecida):

Que medidas foram adotadas para corrigir as causas do incidente?

Impactos do Incidente Sobre os Dados Pessoais

De que forma o incidente afetou os dados pessoais (admita mais de uma marcação):

- | | |
|--|--|
| ☐ Confidencialidade | Houve acesso não autorizado aos dados, violando seu sigilo. |
| ☐ Integridade | Houve alteração ou destruição de dados de maneira não autorizada ou acidental. |
| ☐ Disponibilidade | Houve perda ou dificuldade de acesso aos dados por período significativo. |

Se aplicável, quais os tipos de dados pessoais sensíveis foram violados? (admita mais de uma marcação)

- | | | |
|---|--|--|
| ☐ Origem racial ou étnica. | ☐ Convicção religiosa. | ☐ Opinião política. |
| ☐ Referente à saúde. | ☐ Biométrico. | ☐ Genético. |
| ☐ Referente à vida sexual. | ☐ Filiação a organização sindical, religiosa, filosófica ou política. | |

Se aplicável, descreva os tipos de dados pessoais sensíveis violados:

Quais os demais tipos de dados pessoais violados? (admita mais de uma marcação)

- | | | |
|--|--|---|
| ☐ Dados básicos de identificação
(<i>ex: nome, sobrenome, data de nascimento, matrícula</i>) | ☐ Número de documentos de identificação oficial.
(<i>ex: RG, CPF, CNH, passaporte</i>) | ☐ Dados de contato.
(<i>ex: telefone, endereço, e-mail</i>) |
| ☐ Dados de meios de pagamento.
(<i>ex: cartão de crédito/débito</i>) | ☐ Cópias de documentos de identificação oficial. | ☐ Dados protegidos por sigilo profissional/legal. |
| ☐ Dado financeiro ou econômico. | ☐ Nomes de usuário de sistemas de informação. | ☐ Dado de autenticação de sistema.
(<i>ex: senhas, PIN ou tokens</i>) |
| ☐ Imagens / Áudio / Vídeo | ☐ Dado de geolocalização.
(<i>ex: coordenadas geográficas</i>) | ☐ Outros (especifique abaixo) |

Descreva os tipos de dados pessoais não sensíveis violados:

Formulário de Comunicação de Incidente de Segurança

Riscos e Consequências aos Titulares dos Dados		
Foi elaborado um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) das atividades de tratamento afetadas pelo incidente?		
☐ Sim ☐ Não		
Qual o número total de titulares cujos dados são tratados nas atividades afetadas pelo incidente?		
Qual a quantidade aproximada de titulares afetados ¹ pelo incidente?		
Total de titulares afetados		
Crianças e/ou adolescentes		
Outros titulares vulneráveis		
Se aplicável, descreva as categorias de titulares vulneráveis afetados:		
Quais as categorias de titulares foram afetadas pelo incidente? (admite mais de uma marcação)		
☐ Funcionários.	☐ Prestadores de serviços.	☐ Estudantes/Alunos.
☐ Clientes/Cidadãos.	☐ Usuários.	☐ Inscritos/Filiados.
☐ Pacientes de serviço de saúde.	☐ Ainda não identificadas.	☐ Outros. (especifique abaixo)
Informe o quantitativo de titulares afetados, por categoria:		

Quais as prováveis consequências do incidente para os titulares? (admite mais de uma marcação)		
☐ 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.
☐ Restrições de direitos.	☐ Perda de acesso a dados pessoais.	☐ Outros (especifique abaixo).
Se cabível, descreva as prováveis consequências do incidente para cada grupo de titulares:		
Qual o provável impacto do incidente sobre os titulares? (admite só uma marcação)		
☐ Podem não sofrer danos, sofrer danos negligenciáveis ou superáveis sem dificuldade.		
☐ Podem sofrer danos, superáveis com certa dificuldade.		
☐ Podem sofrer danos importantes, superáveis com muita dificuldade.		
☐ Podem sofrer lesão ou ofensa a direitos ou interesses difusos, coletivos ou individuais, que, dadas as circunstâncias, ocasionam ou tem potencial para ocasionar dano significativo ou irreversível.		
Se cabível, quais medidas foram adotadas para mitigação dos riscos causados pelo incidente aos titulares?		



