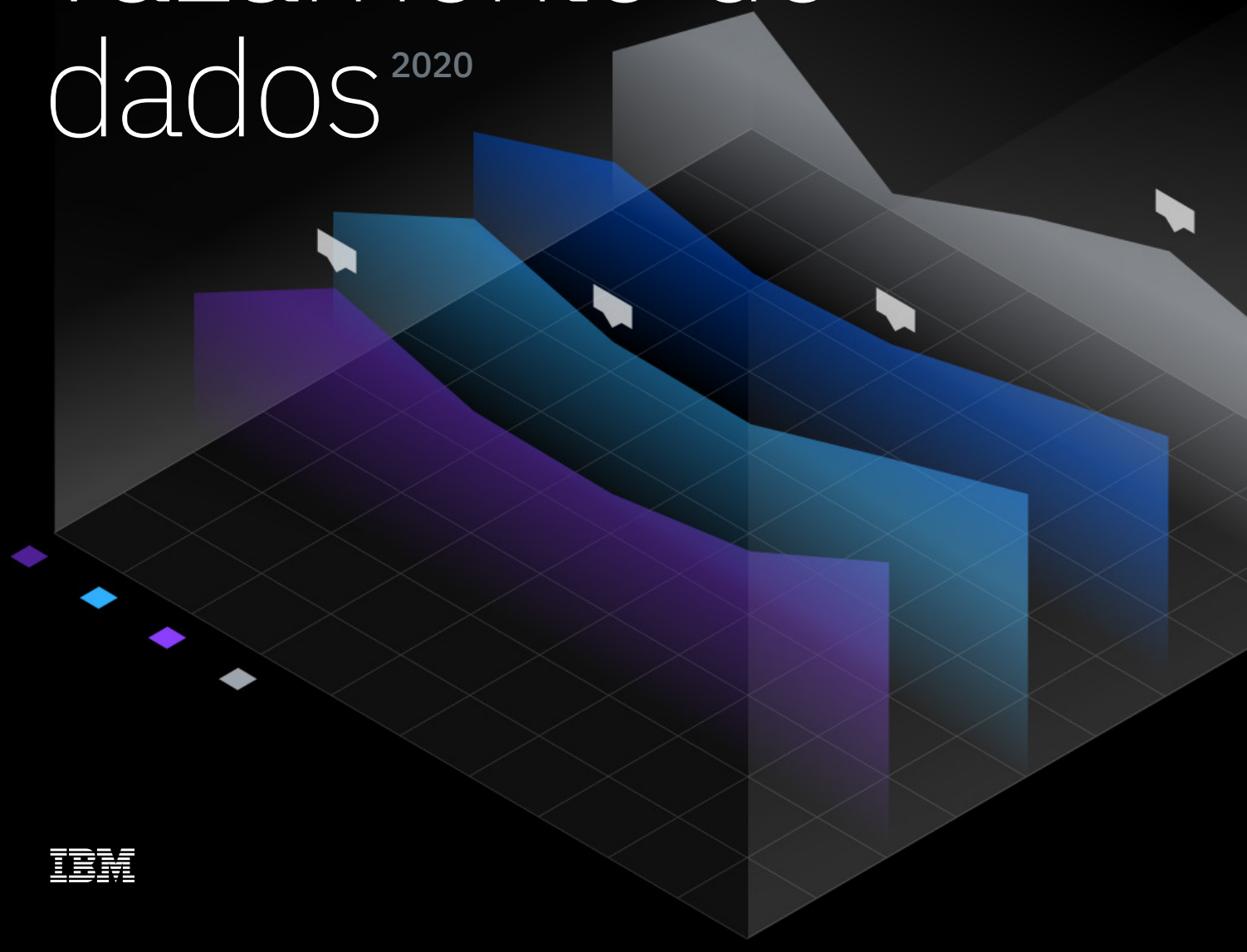
IBM Security

Relatório sobre o prejuízo de um vazamento de dados 2020



IBM

Sumário

Resumo executivo

Este é o 15º ano em que o Ponemon Institute conduziu a pesquisa para produzir o relatório anual *"Prejuízo de um vazamento de dados"*, incluindo os últimos cinco anos. Ele foi patrocinado e publicado pela IBM Security. Nossa esperança é que as empresas possam usar esta pesquisa para promover a inovação, mantendo a confiança do cliente em um momento em que os vazamentos de dados e os incidentes de segurança virtual colocam em risco organizações de todos os tipos e tamanhos.

Este relatório se tornou uma das principais ferramentas de estudo comparativo no setor de segurança virtual, oferecendo aos líderes de TI, gerenciamento de riscos e segurança uma visão pontual dos fatores que reduzem ou aumentam o prejuízo de um vazamento de dados. Ele também oferece uma visão das tendências de vazamentos de dados, demonstrando consistências e flutuações nos prejuízos que analisamos ao longo do tempo.

Para o relatório *Prejuízo de um vazamento de dados de 2020**, o Ponemon Institute recrutou 524 organizações que sofreram com vazamentos de dados entre agosto de 2019 e abril de 2020. Para garantir que a pesquisa seja relevante para um grande número de empresas, as organizações do estudo são compostas por vários tamanhos, abrangendo 17 países e regiões, além de 17 setores. Nossos pesquisadores entrevistaram mais de 3.200 pessoas que conhecem bem os incidentes de vazamento de dados nas organizações onde trabalham.

Números do relatório sobre o prejuízo de um vazamento de dados

524
Organizações afetadas

3.200
Pessoas entrevistadas

17
Países e regiões

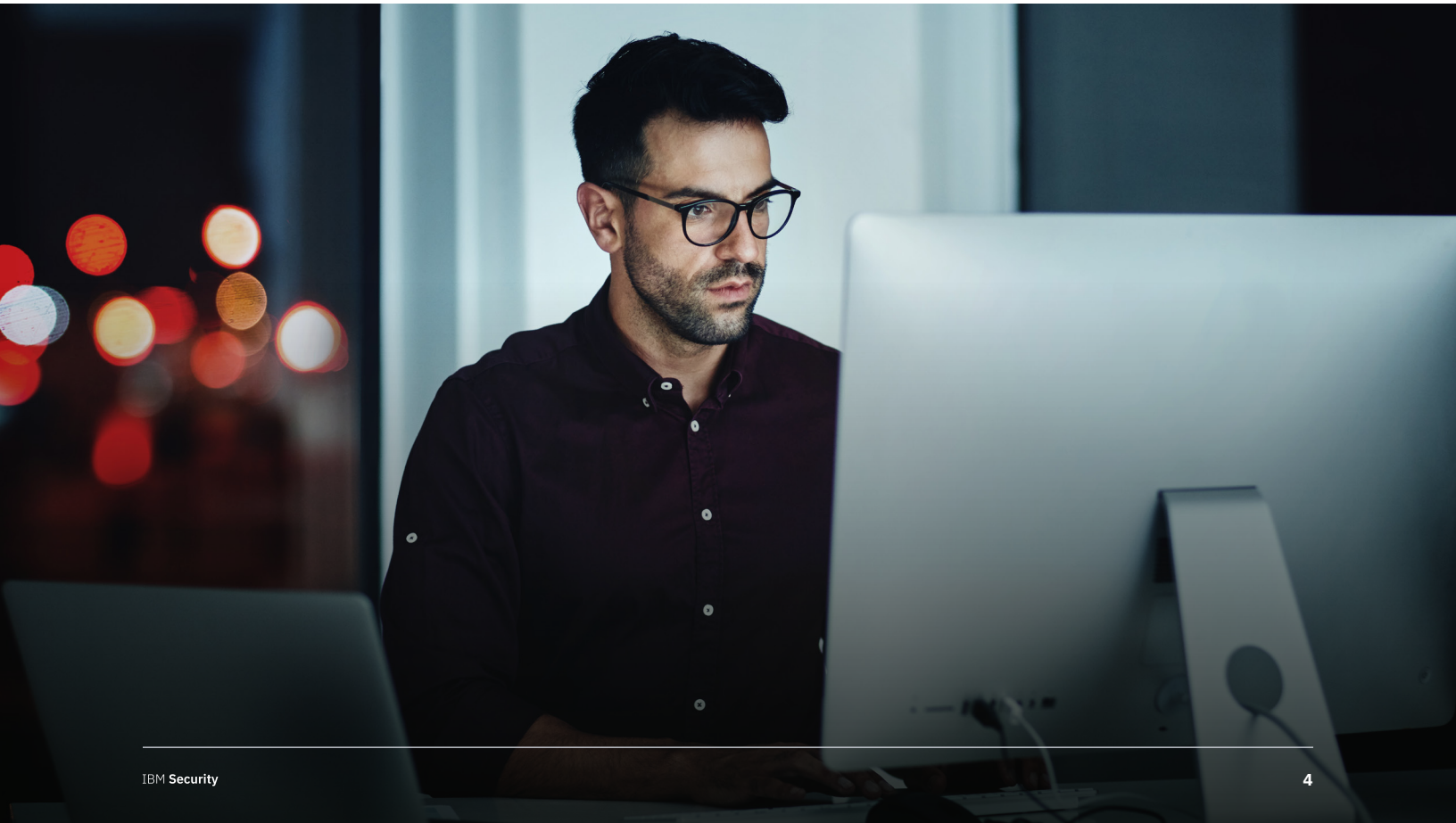
17
Setores

*Os anos neste relatório referem-se ao ano da publicação, não necessariamente ao ano em que os vazamentos ocorreram. Os vazamento de dados analisados no relatório de 2020 ocorreram entre agosto de 2019 e abril de 2020.

No decorrer das entrevistas, fizemos dezenas de perguntas para determinar quanto as organizações gastaram com atividades de detecção e a resposta imediata a um vazamento de dados. Outros problemas abordados que podem ter influenciado esse prejuízo foram as causas principais do vazamento de dados, o tempo que as organizações levaram para detectar e conter o incidente e o custo estimado da paralisação dos negócios e da perda de clientes como resultado do vazamento. Examinamos muitos outros fatores de custo, como as medidas de segurança implementadas antes do vazamento e as características da organização e do ambiente de TI dela.

O resultado é um relatório com um vasto conjunto de dados, ampla análise e informações sobre tendências. Nas páginas seguintes deste resumo executivo, você encontrará uma breve explicação de como o prejuízo de um vazamento de dados é calculado e as principais conclusões desta pesquisa. Para uma análise mais aprofundada dos dados, a seção conclusões completas oferece 49 gráficos analíticos e demográficos.

Para líderes de TI, estrategistas de segurança virtual e executivos de gerenciamento de riscos, oferecemos recomendações de medidas de segurança que podem reduzir os possíveis danos financeiros e à marca causados por um vazamento de dados, com base no que a pesquisa observou como sendo mais eficaz para as organizações participantes do estudo. Encerramos o relatório com uma explicação detalhada sobre a nossa metodologia de pesquisa.



Novidades no relatório de 2020

Nosso objetivo é renovar o relatório a cada ano para oferecer análises baseadas em relatórios anteriores e abrir novos caminhos para acompanhar as mudanças nas tecnologias e tendências, a fim de formar uma imagem mais completa dos riscos e padrões para a proteção de dados.

E 2020 acabou sendo um ano muito importante. Além das mudanças cíclicas de tecnologia e ameaças, uma pandemia global mudou a realidade de empresas e consumidores em todo o mundo.

Embora esta pesquisa tenha começado meses antes de a pandemia de COVID-19 se espalhar e após a ocorrência da maioria dos incidentes de vazamento estudados, pedimos aos participantes que respondessem a perguntas complementares da pesquisa sobre o possível impacto do trabalho remoto decorrente da pandemia. Descobrimos que a maioria das organizações (76%) previu que o trabalho remoto tornaria a resposta a um possível vazamento de dados uma tarefa muito mais difícil.

