

VIOLAÇÃO DE DADOS

Uma violação de dados é um incidente em que as informações são roubadas ou retiradas de um sistema sem o conhecimento ou a autorização do proprietário.

Em 2022

US\$ 4,35 milhões

Média de custo total de uma violação de dados

45% das violações

eram baseadas na nuvem

Levou-se, em média, **277 dias** (cerca de 9 meses) para identificar e conter uma violação

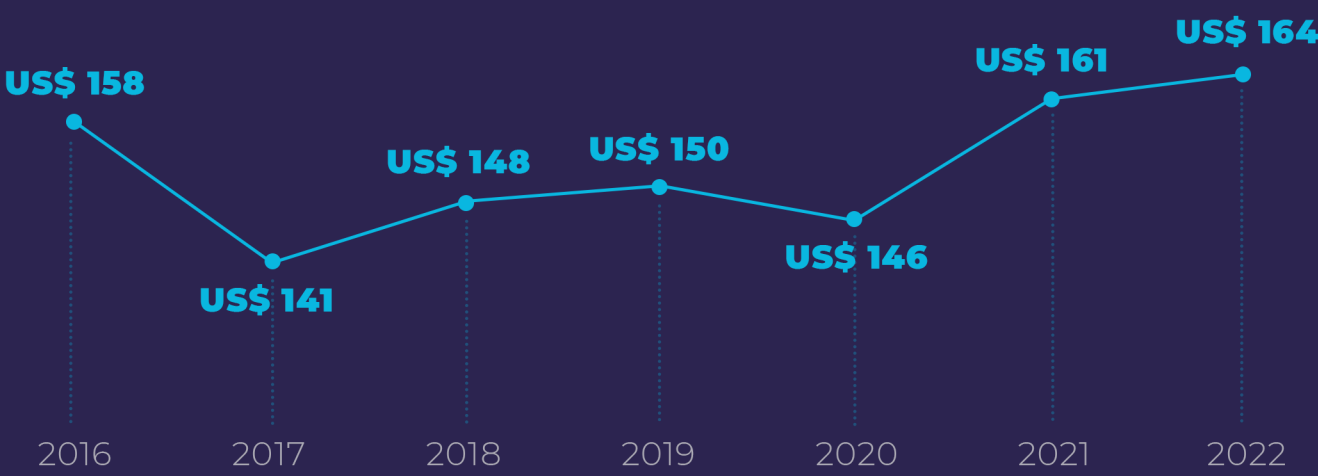
83%

Percentual de empresas que tiveram mais de uma violação



Custo médio por registro de uma violação de dados

(US\$)



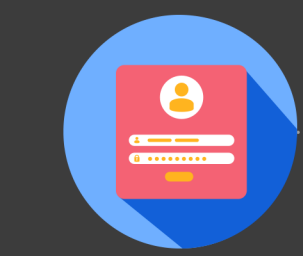
Tempo médio para identificar e conter uma violação de dados

Ano	Tempo médio para identificar (Dias)	Tempo médio para conter (Dias)	Total (Dias)
2022	207	70	277
2021	212	75	287
2020	207	73	280
2019	206	73	279
2018	197	69	266
2017	191	66	257
2016	201	70	271

■ Tempo médio para identificar ■ Tempo médio para conter

(Dias)

Principais vetores de ataque inicial



credenciais comprometidas
19%



phishing
16%



configuração incorreta da nuvem
15%



vulnerabilidade em software de terceiros
13%

O tempo médio para identificar e conter uma violação de dados por vetor de ataque inicial

Vetor de ataque	Tempo médio para identificar (Dias)	Tempo médio para conter (Dias)	Total (Dias)
Credenciais roubadas ou comprometidas	243	84	327
Comprometimento de e-mail corporativo	234	74	308
Phishing	219	76	295
Vulnerabilidade em software de terceiros	214	70	284
Usuário interno mal-intencionado	216	68	284
Comprometimento de segurança física	217	63	280
Engenharia social	201	69	270
Perda acidental de dados ou perda de dispositivo	189	69	258
Problema na configuração da nuvem	183	61	244
Outros problemas de configuração técnica	149	67	216

■ Tempo médio para identificar ■ Tempo médio para conter

(Dias)

Reduzir o tempo necessário para identificar e conter uma violação de dados para 200 dias ou menos pode economizar dinheiro.

MELHORES PRÁTICAS



- Aplicar regularmente os patches
- Ter uma equipe qualificada em segurança da informação
- Implementar medidas de segurança
- Estabelecer auditorias periódicas de segurança
- Criar plano de contingência
- Definir uma Política de Segurança e fazer com que seja cumprida
- Educar os funcionários

- Atenção aos golpes usando engenharia social
- Não publicar detalhes pessoais nem sobre clientes nas redes sociais
- Manter atualizado o software de segurança em todos os dispositivos
- Usar senhas diferentes para cada conta de e-mail e trocá-las frequentemente
- Não abrir e-mails de remetentes desconhecidos