Formulário de Comunicação de Incidente de Segurança

Medidas de Segurança Técnicas e Administrativas para a Proteção dos Dados Pessoais

Os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares?

- ☐ Sim, integralmente protegidos por criptografia / pseudonimização. ☐ Sim, parcialmente protegidos por criptografia / pseudonimização. ☐ Não.

Descreva os meios utilizados para proteger a identidade dos titulares, e a quais tipos dados foram aplicados:

Antes do incidente, quais das seguintes medidas de segurança eram adotadas? (admite mais de uma marcação)

- | | | |
|--|---|---|
| ☐ Políticas de segurança da informação e privacidade. | ☐ Processo de Gestão de Riscos. | ☐ Registro de incidentes. |
| ☐ Controle de acesso físico. | ☐ Controle de acesso lógico. | ☐ Segregação de rede. |
| ☐ Criptografia/Anonimização. | ☐ Cópias de segurança. (<i>backups</i>) | ☐ Gestão de ativos. |
| ☐ Antivírus. | ☐ Firewall. | ☐ Atualização de Sistemas. |
| ☐ Registros de acesso (logs). | ☐ Monitoramento de uso de rede e sistemas. | ☐ Múltiplos fatores de autenticação. |
| ☐ Testes de invasão. | ☐ Plano de resposta a incidentes. | ☐ Outras (especifique). |

Descreva as demais medidas de segurança técnicas e administrativas adotadas antes do incidente:

Após o incidente, foi adotada alguma nova medida de segurança? (admite mais de uma marcação)

- | | | |
|--|---|---|
| ☐ Políticas de segurança da informação e privacidade. | ☒ Processo de Gestão de Riscos. | ☐ Registro de incidentes. |
| ☐ Controle de acesso físico. | ☐ Controle de acesso lógico. | ☐ Segregação de rede. |
| ☐ Criptografia/Anonimização. | ☐ Cópias de segurança. (<i>backups</i>) | ☐ Gestão de ativos. |
| ☐ Antivírus. | ☐ Firewall. | ☐ Atualização de Sistemas. |
| ☐ Registros de acesso (logs). | ☐ Monitoramento de uso de rede e sistemas. | ☐ Múltiplos fatores de autenticação. |
| ☐ Testes de invasão. | ☐ Plano de resposta a incidentes. | ☐ Outras (especifique). |

Se cabível, descreva as medidas de segurança adicionais adotadas após o incidente:

As atividades de tratamento de dados afetadas estão submetidas a regulações de segurança setoriais?

- ☐ Sim ☐ Não

Se cabível, indique as regulamentações setoriais de segurança aplicáveis às atividades de tratamento de dados afetadas pelo incidente:

Declaro, sob as penas da lei, serem verdadeiras as informações prestadas acima.

<ASSINATURA>

Da Teoria à Prática: Um Panorama sobre Proteção de Dados Pessoais e Gestão de Incidentes de Segurança

Gestão de Incidentes de Segurança:
Comunicação do incidente para titulares de dados



Em que situações comunicar os titulares?

- **Critérios (mesmo critério para ANPD):**

O incidente deve ter **ocorrência confirmada**.

Envolver dados pessoais que acarretem **risco ou dano relevante** aos titulares.

- **Responsabilidade:**

Cabe ao controlador notificar diretamente os titulares afetados no prazo de 3 dias úteis.

O operador deve informar o controlador sobre o incidente sem demora.

Comunicação do incidente aos titulares de dados



- **Casos em que a comunicação pode não ser necessária:**

- Dados protegidos por criptografia ou outras medidas de segurança eficazes (dispositivo perdido, mas com dados criptografados e senha de acesso).
- Não há risco ou dano relevante (o incidente somente impactou nome e CPF, por exemplo).

Comunicação do incidente aos titulares de dados



Elementos obrigatórios (Art. 9º Res. 15/2024)

- I. a descrição da natureza e da categoria de dados pessoais afetados;
- II. as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- III. os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
- IV. os motivos da demora, no caso de a comunicação não ter sido feita no prazo do caput deste artigo;
- V. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;
- VI. a data do conhecimento do incidente de segurança; e
- VII. o contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado.