Novas pesquisas introduzidas com o relatório deste ano fornecem uma análise mais profunda dos tipos de dados que exploramos há muito tempo, como o prejuízo de um vazamento de dados por registro e as principais causas dos vazamento de dados. Neste estudo, pela primeira vez, segmentamos o prejuízo por registro comprometido para determiná-lo com base no tipo de registro vazado, como PII (informações de identificação pessoal) do cliente, PII do funcionário e PI (propriedade intelectual). Na análise das principais causas do vazamento de dados, adicionamos uma camada de profundidade para analisar tipos mais específicos de vazamentos mal-intencionados, desde credenciais roubadas até ameaças internas.

Pela primeira vez, pedimos aos participantes que identificassem o tipo de invasor supostamente responsável pelo vazamento, como invasores de estado-nação e motivados financeiramente, com a nossa análise de prejuízo demonstrando que o tipo mais comum de vazamento mal-intencionado, aquele provocado por criminosos virtuais com motivações financeiras, não era o que causava o maior prejuízo.

E, à medida que os ataques de malware destrutivo e ransomware se tornaram mais comuns, adicionamos novas análises de prejuízo ao relatório deste ano, que observou que esses ataques perniciosos causaram um prejuízo médio maior em um vazamento de dados do que o prejuízo médio geral em um vazamento de dados.

Estatísticas do vazamento de dados

US$ 3,86 milhões

Prejuízo total médio

Estados Unidos

País com maior prejuízo

Saúde

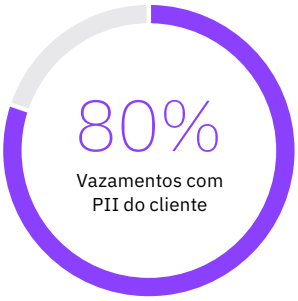
Setor com maior prejuízo

280 dias

Tempo médio para identificar e conter

Vários novos fatores de prejuízo foram adicionados à pesquisa deste ano, como o impacto da vulnerabilidade e os testes de equipe vermelhos, que usam uma abordagem diferente da aplicada nos testes de penetração, bem como a influência do trabalho remoto e da escassez de especialistas em segurança. Talvez sem surpresa, a escassez de especialistas ficou entre os três principais fatores que aumentaram o prejuízo médio de um vazamento de dados, em uma lista de 25, enquanto os testes de equipe vermelhos estrearam entre cinco principais fatores de prejuízo que reduzem o prejuízo médio de um vazamento.

Entre outras novas questões examinadas estavam o aprofundamento do papel desempenhado pelo CISO (Diretor de Informações) e os tipos de gastos cobertos por seguros de segurança virtual.



Vale ressaltar que o prejuízo total médio de um vazamento de dados diminuiu levemente no relatório deste ano, de US$ 3,92 milhões no ano passado para US$ 3,86 milhões este ano, o que pode levar algumas pessoas a acreditar que ele chegou a um pico.

Pelo contrário, nosso estudo parece comprovar uma crescente divisão no prejuízo de um vazamento de dados entre organizações com processos de segurança mais avançados, como equipes de automação e resposta a incidentes formais, e aquelas com posturas de segurança menos avançadas nessas áreas.

Por se tratar de um relatório global, a vastidão da pesquisa coletada significa que não podemos destacar todas as nuances no prejuízo de um vazamento de dados para todos os países e setores deste estudo. Por isso, desenvolvemos uma calculadora on-line e uma ferramenta de exploração de dados em ibm.com/databreach para você personalizar e tirar suas próprias conclusões.

Esperamos que você encontre informações significativas para a sua organização e tire conclusões que possam ajudá-lo a proteger melhor os dados que são fundamentais para o sucesso da sua empresa.

Como calculamos o prejuízo de um vazamento de dados

Para calcular o prejuízo médio de um vazamento de dados, esta pesquisa exclui vazamentos muito pequenos e muito grandes. Os vazamentos de dados examinados no estudo de 2020 variaram entre 3.400 e 99.730 registros comprometidos. Usamos outra análise para examinar o prejuízo de "megavazamentos", que veremos em mais detalhes na seção de conclusões completas do relatório.

Uma explicação mais aprofundada sobre os métodos usados neste relatório está disponível na seção sobre metodologia de pesquisa.

Esta pesquisa usa um método contábil chamado custeio baseado em atividades, que identifica atividades e atribui um custo de acordo com o uso real. Quatro atividades relacionadas ao processo geram uma série de despesas associadas ao vazamento de dados de uma organização: detecção e encaminhamento, notificação, resposta após o vazamento de dados e perda de negócios.

Os quatro centros de custo estão descritos abaixo.

Detecção e encaminhamento

Atividades que permitem que uma empresa detecte razoavelmente o vazamento.

- Atividades forenses e de investigação
- Serviços de avaliação e auditoria
- Gerenciamento de crise
- Comunicações a executivos e conselhos

Perda de negócios

Atividades que tentam minimizar a perda de clientes, a paralisação dos negócios e a perda de receita.

- Interrupção nos negócios e perdas de receita devido à paralisação do sistema
- Custo da perda de clientes e da aquisição de novos clientes
- Perdas de reputação e redução da clientela

Notificação

Atividades que permitem à empresa notificar titulares de dados, reguladores de proteção de dados e outros terceiros.

- E-mails, cartas, chamadas realizadas ou avisos gerais para os titulares dos dados
- Determinação de requisitos regulatórios
- Comunicação com reguladores
- Contratação de especialistas externos

Resposta pós-incidente

Atividades para ajudar as vítimas de um vazamento a se comunicar com a empresa e atividades de reparação para vítimas e reguladores.

- Suporte técnico e comunicações de entrada
- Serviços de monitoramento de crédito e proteção de identidade
- Abertura de novas contas ou emissões de novos cartões de crédito
- Despesas legais
- Descontos em produtos
- Multas regulatórias

Principais conclusões

As principais conclusões descritas aqui são baseadas na análise feita pela IBM Security dos dados da pesquisa compilados pelo Ponemon Institute.

-1,5%

Variação líquida do prejuízo total médio, 2019-2020

O prejuízo total médio de um vazamento de dados diminuiu ligeiramente em relação ao ano anterior, mas o prejuízo aumentou para muitas organizações.

Apesar de uma queda nominal de US$ 3,92 milhões, no estudo de 2019, para US$ 3,86 milhões, no estudo de 2020, o prejuízo foi muito mais baixo para algumas das empresas e setores mais maduros e muito mais alto para organizações que ficaram para trás em áreas como automação da segurança e processos de resposta a incidentes. Da mesma forma, uma análise mais profunda do prejuízo médio de um único registro perdido ou roubado (prejuízo por registro) mostrou grande variação, dependendo dos tipos de dados perdidos ou roubados em um vazamento.

US$ 150

Prejuízo médio por PII do cliente por registro

As informações de identificação pessoal (PII) dos clientes foram o tipo de registro mais frequentemente comprometido e o que mais causou prejuízo nos vazamentos de dados estudados.

Oitenta por cento das organizações afetadas declararam que as PII do cliente foram comprometidas durante o vazamento, muito mais do que qualquer outro tipo de registro. Enquanto o prejuízo médio por registro perdido ou roubado foi de US$ 146 em todos os vazamentos de dados, os que contêm informações de identificação pessoal do cliente custam às empresas US$ 150 por registro comprometido.

O prejuízo por registro de informações pessoais do cliente aumentou para US$ 175 em vazamentos causados por um ataque mal-intencionado. Dados anônimos do cliente estavam envolvidos em 24% dos vazamentos no estudo, a um prejuízo médio de US$ 143 por registro, que aumentou para US$ 171 por registro em vazamentos causados por ataques mal-intencionados.

+US$ 137.000

Trabalho remoto impacto no prejuízo total médio

O trabalho remoto durante a pandemia de COVID-19 foi apontado como possível fator de aumento do prejuízo de um vazamento de dados e dos tempos de resposta a incidentes.

Das organizações que exigiram trabalho remoto em decorrência da COVID-19, 70% disseram que isso aumentaria o prejuízo de um vazamento de dados e 76% disseram que aumentaria o tempo para identificar e conter um possível vazamento de dados. Ter uma força de trabalho remota aumentou o prejuízo total médio de um vazamento de dados de US$ 3,86 milhões em quase US$ 137.000, para um prejuízo total médio ajustado de US$ 4 milhões.

Credenciais roubadas ou comprometidas causaram o maior prejuízo nos vazamentos de dados mal-intencionados.

Uma em cada cinco empresas (19%) que sofreram com vazamentos de dados mal-intencionados foi invadida devido a credenciais roubadas ou comprometidas, aumentando o prejuízo total médio de um vazamento para essas empresas em quase US$ 1 milhão, para US$ 4,77 milhões. No geral, ataques mal-intencionados foram registrados como a causa principal mais frequente (52% dos vazamentos no estudo) em comparação com erro humano (23%) ou falhas no sistema (25%), a um prejuízo total médio de US$ 4,27 milhões.

+14%

Configuração incorreta da nuvem impacto no prejuízo total médio

Nuvens mal configuradas foram a principal causa dos vazamentos.

Além das credenciais roubadas ou comprometidas, os servidores em nuvem mal-configurados foram relacionados como o vetor de ameaças inicial mais frequente nos vazamentos causados por ataques mal-intencionados, em 19%. Como decorrência dos vazamentos causados por configurações incorretas da nuvem, o prejuízo médio de um vazamento aumentou em mais de meio milhão de dólares, para US$ 4,41 milhões.

US$ 1,52 milhão

Perda de negócios Prejuízo total médio

A perda de negócios seguiu contribuindo como o maior fator de prejuízo.

O prejuízo causado pela perda de negócios representou quase 40% do prejuízo total médio de um vazamento de dados, passando de US$ 1,42 milhão, no estudo de 2019, para US$ 1,52 milhão, no estudo de 2020. Essa conta englobou o aumento da rotatividade dos clientes, a perda de receita devido à paralisação do sistema e o aumento do custo de aquisição de novos negócios devido à reputação manchada.

US $ 3,58 milhões

Economia média de custos de automação de segurança totalmente implantada vs. sem automação de segurança

O impacto da automação da segurança no prejuízo de um vazamento de dados aumentou nos últimos três anos.

A parcela de empresas com automação da segurança totalmente implantada, definida como o uso de plataformas de inteligência artificial e a orquestração automatizada de vazamentos, cresceu de apenas 15%, em 2018, para 21%, no estudo de 2020.

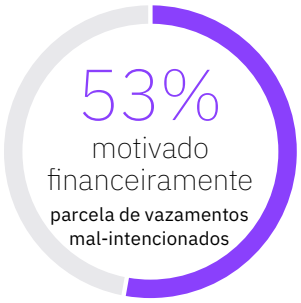
Enquanto isso, a eficácia da automação da segurança na redução do prejuízo médio de um vazamento de dados continuou a crescer. As empresas que não implantaram a automação da segurança tiveram um prejuízo total médio de US$ 6,03 milhões, mais do que o dobro do prejuízo médio de um vazamento de dados de US$ 2,45 milhões para as empresas que implantaram totalmente a automação da segurança. A economia de US$ 3,58 milhões no prejuízo médio de um vazamento, para as empresas que implantaram totalmente a automação da segurança em relação àquelas que não a implantaram, cresceu: no estudo de 2018, ela era de US$ 1,55 milhão.

100x

Multiplicador do prejuízo para > 50 milhões de registros vs. vazamento médio

O prejuízo de um megavazamento cresceu aos milhões.

As empresas que sofreram com vazamentos de mais de 1 milhão de registros continuaram vendo um prejuízo, muitas vezes, superior à média geral, em uma amostra de vazamentos de dados muito grandes. Vazamentos de 1 milhão a 10 milhões de registros custam, em média, US$ 50 milhões, mais de 25 vezes o custo médio de US$ 3,86 milhões para vazamentos de menos de 100 mil registros. Em vazamentos de mais de 50 milhões de registros, o prejuízo médio foi de US$ 392 milhões, mais de 100 vezes a média.



Vazamentos causados por invasores de estado-nação resultaram no maior prejuízo.

Embora a maioria dos vazamentos mal-intencionados tenha sido causada por ataques virtuais motivados financeiramente, os provocados por invasores de estado-nação resultaram no maior prejuízo. Cinquenta e três por cento dos vazamentos mal-intencionados no estudo de 2020 foram provocados por criminosos virtuais motivados financeiramente, em comparação com 13% por invasores de estado-nação, 13% por hacktivistas e 21% desconhecidos. No entanto, os vazamentos supostamente patrocinados por estados custam em média US$ 4,43 milhões, em comparação com US$ 4,23 milhões em vazamentos motivados financeiramente.

