

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

LGPD Art. 46º

Acessos não autorizados + situações acidentais:

 Destruição


 Perda

 Alteração

 Comunicação indevida

 Tratamento inadequado ou ilícito


Segurança da informação:

 responsabilidade **solidária** do controlador e do operador

Incidente de Segurança é qualquer evento que afete a **tríade da segurança da informação**:



Consequências:

 danos reputacionais e materiais para os agentes de tratamento


Comunicação obrigatória a Titulares e ANPD (LGPD Art. 48º)

Aos titulares via:

 SMS

 E-mail

 Banners

 Notificações em sites

 Comunicações postais


 Anúncios

Quando aplicável, comunicação ao BACEN e à SENACON
(Decreto 9.936/2019, art. 18º – regulamenta a Lei do Cadastro Positivo (12.414/2011))

Eventuais sanções (LGPD art. 52º)

 Advertência

 Multa de até 2% do faturamento da empresa/grupo

 Bloqueio dos dados pessoais correspondentes à infração até a regularização

 Eliminação dos dados correspondentes

PLANO DE RESPOSTA A INCIDENTES



I. Preparação

Prevenção à incidentes

- Estruturação de uma governança de proteção de dados
- Risk assessments das operações de tratamento
- Medidas de segurança técnicas e organizacionais (e.g elaboração do plano de resposta a incidentes)
- Simulação de incidentes de segurança (*Tabletop exercises*)
- Contratação de apólice de seguro cibernético



II. Resposta

Contenção à incidentes

- Acionamento do Plano de Respostas
- Criação de um Comitê de Crise Multidisciplinar
- *Check-list*: ações imediatas de mitigação
- Avaliação de riscos aos titulares
- Eventual notificação a autoridades competentes
- Dimensionamento da extensão do dano
- Preservação de evidências
- Documentação
- Engajamento de consultoria técnica externa*
- Elaboração do relatório de investigação forense



III. Avaliação

Pós incidentes: prevenção a incidentes futuros

- Atualização do plano de respostas
- Auditoria e revisão dos contratos com fornecedores
- Reavaliação de procedimentos internos de controle
- Revisão das diretrizes de notificação
- Avaliação de sistemas e ferramentas de segurança