Comunicação do incidente aos titulares de dados



Forma da comunicação aos titulares

Art. 9º, §1º, Res. n. 15/2024: estabelece os critérios para a comunicação do incidente aos titulares afetados.

- **Linguagem simples:** clareza e objetividade são essenciais.
- **Forma direta:** preferencialmente, comunicação individual (e-mail, mensagem ou telefone).
- **Ampla divulgação:** caso não seja possível identificar todos os titulares, usar meios como site oficial ou redes sociais, com direta e fácil visualização, pelo período mínimo de três meses.

Comunicação do incidente aos titulares de dados



Boas práticas para comunicação dos titulares:

- Use linguagem acessível e evite termos técnicos (quando possível).
- Seja objetivo e direto, sem omitir informações relevantes.
- Ofereça suporte, como canais de atendimento ou recomendações
- **Meio preferencial:** e-mail (fácil de disparar e de guardar evidência);
- **Assunto:** Notificação de incidente de segurança;
- **Corpo:** explicação do incidente, indicando data de conhecimento, dados pessoais afetados, riscos e possíveis impactos, medidas adotadas e informações de contato.

Comunicação do incidente aos titulares de dados



O que não fazer:

“Prezada D. Maria, serve a presente para notificá-la acerca da ocorrência de um incidente cibernético que impactou dados pessoais de sua titularidade. Este incidente pode afetar de forma significativa seus interesses e direitos fundamentais, especialmente decorrente de práticas de engenharia social”.

Comunicação do incidente aos titulares de dados



Declaração de comunicação de incidente

Art. 9º § 4º O controlador deverá juntar ao processo de comunicação de incidente uma declaração de que foi realizada a comunicação aos titulares, constando os meios de comunicação ou divulgação utilizados, em até três dias úteis, contados do término do prazo de que trata o caput deste artigo.

Recomendações:

- Data da comunicação; Meio de comunicação (anexar exemplo); Total de titulares comunicados;
- Documento assinado pelo Encarregado.

Comunicação do incidente aos titulares de dados



Consequências da falha ou da ausência de comunicação

- Multas e penalidades administrativas, conforme legislação.
- Danos reputacionais à companhia.
- Ações judiciais por titulares afetados – o dano deve ser comprovado.

Comunicação do incidente aos titulares de dados



Benefícios de uma comunicação eficiente

- **Transparência:** reforça a credibilidade da organização.
- **Mitigação de riscos:** reduz impactos legais e reputacionais.
- **Confiança:** ajuda a manter a relação com clientes e parceiros.

Comunicação do incidente aos titulares de dados



Da Teoria à Prática: Um Panorama sobre Proteção de Dados Pessoais e Gestão de Incidentes de Segurança

Gestão de Incidentes de Segurança: Registro do incidente de segurança



O que é o Registro do Incidente de Segurança?

Documento obrigatório (regulado) que reúne as informações detalhadas e relevantes sobre um incidente de segurança, mesmo quando ele não for comunicado à ANPD ou aos titulares.

Base Legal: Art. 10 da Resolução n. 15/2024 exige que o controlador mantenha esses registros por, no mínimo, 5 anos, salvo obrigações adicionais que demandem maior prazo.

Registro do incidente



Registro do incidente

Importância

- **Conformidade Legal:** evita penalidades administrativas em auditorias da ANPD.
- **Transparência interna:** documenta o incidente para consultas futuras e aprendizado organizacional.
- **Base Estratégica:** suporta ações preventivas e corretivas, como a revisão de políticas de segurança ou medidas técnicas.



Elementos obrigatórios (Art. 10, §1º)

- **Data de conhecimento do incidente:** quando a organização tomou ciência do evento.
- **Descrição geral das circunstâncias:** detalhes das condições que permitiram o incidente, como erros humanos ou falhas técnicas.
- **Natureza e categoria de dados afetados:** identificar se os dados são sensíveis, financeiros, crianças, idosos, entre outros.
- **Número de titulares impactados:** total aproximado de pessoas afetadas.