+US$ 292.000

Impacto da complexidade do sistema de segurança no prejuízo total médio

A complexidade da segurança e a migração para a nuvem deram mais prejuízo às empresas.

A complexidade do sistema de segurança foi o mais caro dos 25 fatores de prejuízo, aumentando o prejuízo total médio de um vazamento em US$ 292.000, para um prejuízo total médio ajustado de US$ 4,15 milhões. Passar por uma ampla migração para a nuvem no momento do vazamento aumentou o prejuízo médio de um vazamento em mais de US$ 267.000, para um prejuízo médio ajustado de US$ 4,13 milhões.

+96 dias

Setor de saúde vs. financeiro ciclo de vida do vazamento

O tempo médio para identificar e conter um vazamento variou amplamente, dependendo do setor, da localização e da maturidade da segurança.

Em média, as empresas no estudo de 2020 precisaram de 207 dias para identificar e 73 dias para conter um vazamento em 2019, somando um “ciclo de vida” médio de 280 dias.

Enquanto o ciclo de vida de um vazamento chegou, em média, a 329 dias no setor de saúde, ele foi 96 dias mais curto no setor financeiro (233 dias). A implantação total da automação da segurança ajudou as empresas a reduzir o ciclo de vida de um vazamento em 74 dias em comparação com as empresas sem automação da segurança, de 308 para 234 dias.

US $ 2 milhões

Redução de custos médios com equipes de resposta a incidentes e teste de IR versus nenhuma equipe ou teste de IR

A preparação para a resposta a incidentes (RI) foi o fator que mais reduziu o prejuízo das empresas.

O prejuízo total médio de um vazamento de dados nas empresas com uma equipe de RI e que também testaram um plano de RI usando exercícios ou simulações de mesa foi de US$ 3,29 milhões, em comparação com US$ 5,29 milhões nas empresas sem equipe de RI nem testes de um plano de RI, uma diferença de US$ 2 milhões. A diferença no prejuízo entre esses grupos foi de US$ 1,23 milhão no estudo de 2019.

12 de 16

Países com aumento no prejuízo total médio desde 2019

As diferenças entre regiões e setores apresentaram algumas grandes mudanças em comparação com 2019.

Os Estados Unidos continuaram sofrendo o maior prejuízo com vazamentos de dados no mundo, com US$ 8,64 milhões, em média, seguidos pelo Oriente Médio, com US$ 6,52 milhões. O custo total médio aumentou em 12 dos 16 países ou regiões estudados em 2019 e 2020, com o maior aumento na Escandinávia, em 12,8%.

Pelo décimo ano consecutivo, o setor de saúde teve o maior prejuízo médio de um vazamento, com US$ 7,13 milhões, um aumento de 10.5% em relação ao estudo de 2019. Da mesma forma, o setor de energia registrou um aumento de 14.1% em relação a 2019, para uma média de US$ 6,39 milhões no estudo de 2020. No geral, 13 dos 17 setores tiveram quedas, em média, no prejuízo total em relação ao ano anterior, com as mais acentuadas nos setores de mídia, educação, público e de hospitalidade.

Conclusões completas

Nesta seção, fornecemos os resultados detalhados desta pesquisa. Os tópicos são apresentados na seguinte ordem:

1. Conclusões e destaques globais
2. Principais causas de um vazamento de dados
3. Fatores que influenciam no prejuízo de um vazamento de dados
4. Tendências e eficácia da automação da segurança
5. Tempo para identificar e conter um vazamento de dados
6. Prejuízo duradouro de um vazamento de dados
7. Possíveis impactos da COVID-19
8. O prejuízo de um megavazamento de dados

Conclusões e destaques globais

O relatório *"Prejuízo de um vazamento de dados"* é um relatório global, combinando resultados de 524 organizações em 17 países e regiões e 17 setores para fornecer médias globais. No entanto, em alguns casos, o relatório detalha os resultados por país/região ou setor para fins comparativos. Embora o tamanho da amostra em alguns países/regiões e setores seja bastante pequeno, as organizações do estudo foram selecionadas na tentativa de serem representativas.

Principais conclusões

US$ 7,13 milhões

O prejuízo médio de um vazamento de dados no setor de saúde, um aumento de 10% em comparação com o estudo de 2019

80%

Parte dos vazamentos que incluíram registros com informações pessoais do cliente, a um prejuízo médio de US$ 150 por registro

US$ 5,52 milhões

Prejuízo total médio de um vazamento em empresas com mais de 25.000 funcionários, comparado a US$ 2,64 milhões para organizações com menos de 500 funcionários

Figura 1

Visão geral do estudo global

País/região	Amostra de 2020	Porcentagem da amostra	Moeda	Anos de estudo
Estados Unidos	63	12%	USD	15
Índia	47	9%	INR	9
Reino Unido	44	8%	GBP	13
Alemanha	37	7%	Euro	12
França	36	7%	Euro	7
Brasil	35	7%	BRL	9
Japão	33	6%	Iene	11
Oriente Médio*	29	6%	Riyal	7
Canadá	26	5%	Dólar CA	6
Coreia do Sul	24	5%	Won (KRW)	3
ASEAN#	23	4%	Dólar de Cingapura	2
Austrália	23	4%	Dólar AU	11
Escandinávia+	23	4%	Coroa	2
Itália	21	4%	Euro	9
América Latina**	21	4%	Peso	1
Turquia	20	4%	Lira turca	3
África do Sul	19	4%	Dólar SA	5
Total	524			

O estudo deste ano examinou vazamentos em empresas usando amostras de 17 países ou regiões.

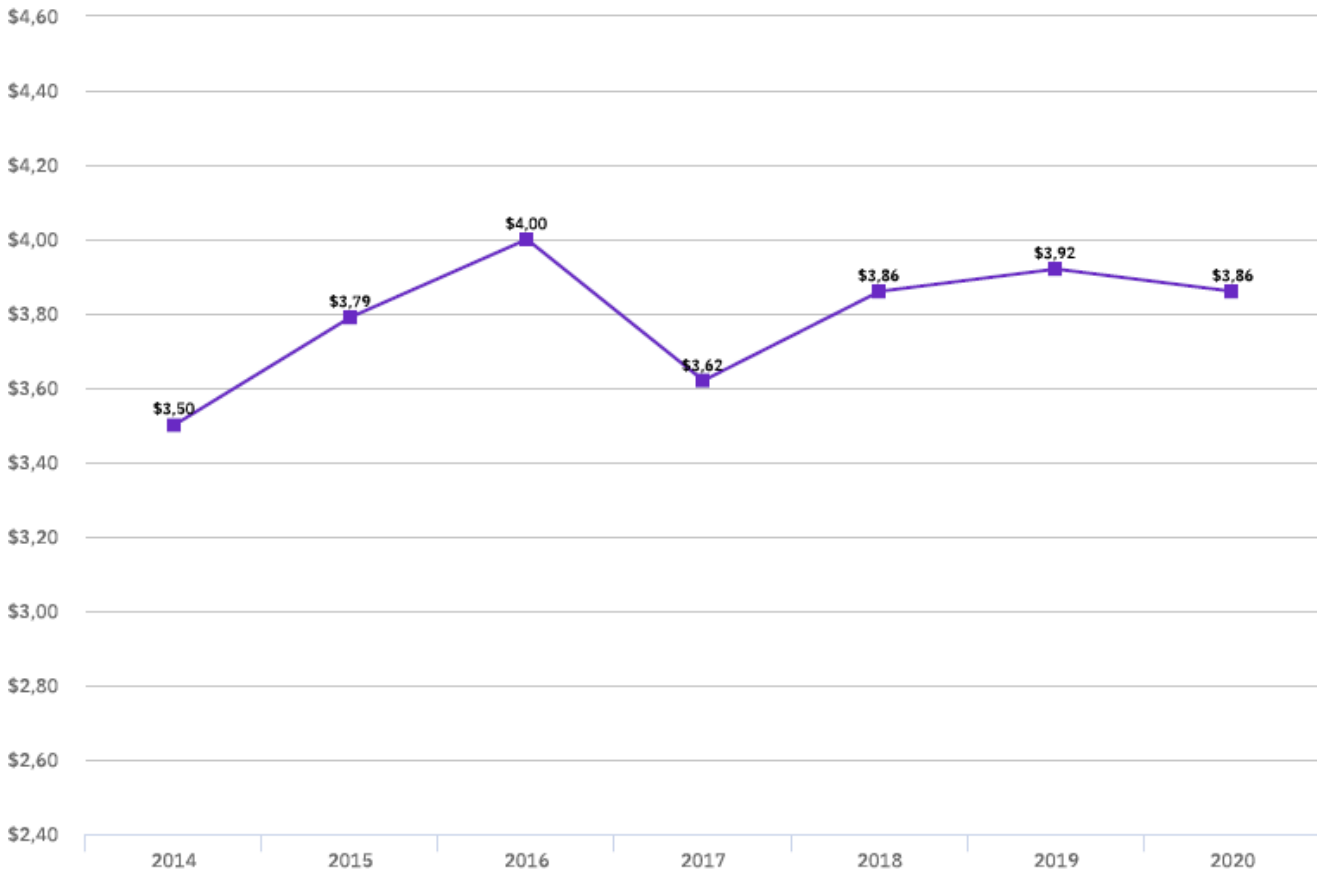
Entre eles estão Estados Unidos, Índia, Reino Unido, Alemanha, Brasil, Japão, França, Oriente Médio, Canadá, Itália, Coreia do Sul, Austrália, Turquia, ASEAN, África do Sul, Escandinávia e, pela primeira vez, América Latina, uma região que inclui México, Argentina, Chile e Colômbia. **A Figura 1** apresenta o tamanho da amostra, a moeda de cada país/região e o número de anos em que o país/região foi incluído na pesquisa.

*Oriente Médio representa um grupo de empresas na Arábia Saudita e nos Emirados Árabes Unidos
#ASEAN representa um grupo de empresas em Cingapura, na Indonésia, nas Filipinas, na Malásia, na Tailândia e no Vietnã
+Escandinávia representa um grupo de empresas na Dinamarca, na Suécia, na Noruega e na Finlândia
**América Latina representa um grupo de empresas no México, na Argentina, no Chile e na Colômbia

Figura 2

Prejuízo total médio de um vazamento de dados

Medido em milhões de dólares (US$)



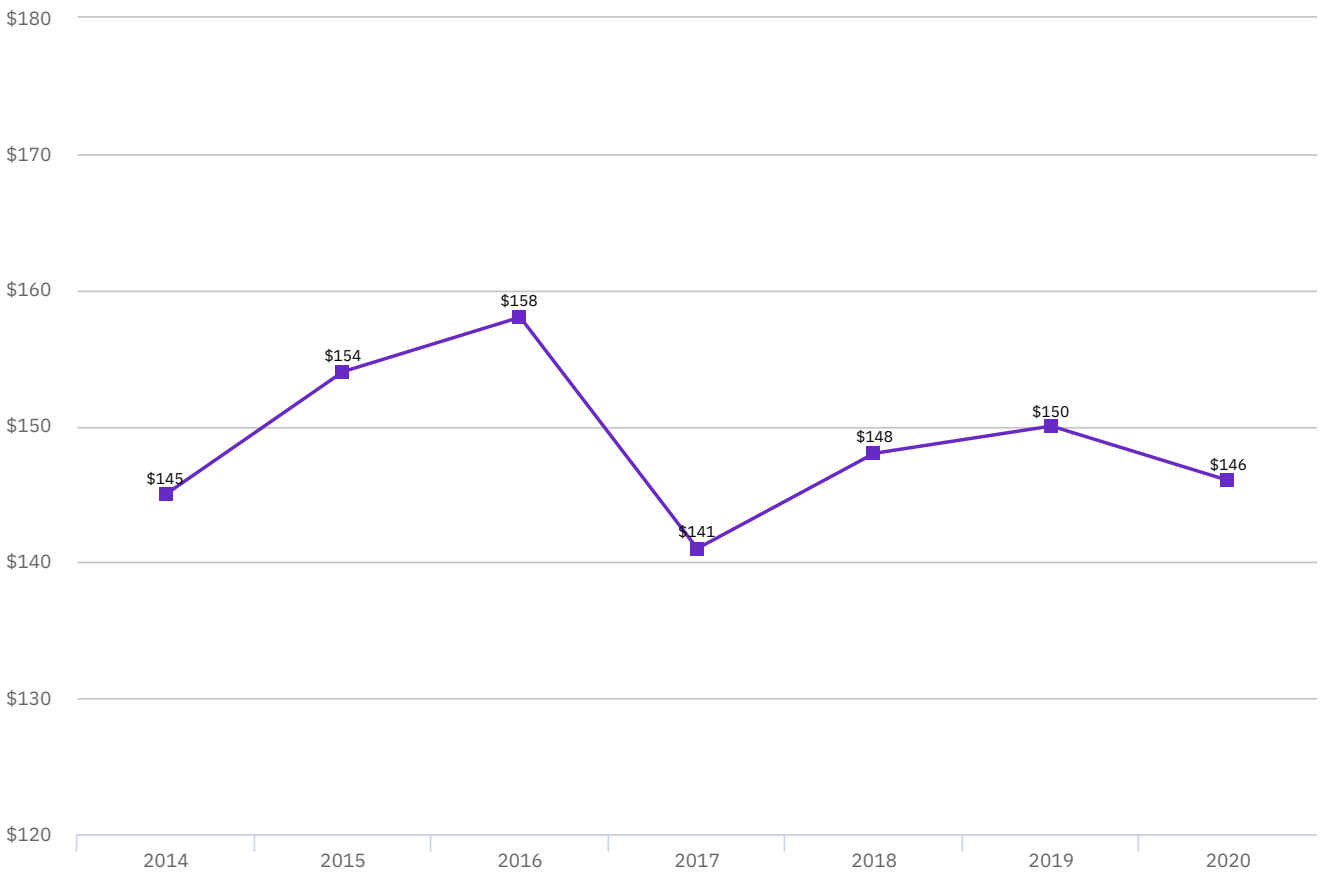
O prejuízo total médio de um vazamento de dados aumentou 10% desde 2014.

A Figura 2 apresenta o prejuízo total médio global de um vazamento de dados em sete anos. O prejuízo total médio consolidado no estudo de 2020 foi de US$ 3,86 milhões, uma ligeira queda em relação aos US$ 3,92 em 2019. A média ponderada é de US$ 3,79 milhões em sete anos.

Figura 3

Prejuízo médio de um vazamento de dados por registro

Medido em dólares (US$)



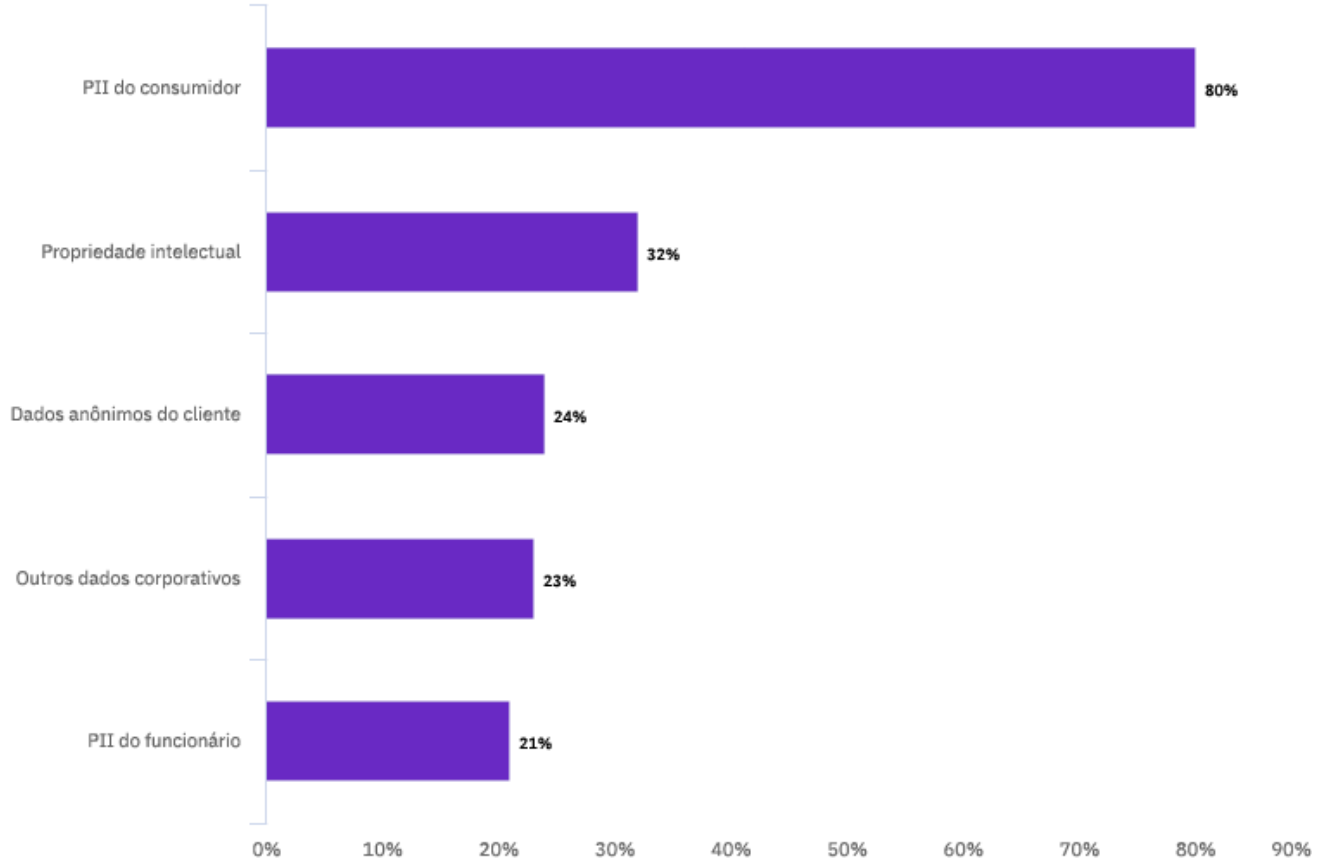
O prejuízo de um vazamento de dados por registro diminuiu ligeiramente para US$ 146.

A Figura 3 mostra o prejuízo médio do vazamento de dados por registro comprometido nos últimos sete anos. A média ponderada em sete anos é de US$ 149 por registro.

Figura 4

Tipos de registros comprometidos

Porcentagem de vazamentos envolvendo dados em cada categoria



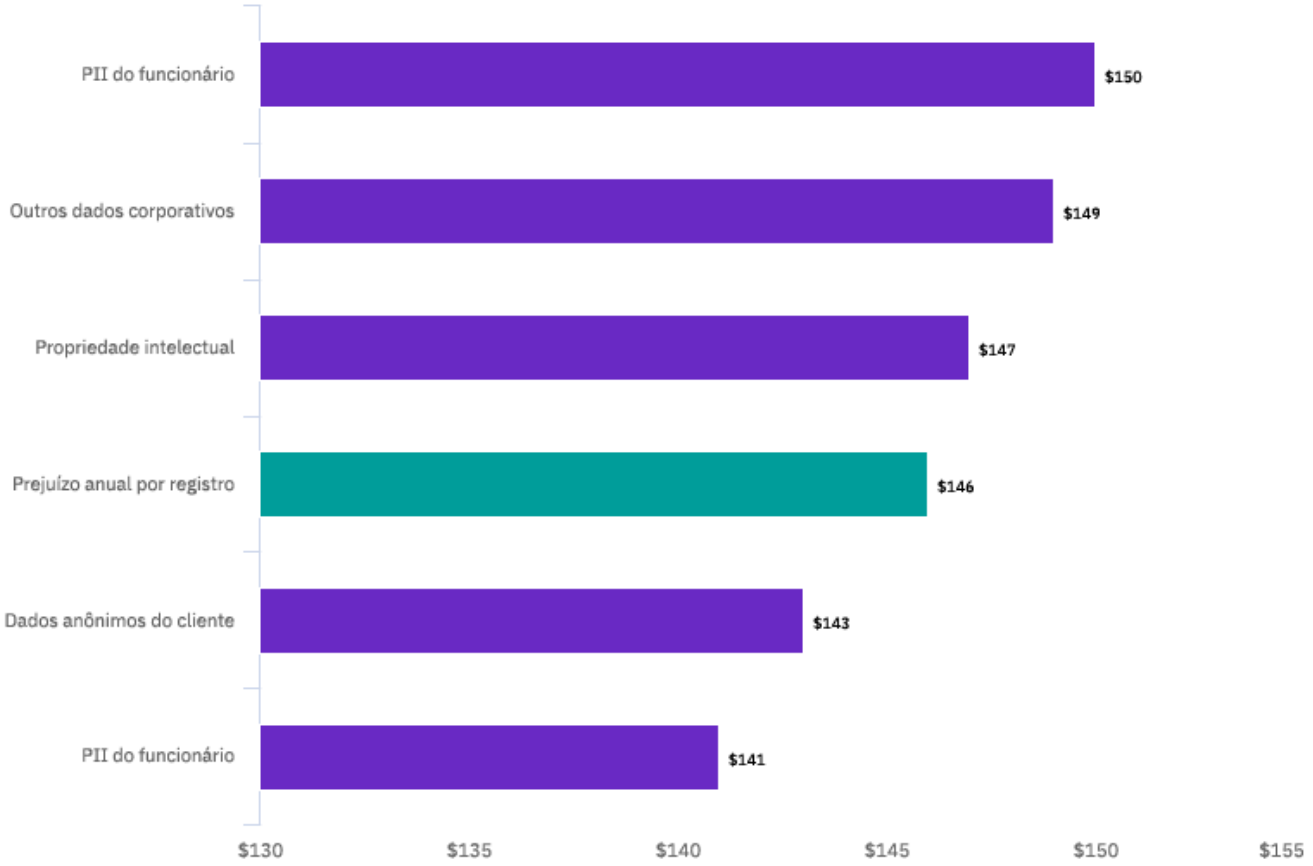
As informações pessoais do cliente foram o tipo de dados mais frequentemente perdido ou roubado nos vazamentos.

A Figura 4 mostra que 80% dos vazamentos de dados incluíram PII do cliente. A propriedade intelectual foi comprometida em 32% dos vazamentos, enquanto que os dados anônimos do cliente foram comprometidos em 24% dos vazamentos.