(continua)

Registro do incidente



Registro do incidente

Elementos obrigatórios (Art. 10, §1º)

- **Avaliação do risco e danos:** riscos potenciais, como vazamento de dados sensíveis, fraude financeira ou impacto reputacional.
- **Medidas de correção e mitigação:** ações implementadas, como reforço na segurança ou notificação de parceiros.
- **Forma e conteúdo da comunicação:** se o incidente foi comunicado à ANPD e aos titulares, incluir detalhes do comunicado.
- **Motivo da ausência de comunicação:** justificar por que o incidente não foi considerado relevante para notificação.



Passos sugeridos para registrar incidentes

1. **Identificação e classificação:** determinar a gravidade do incidente e a natureza dos dados afetados.
2. **Coleta de evidências:** capturar logs, registros de sistemas e documentos relevantes, preservando sua integridade.
3. **Preenchimento do Registro:** incluir todos os elementos mínimos obrigatórios, detalhando a avaliação de riscos e as medidas adotadas.
4. **Revisão interna:** garantir precisão das informações registradas e conformidade com requisitos legais.
5. **Armazenamento seguro:** manter o registro e as evidências por, no mínimo, 5 anos, ou mais, caso exigido por normas adicionais.

Registro do incidente



E se não registrar o incidente?

Descumprimento Legal:

- Não manter o registro de incidentes viola o art. 10 da Resolução 15/2024 e pode resultar em penalidades administrativas impostas pela ANPD.
- Em auditorias ou investigações, a ausência do registro pode ser interpretada como negligência na proteção de dados pessoais.

Registro do incidente

(continua)



Impactos organizacionais:

- Perda de informações valiosas sobre o incidente, dificultando a identificação de padrões e a prevenção de recorrências.
- Comprometimento da confiança de titulares e parceiros ao não demonstrar transparência e conformidade na gestão de incidentes.

Riscos Reputacionais e Legais:

- Litígios por parte de titulares afetados podem ser agravados pela falta de registros claros e detalhados.
- A incapacidade de apresentar evidências pode enfraquecer a defesa da organização em casos de disputas legais ou regulatórias.

Registro do incidente



Template para Registro do Incidente

Impacto da Resolução CD-ANPD nº 15/2024 na atuação dos CSIRTs: Registro de Incidentes e Conformidade Legal

Guilherme Ochsendorf, Tiago Neves e Vinícius Azevedo, Opice Blum

TLP:CLEAR

SLIDES

Modelo Relatório ANPD

Em 26 de abril de 2024, a ANPD publicou a Resolução CD/ANPD nº 15/2024, para regulamentar o processo de comunicação de incidentes de segurança, previsto no artigo 48 da Lei Geral de Proteção de Dados (LGPD). O texto, que passou por consulta pública, estabelece várias regras como prazo para comunicação, insumos para classificação do que vem a ser risco ou dano relevante, medidas preventivas a serem adotadas pela ANPD no curso do processo, obrigação legal de registro de incidente, dentre outras. Esta palestra destacará os principais pontos da resolução, os temas que merecem atenção, bem como os principais impactos da resolução na atuação de um time de CSIRT.

Disponível em: <https://forum.cert.br/forum2024/slides/forumcsirts2024-opiceblum-modelo-relatorio.pdf>



Da Teoria à Prática: Um Panorama sobre Proteção de Dados Pessoais e Gestão de Incidentes de Segurança

Gestão de Incidentes de Segurança:
Preservação de evidências e outras medidas



Processo de identificação, coleta, armazenamento e proteção de informações e registros relacionados a um incidente de segurança, garantindo sua integridade para análises forenses, auditorias e relatórios técnicos. A preservação adequada assegura que as evidências sejam confiáveis e utilizáveis em contextos legais e regulatório

Por que preservar evidências?

- **Integridade das informações:** garante a veracidade dos dados coletados para análises e relatórios.
- **Base para auditorias:** fundamenta o registro do incidente e demonstra conformidade com regulamentações.
- **Análise forense:** permite identificar a origem do incidente, método de ataque e possíveis vulnerabilidades.

Preservação das evidências



Boas Práticas:

- Registrar a cadeia de custódia, detalhando quem acessou as evidências e em que circunstâncias.
- Utilizar ferramentas confiáveis para coleta e armazenamento, como sistemas de monitoramento de logs e imagens forenses.
- Manter capturas de tela, registros de acessos e comunicações relacionadas ao incidente.
- Armazenar evidências em local seguro, com controle de acesso.