Figura 5

Prejuízo médio por registro, por tipo de dados comprometidos

Medido em dólares (US$)



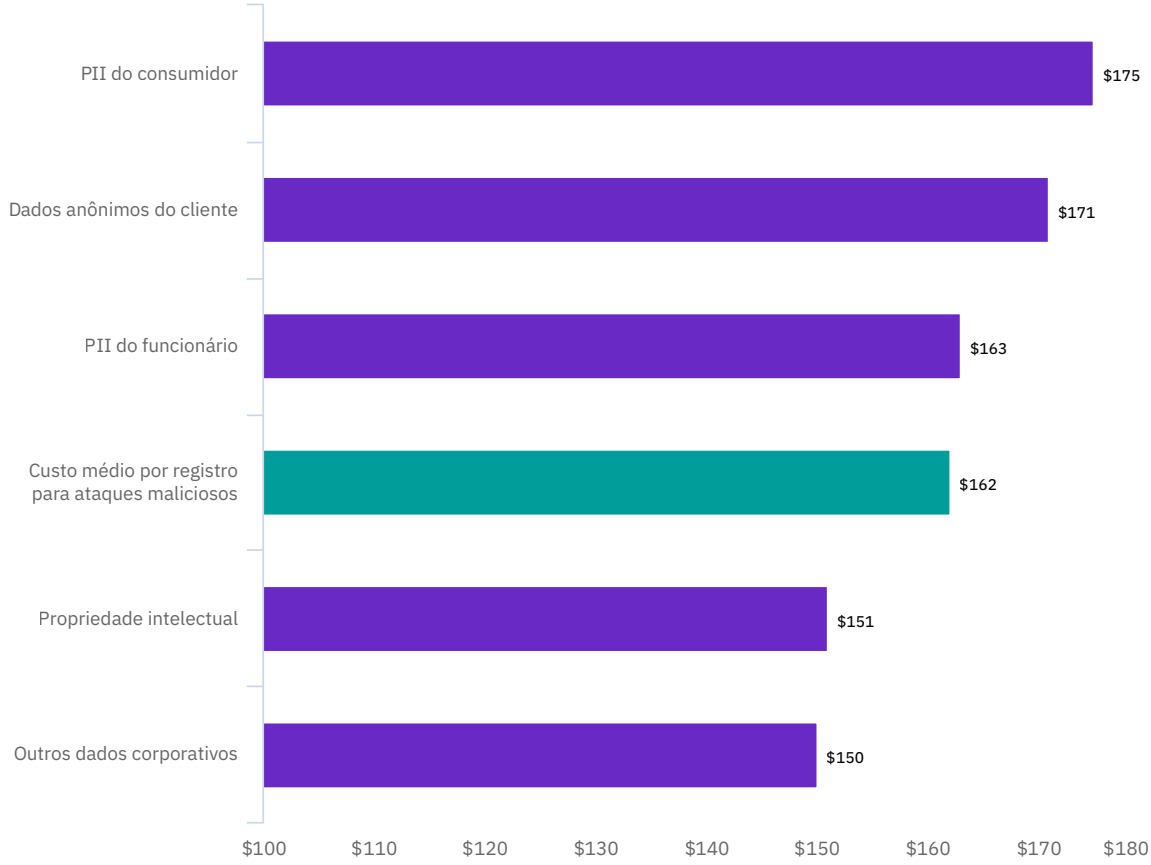
As informações pessoais do cliente foram o tipo de dados comprometidos nos vazamentos com o maior prejuízo.

As PII do cliente custam em média US$ 150 por registro perdido ou roubado, como mostra a **Figura 5**. A propriedade intelectual custa US$ 147 por registro, os dados anônimos do cliente (não PII) custam US$ 143 por registro e as PII dos funcionários custam US$ 141 por registro.

Figura 6

Prejuízo médio por registro, por tipo de dados comprometidos em um ataque mal-intencionado

Medido em dólares (US$)



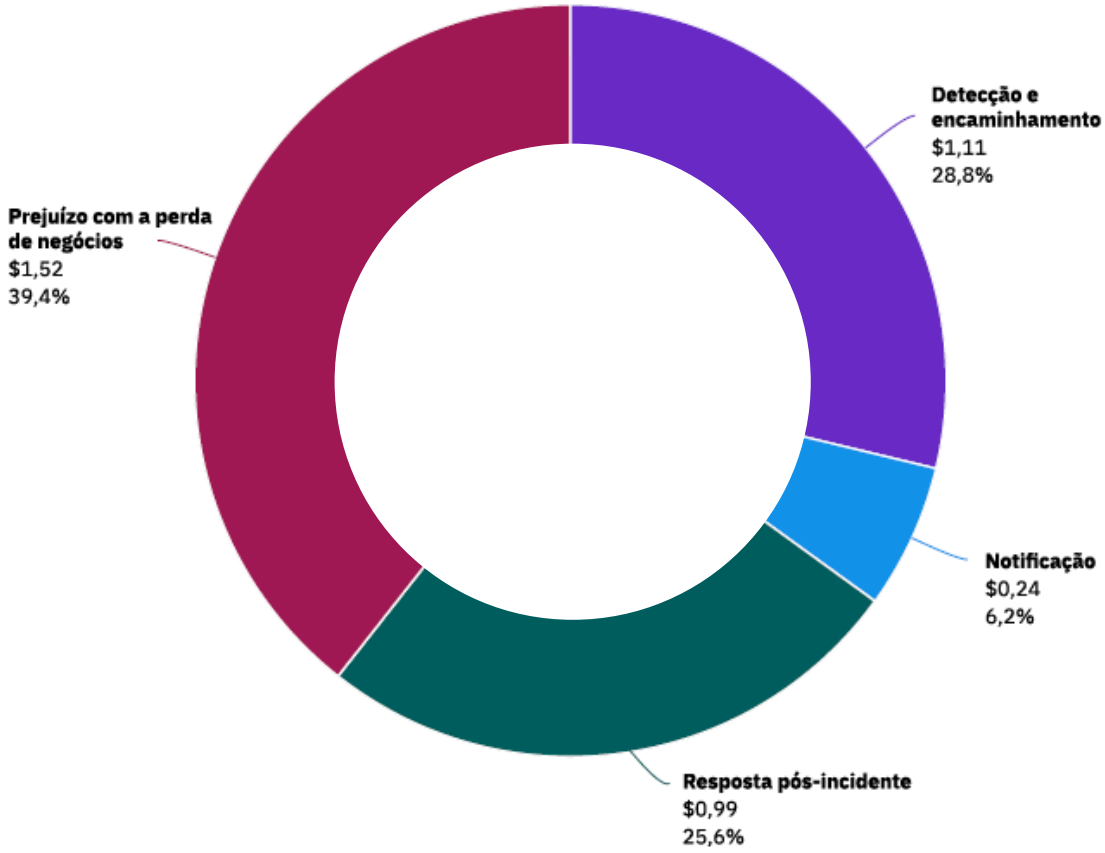
Os prejuízos por registro foram mais altos em vazamentos resultantes de ataques mal-intencionados.

Como mostra a **Figura 6**, o prejuízo por registro das PII do cliente foi de US$ 175 em ataques mal-intencionados, quase 17% a mais do que a média geral do prejuízo das PII do cliente (US$ 150 por registro) comprometidas em outros tipos de vazamento.

Figura 7

Prejuízo total médio de um vazamento de dados dividido em quatro categorias

Medido em milhões de dólares (US$)



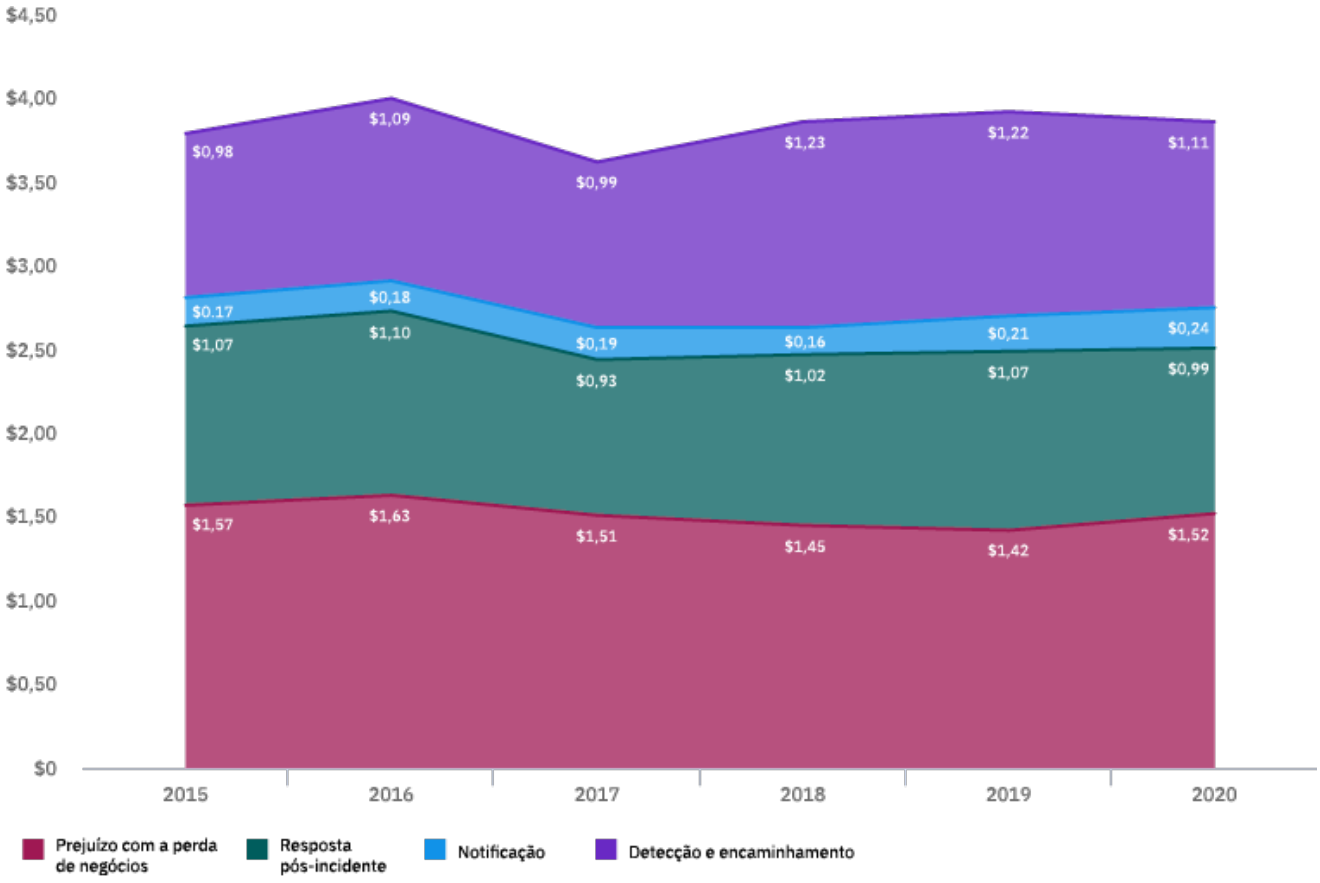
O prejuízo decorrente de negócios perdidos representou a maior parcela do prejuízo médio de um vazamento de dados.

A Figura 7 apresenta os quatro segmentos de prejuízo em dólares americanos e a porcentagem do prejuízo total de um vazamento de dados. A perda de negócios custa em média US$ 1,52 milhão, ou 39% do prejuízo total. O valor mais baixo foi com a notificação do vazamento de dados, de US$ 240.000, ou 6% do prejuízo total.

Figura 8

Tendência no prejuízo médio de um vazamento de dados em quatro categorias

Medido em milhões de dólares (US$)



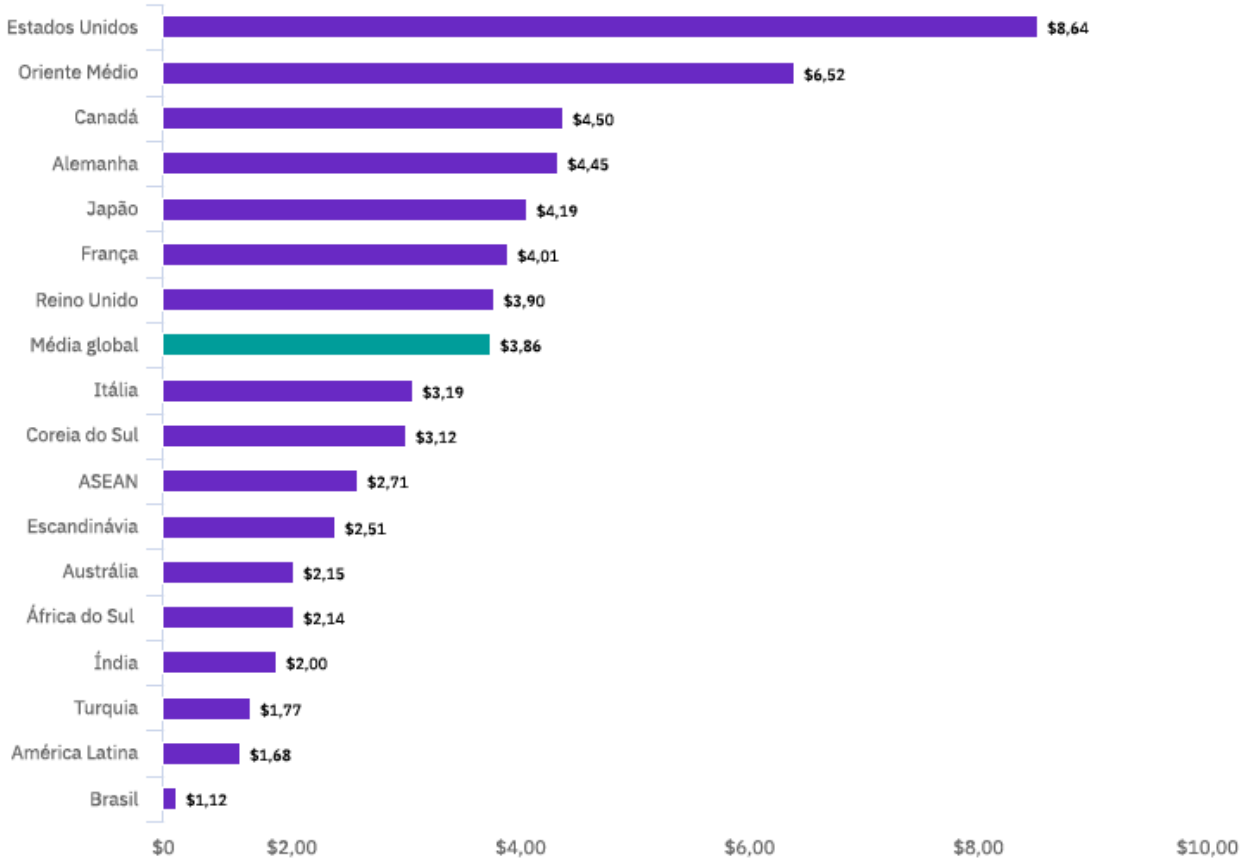
O prejuízo com a perda de negócios aumentou ligeiramente de um ano para o outro.