Preservação das evidências



Objetivo: gerenciar a reputação da companhia e evitar desinformação durante a crise.

Estratégias:

- Preparar notas reativas antecipadamente (evitar nota proativa).
- Usar linguagem acessível e responsável para explicar o incidente e as ações de resposta adotadas.
- Evitar informações técnicas excessivas ou especulativas (que podem ser desmentidas no decorrer das investigações).

Na prática: nota oficial sobre um vazamento de dados, destacando medidas de contenção e suporte aos titulares (continua com exemplo de estrutura no próximo slide).

Comunicação à mídia / imprensa



Comunicação à mídia / imprensa

- Vítima de ataque cibernético; não realizou pagamento porque não compactua com o crime.
- Medidas de segurança adotadas pela companhia.
- Contato direto para o titular.
- Comunicação com autoridades (ANPD, Polícia).
- Reforço do compromisso com a proteção de dados.

Comunicação à mídia / imprensa



Exemplos de notas públicas:

*"Nota Oficial – Real Hospital Português
Recife, 01 de setembro de 2024 – 15h*

O Real Hospital Português informa que sofreu um incidente de segurança cibernética, o qual foi prontamente interrompido por nossas equipes técnicas.

Desde o primeiro momento, o hospital tem tomado todas as medidas técnicas e administrativas necessárias para mitigar os efeitos desse incidente através de equipes internas e externas de especialistas.

Gostaríamos de assegurar a toda a sociedade que, apesar do ocorrido, o hospital continua a operar normalmente, mantendo nosso compromisso com a segurança e a qualidade dos atendimentos prestados.

*Diretoria Executiva
Real Hospital Português*

Fonte: <https://securityleaders.com.br/real-hospital-portugues-confirma-ocorrencia-de-incidente-cibernetico/>

"Desde o início deste incidente, o AGF tem se comprometido com a mais alta transparência e responsabilidade. Tomamos todas as medidas legais e técnicas necessárias para investigar a fundo o ocorrido. Informamos proativamente nossos clientes e autoridades competentes, incluindo a ANPD, sobre a situação. Além disso, registramos boletim de ocorrência e está em andamento uma investigação policial em para apuração do ilícito.

Apesar das investigações intensivas, até o momento, não encontramos evidências concretas que comprovem a extração de informações, exceto pelas fotos de telas fornecidas anonimamente. Entendemos a gravidade das alegações e continuamos comprometidos em proteger a integridade dos dados de nossos clientes.

É importante ressaltar que, em linha com nossos princípios éticos e compromisso com a legalidade, o AGF não efetuou e não efetuará qualquer tipo de pagamento em resposta a esta tentativa de extorsão. Não compactuamos com o crime e acreditamos firmemente na importância de seguir os caminhos legais para resolver tais questões".

Fonte: <https://www.tecmundo.com.br/seguranca/276925-agencia-investimento-agf-sofre-ataque-ransomware-vazamento-policia-investiga.htm>



- **Base Jurídica:** cláusulas contratuais de notificação em caso de incidentes que afetem operações conjuntas. É comum que essas cláusulas tenham dever de comunicação imediato ou em prazo muito curto.
- **Boas Práticas:**
 - Analisar contratos para identificar prazos e responsabilidades;
 - Ter uma matriz de comunicação nos procedimentos de resposta a incidentes.

Notificações para parceiros (contratos)



- **Objetivo:** cobrir custos relacionados ao incidente, como:
 - Perdas financeiras.
 - Contratação de consultorias técnicas e jurídicas.
 - Multas e reparações aos titulares.

- **Boas Práticas:**
 - Consultar a apólice para verificar cobertura e prazos. Indicar no Plano de Resposta a Incidentes.
 - Notificar imediatamente a seguradora após identificar o incidente para evitar negativa de cobertura.

Acionamento de seguro cibernético



Da Teoria à Prática: Um Panorama sobre Proteção de Dados Pessoais e Gestão de Incidentes de Segurança

Gestão de Incidentes de Segurança:
Medidas de segurança administrativas



O que são medidas administrativas de segurança da informação?

Medidas administrativas de segurança da informação são ações que visam proteger os dados de uma empresa, por meio da implementação de procedimentos, treinamento e definições de competências.

Importância

- **Base para medidas técnicas eficazes**
- **Conformidade** com regulamentações
- **Governança**: estruturam a proteção da informação como parte da cultura organizacional.

Medidas de segurança administrativas



Principais medidas de segurança administrativas

- **Política de Segurança da Informação:** consiste em um conjunto de diretrizes e regras que tem por objetivo possibilitar o planejamento, a implementação e o controle de ações relacionadas à segurança da informação em uma organização.
- **Plano de Resposta a Incidentes:** conjunto de procedimentos estruturados para identificar, conter, resolver e documentar incidentes de segurança, minimizando danos e acelerando a recuperação.

Medidas de segurança administrativas



Em abril de 2025 o NIST publicou o “NIST SP 800-61 Rev. 3”

Esse documento auxilia organizações a incorporar recomendações e considerações de resposta a incidentes de segurança cibernética em suas atividades de gerenciamento de riscos de segurança cibernética, conforme descrito no NIST Cybersecurity Framework (CSF) 2.0. Além disso, pode ajudar as organizações a se prepararem para respostas a incidentes, reduzir o número e o impacto dos incidentes que ocorrem e melhorar a eficiência e a eficácia de suas atividades de detecção, resposta e recuperação de incidentes.

(<https://csrc.nist.gov/pubs/sp/800/61/r3/final>)

Plano de Resposta a Incidentes | NIST



Plano de Resposta a Incidentes | NIST

Table 1. Previous incident response life cycle model's phases and corresponding CSF 2.0 Functions

Previous Incident Response Life Cycle Model Phase	CSF 2.0 Functions
Preparation	Govern
	Identify (all Categories)
	Protect
Detection & Analysis	Detect
	Identify (Improvement Category)
Containment, Eradication & Recovery	Respond
	Recover
	Identify (Improvement Category)
Post-Incident Activity	Identify (Improvement Category)

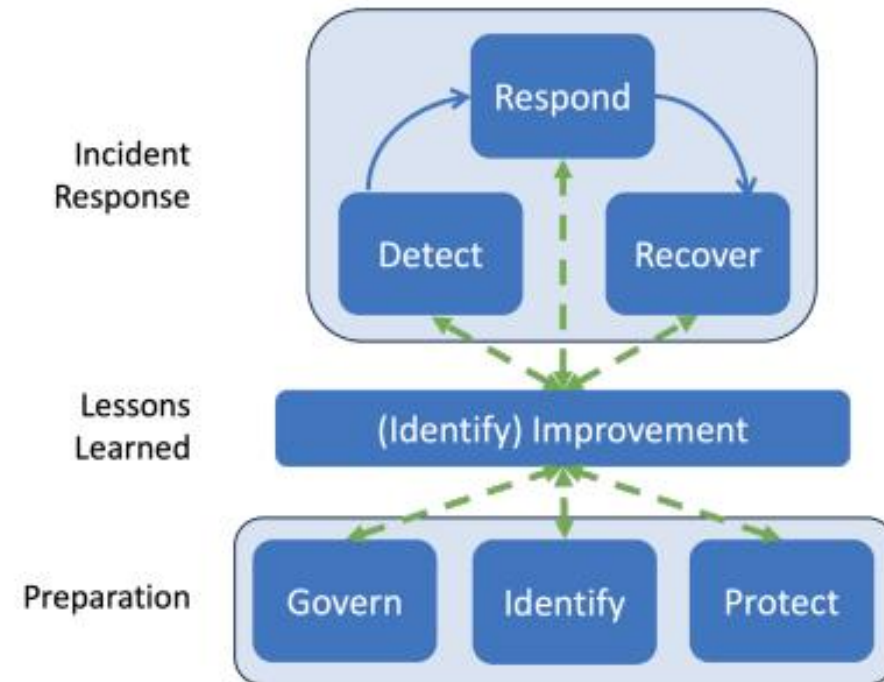


Fig. 2. Incident response life cycle model based on CSF 2.0 Functions



GUIA ORIENTATIVO

SEGURANÇA DA
INFORMAÇÃO PARA
AGENTES DE
TRATAMENTO DE
PEQUENO PORTE

VERSÃO 1.0
OUT. 2021



Guia orientativo da ANPD

- Mínimo que a ANPD espera
- Medidas administrativas (PSI)
- Medidas técnicas (Controle de acesso)



Da Teoria à Prática: Um Panorama sobre Proteção de Dados Pessoais e Gestão de Incidentes de Segurança

Gestão de Incidentes de Segurança:
Decisões da Autoridade Nacional de Proteção de
Dados (ANPD)



Por que os logs são essenciais?