A Figura 8 mostra as tendências no prejuízo decorrente da perda de negócios, resposta pós-incidente, notificação e detecção e encaminhamento nos últimos seis anos. O padrão mostra consistência no prejuízo. A notificação continua sendo o prejuízo mais baixo, e a perda de negócios o mais alto.

Figura 9

Prejuízo total médio de um vazamento de dados por país ou região

Medido em milhões de dólares (US$)



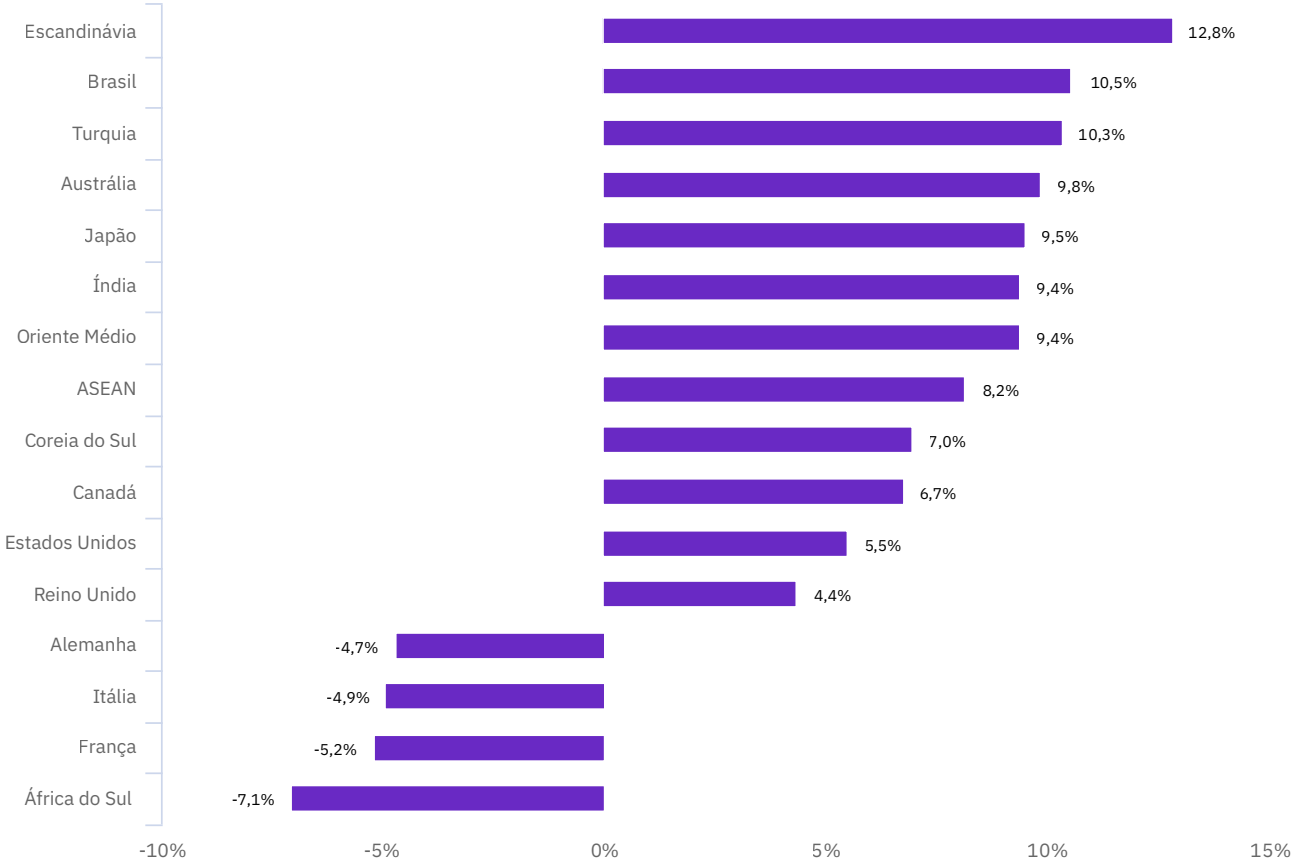
O prejuízo total médio de um vazamento de dados variou por país.

A Figura 9 mostra o prejuízo total médio de um vazamento de dados por país. As organizações nos Estados Unidos tiveram o prejuízo total médio mais alto, com US$ 8,64 milhões, seguidas pelas do Oriente Médio, com US$ 6,52 milhões. Por outro lado, as organizações da América Latina e do Brasil tiveram o menor prejuízo total médio, com US$ 1,68 milhão e US$ 1,12 milhão, respectivamente.

Figura 10

Variação percentual no prejuízo total médio por país ou região, 2019-2020

Calculado usando moeda local



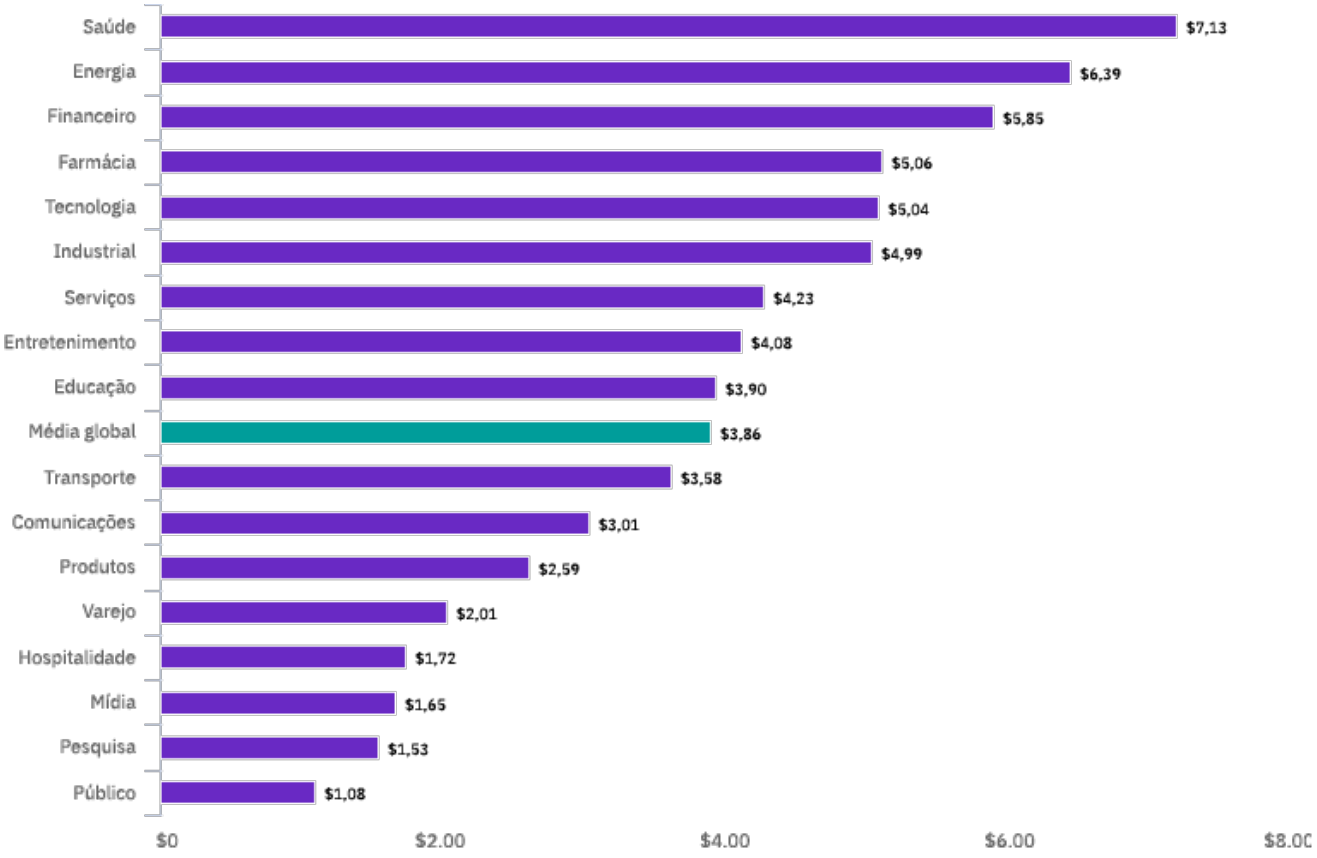
O prejuízo total médio de um vazamento de dados aumentou em 12 dos 16 países.

Como mostra a **Figura 10**, o Scandinavia teve o maior aumento no prejuízo total de um vazamento de dados, e a França e a África do Sul tiveram a maior queda, do estudo de 2019 para o de 2020.

Figura 11

Prejuízo total médio de um vazamento de dados por setor

Medido em milhões de dólares (US$)

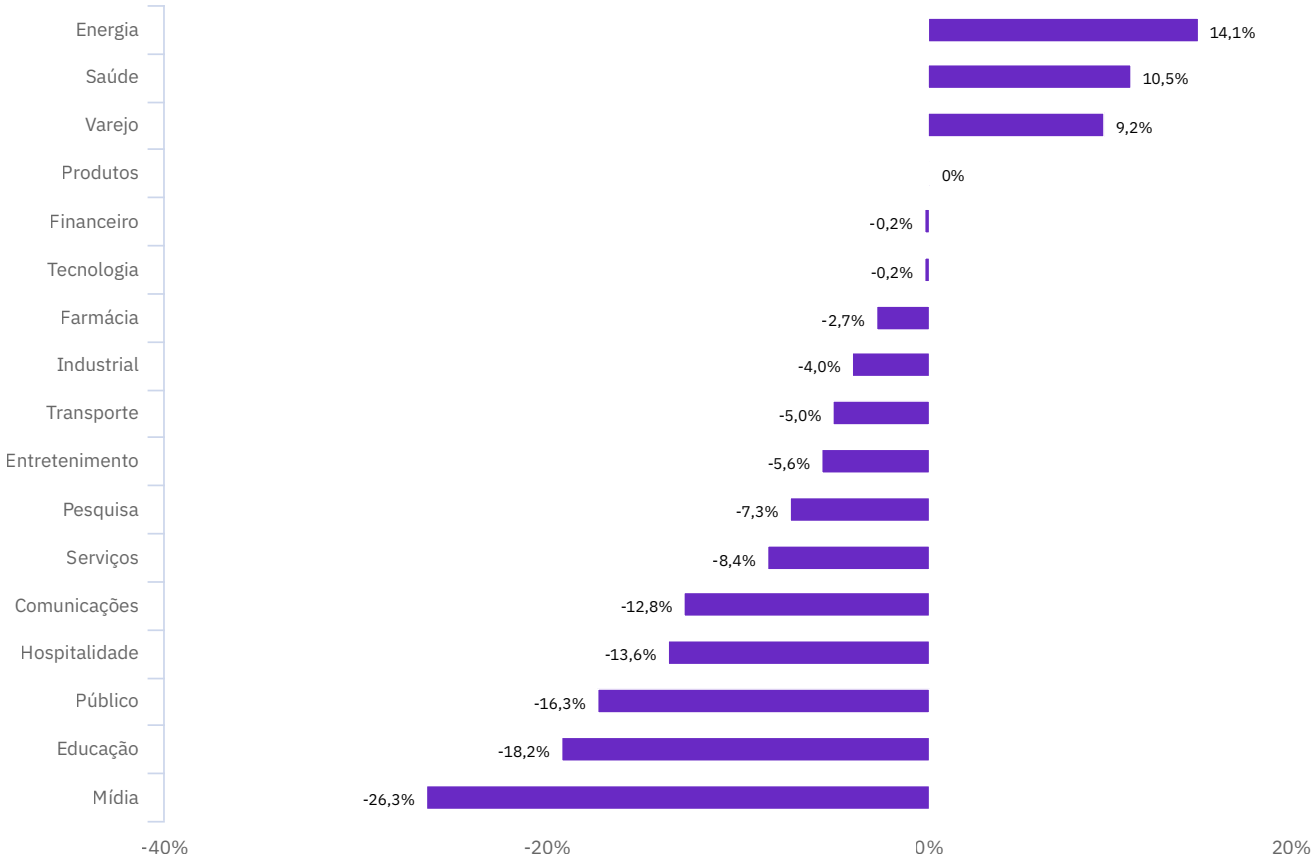


As organizações sujeitas a requisitos regulatórios mais rigorosos tiveram, em média, o prejuízo de um vazamento de dados mais alto.

Como mostra a **Figura 11**, os setores de saúde, energia, financeiro e farmacêutico tiveram um prejuízo total médio de um vazamento de dados significativamente mais alto do que os menos regulamentados, como hospitalidade, mídia e pesquisa. Tradicionalmente, as organizações do setor público têm o menor prejuízo de um vazamento de dados nesta pesquisa, porque é improvável que elas sofram uma perda significativa de clientes como resultado de um incidente desse tipo.

Figura 12

Variação percentual no prejuízo total médio por setor, 2019-2020



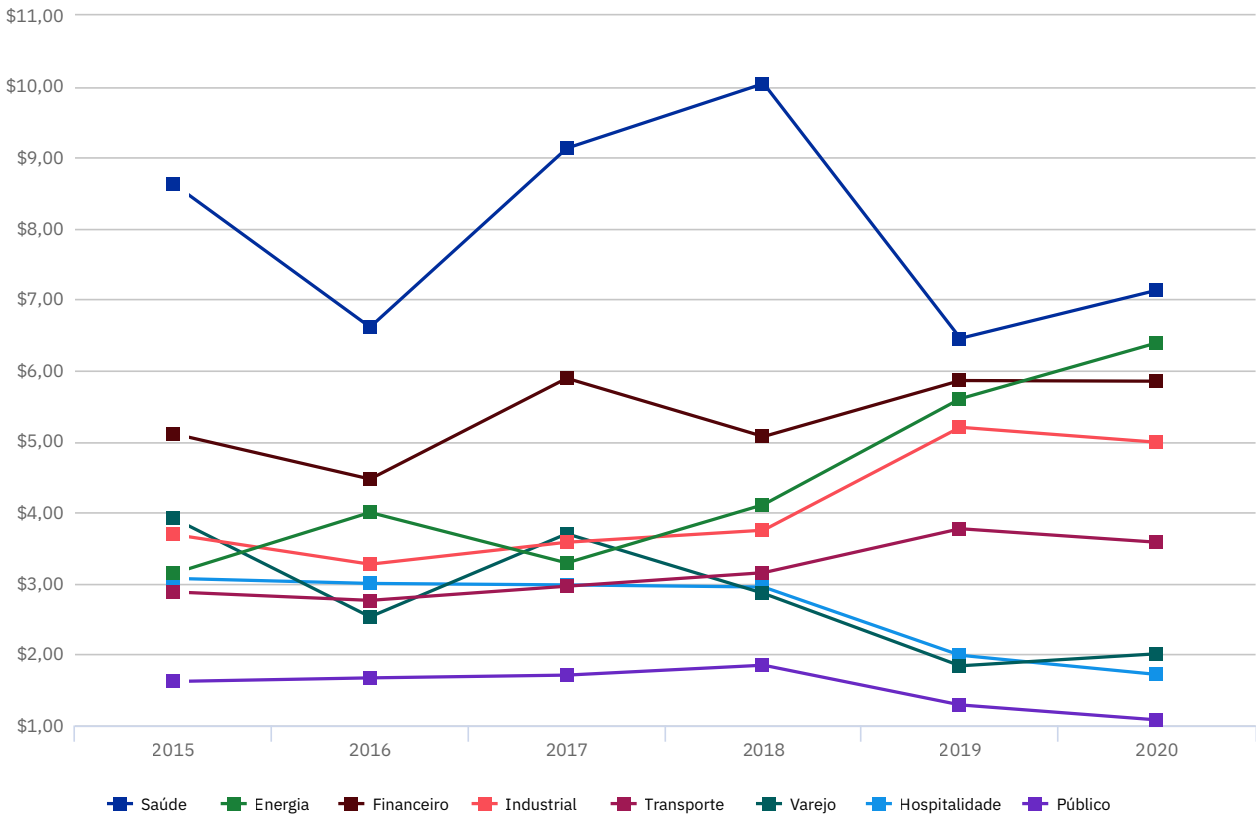
Os setores de energia, saúde e varejo tiveram o maior aumento no prejuízo de um vazamento de dados.

A Figura 12 revela que ocorreu um aumento nos custos de violação de dados em apenas três dos 17 setores entre o estudo de 2019 e o estudo de 2020. Energia, saúde e varejo tiveram os maiores aumentos no prejuízo total médio, enquanto que os setores público, de educação e de mídia tiveram as maiores quedas.

Figura 13

Tendência do prejuízo total médio de um vazamento de dados em oito setores

Medido em milhões de dólares (US$)



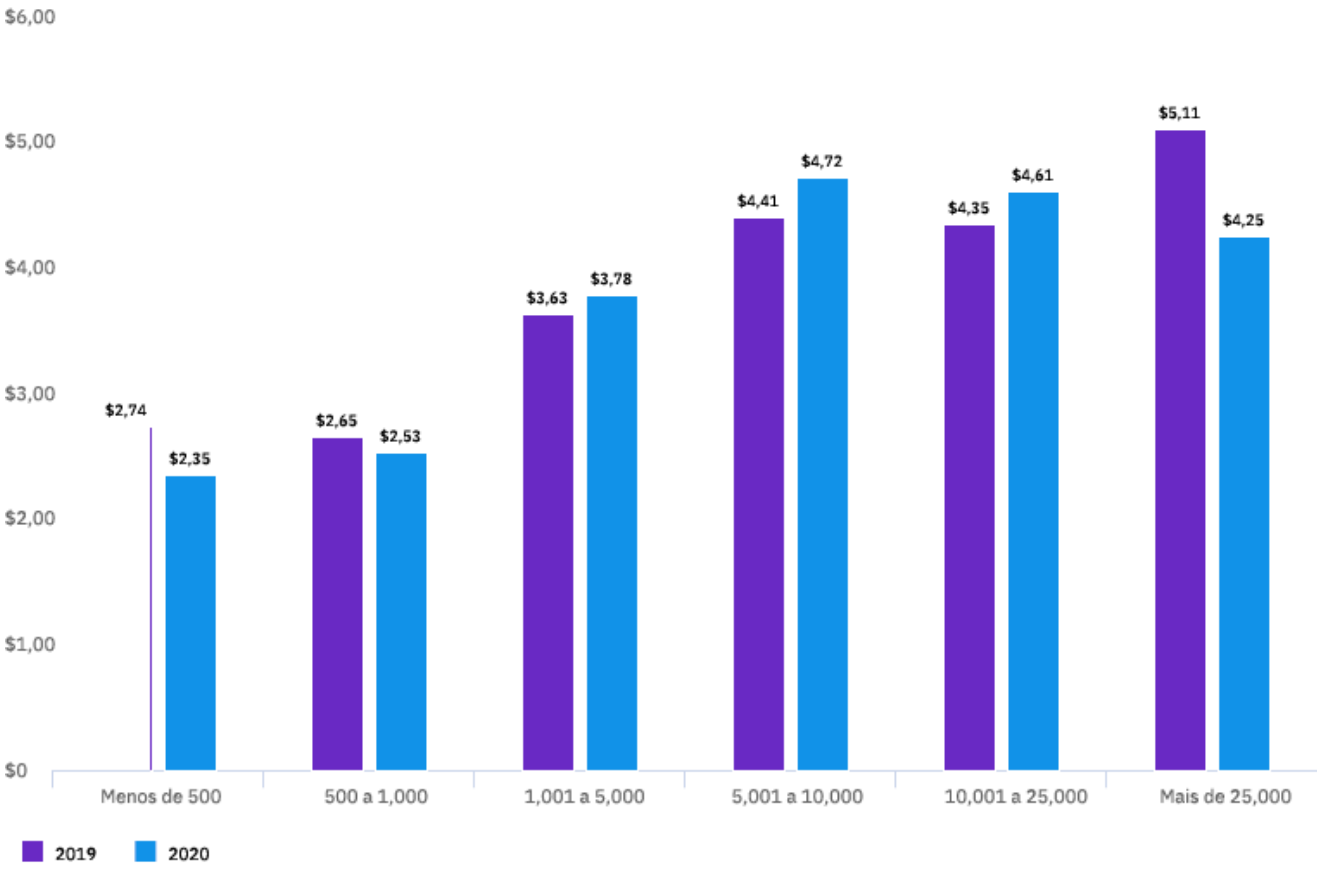
Os setores de saúde e financeiro tiveram os prejuízos mais altos de um vazamento de dados de maneira consistente.

A Figura 13 apresenta um gráfico de linhas para cada um dos oito setores nos últimos seis anos. Consistentemente, o setor de saúde têm o maior prejuízo, e o público o menor.

Figura 14

Prejuízo total médio de um vazamento de dados por tamanho da organização

Medido em milhões de dólares (US$)



O prejuízo médio de um vazamento de dados aumentou nas organizações de médio porte.

A Figura 14 mostra que o prejuízo total médio de um vazamento de dados diminuiu entre os estudos de 2019 e 2020 nas organizações menores (1.000 ou menos funcionários) e nas organizações maiores (mais de 25.000 funcionários). As organizações com mais de 25.000 funcionários sofreram uma queda no prejuízo total médio, de US$ 5,11 milhões em 2019 para US$ 4,25 milhões em 2020, o que representa uma redução de 16.8%. Para organizações de médio porte, no entanto, o prejuízo total de um vazamento aumentou, em média. Na faixa de 5.001 a 10.000 funcionários, o prejuízo de um vazamento aumentou, de US$ 4,41 milhões em 2019 para US$ 4,72 milhões em 2020, em média, representando um aumento de 7%. Proporcionalmente, organizações menores tiveram prejuízos médios mais altos por funcionário.

Principais causas de um vazamento de dados

Por vários anos, este estudo perguntou aos participantes o que causou o vazamento de dados. Nos anos anteriores, essas causas principais foram agrupadas em três categorias: falhas no sistema, incluindo falhas de processos de TI e de negócios; erro humano, incluindo funcionários negligentes ou contratados que, sem querer, causaram um vazamento de dados; e ataques mal-intencionados, que podem ser causados por hackers ou criminosos.