- Permitem identificar **a causa e a extensão** do incidente.
- Ajudam a **delimitar o impacto real**: o que ocorreu, o que foi acessado ou exfiltrado, quais dados foram violados.
- São fundamentais para a avaliação do risco e definição da **obrigação de notificação** à ANPD e aos titulares.

A importância dos Logs na resposta a incidentes



Pior cenário

- Impõe ao controlador a necessidade de **comprovar a origem ou a falsidade das amostras** de dados publicadas.
- Exige a **delimitação do impacto real**: quais sistemas foram comprometidos, quais informações foram expostas e se os dados publicados são autênticos.
- São determinantes para a avaliação da cooperação com a autoridade e para a **definição das consequências regulatórias**.

Consequência da
ausência de logs na
investigação



Qual abordagem adotar?

- **Criação da matriz de risco** e para a tomada de decisão sobre a comunicação, seja a todos os titulares, a grupos de risco identificados, ou a documentação da não comunicação.
- Permite **identificar os tipos de dados** presentes e a extensão do comprometimento dentro do universo de arquivos não estruturados e ajuda a **delimitar o impacto**.

Casos de dados não estruturados



Medidas de segurança aos dados

O dever de comunicação aos titulares só existe quando o incidente for capaz de "acarretar risco ou dano relevante".

Adotar medidas técnicas eficazes podem eliminar ou reduzir drasticamente esse risco, afastando o dever de comunicação.

- Criptografia
- Anonimização (deixa de ser dado pessoal)
- Monitoramento
- Remoção do conteúdo

Medidas técnicas como argumentos de defesa



Olhar do regulador

Construindo a história de um incidente.

- Identificar o que aconteceu (**causa raiz**);
- **Corrigir** as falhas/vulnerabilidades;
- **Implementar** soluções/correções (contenção, erradicação e recuperação);
- Implementar medidas de **mitigação de danos**.
- **Avaliação de risco do incidente para sustentar ou não a comunicação** à ANPD e aos titulares de dados;

O que apreendemos?

- **Logs são ativos críticos** que definem o incidente.
- **Documentação detalhada** subsidiarão a análise jurídica e a tomada de decisão da companhia.
- **Integre** o jurídico com o time técnico para uma avaliação de risco precisa.
- **Utilize** frameworks de referência para políticas, tanto de resposta a incidentes como de segurança da informação (NIST, ISO).



Da Teoria à Prática: Um Panorama sobre Proteção de Dados Pessoais e Gestão de Incidentes de Segurança

Gestão de Incidentes de Segurança: Recomendações



Existe segurança infalível?

- Limitações e avanços tecnológicos
- Fator humano
- Risco residual

Sempre haverá um risco. A segurança absoluta é inalcançável; a gestão de incidentes deve focar na mitigação e resposta eficiente.



É importante que a organização siga um **Plano de Resposta a Incidente** que:

1. Entenda seu **negócio**:

- Identificação de ativos críticos
- Avaliação de riscos
- Definição de tolerância a riscos
- Alinhamento com objetivos de negócio

2. Entenda as **tecnologias utilizadas**:

- Inventário de sistemas e aplicações
- Mapeamento da infraestrutura de rede
- Análise de vulnerabilidades
- Monitoramento de segurança

3. Utilize **frameworks** de referência:

- Normas ISO/IEC 27035,
- NIST 2.0 Cybersecurity Framework, NIST SP 800-61 e SP 800-171.
- Outras normas/regulamentações (ANPD, SUSEP etc.)

4. Invista em **comunicação** e **educação**:

- Equipe de resposta a incidentes multidisciplinar
- Comunicação interna
- Comunicação externa
- Treinamento, simulações e conscientização.



cert.br nie.br egi.br

Opice
BLUM



Guilherme Ochsendorf de Freitas

guilherme.freitas@opiceblum.com.br