O estudo deste ano continua considerando os vazamentos nessas três categorias. No entanto, em uma análise mais profunda, pedimos aos participantes que forneçam informações mais detalhadas sobre a causa dos vazamentos mal-intencionados, incluindo o vetor inicial de ameaças e o tipo de invasor. Nesta seção, mostramos os resultados dessas duas análises.

Principais conclusões

52%

Parcela de vazamentos causados por ataques mal-intencionados, a um prejuízo médio de US$ 4,27 milhões

19%

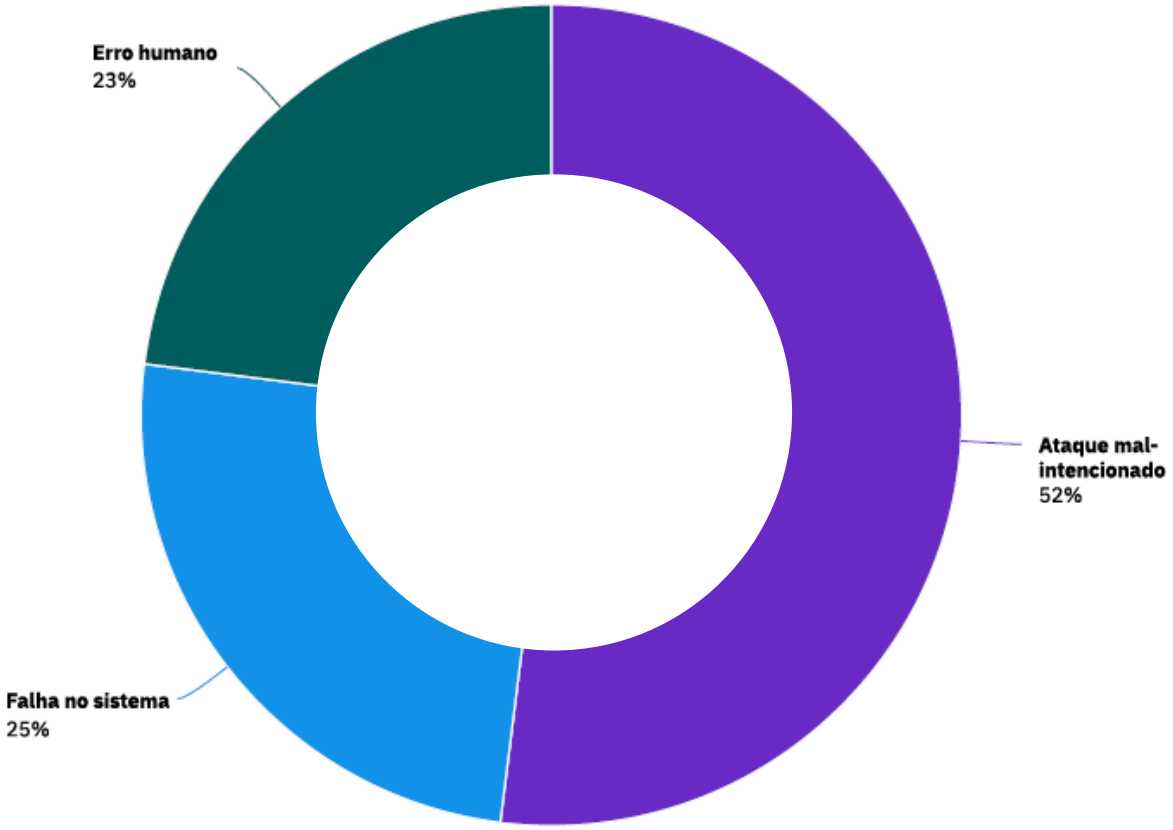
Parcela de vazamentos mal-intencionados causados por credenciais comprometidas (19%) e configuração incorreta da nuvem (19%)

US$ 4,43 milhões

Prejuízo médio dos vazamentos causados por invasores e estado-nação, responsáveis por 13% dos vazamentos mal-intencionados

Figura 15

Distribuição das principais causas do vazamento de dados em três categorias



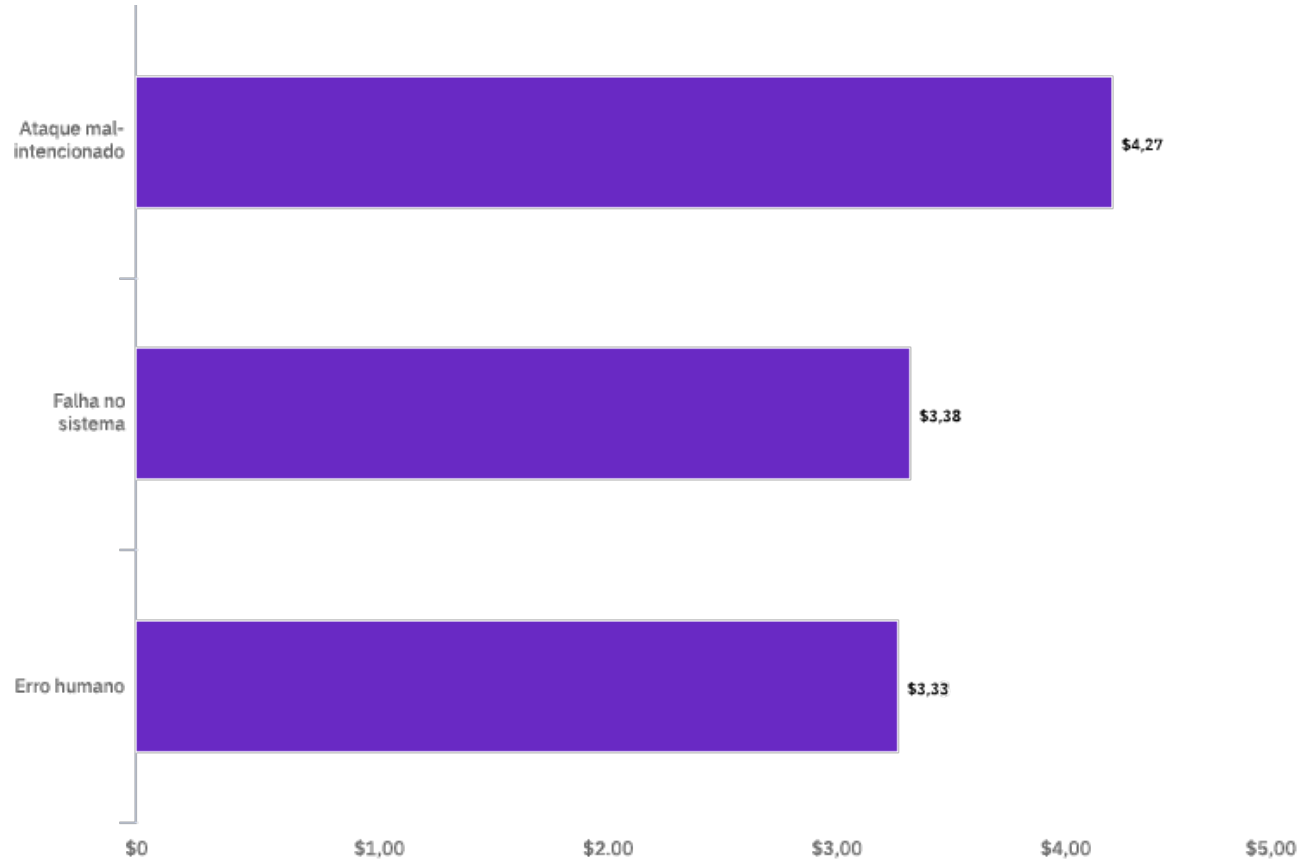
Ataques mal-intencionados causaram a maioria dos vazamentos de dados.

A Figura 15 mostra um resumo das três principais categorias de causas de um vazamento de dados. Cinquenta e dois por cento dos incidentes envolveram um ataque mal-intencionado, em comparação com 25% causados por falhas no sistema e 23% por erro humano.

Figura 16

Prejuízo total médio das três causas principais do vazamento de dados

Medido em milhões de dólares (US$)



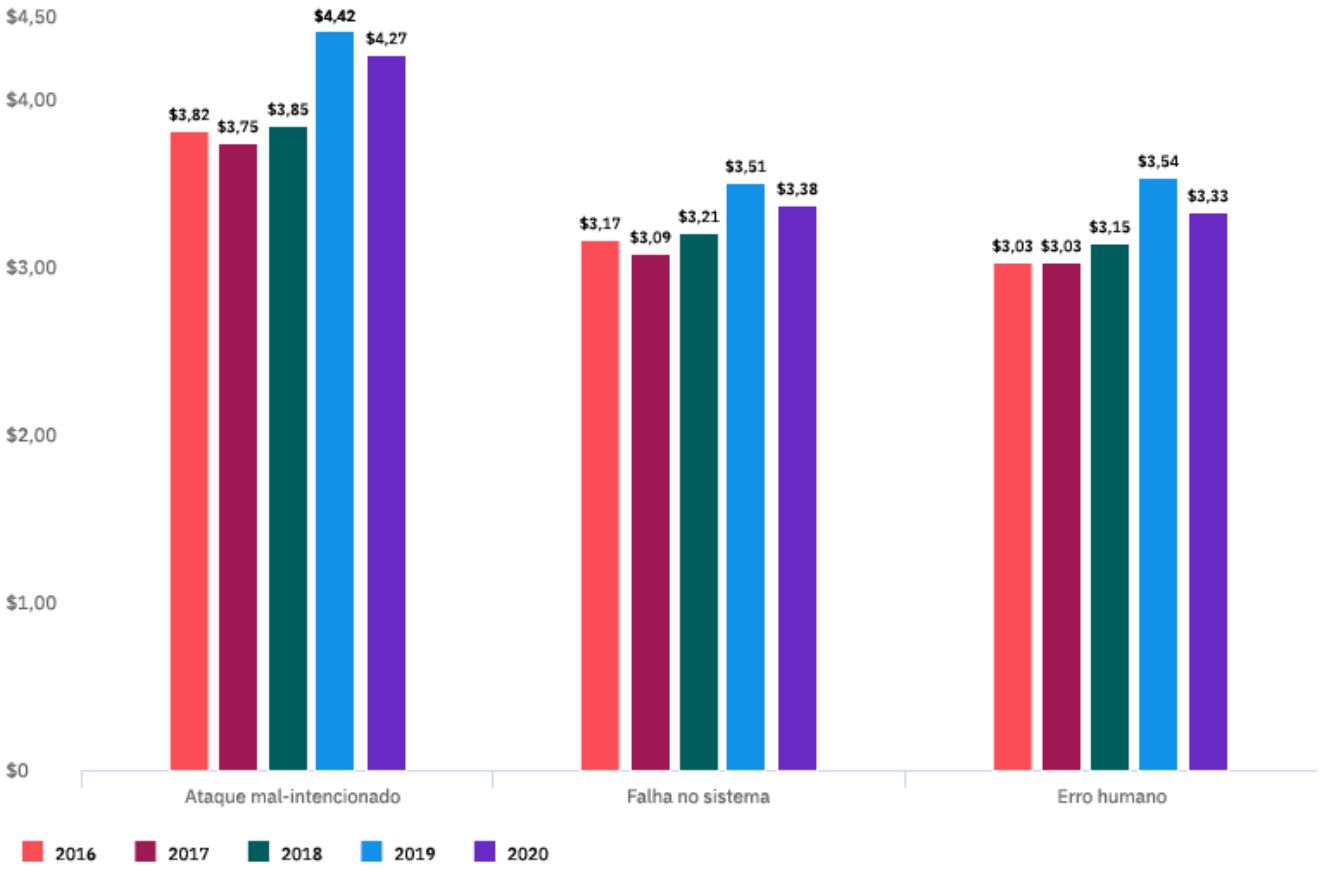
O ataque mal-intencionado foi a causa principal com maior prejuízo.

No estudo de 2020, os vazamentos causados por ataques mal-intencionados custaram, em média, US$ 4,27 milhões, quase US$ 1 milhão a mais do que os causados por falha no sistema ou erro humano, como mostra a **Figura 16**.

Figura 17

Tendência no prejuízo total médio por causa principal do vazamento de dados

Medido em milhões de dólares (US$)

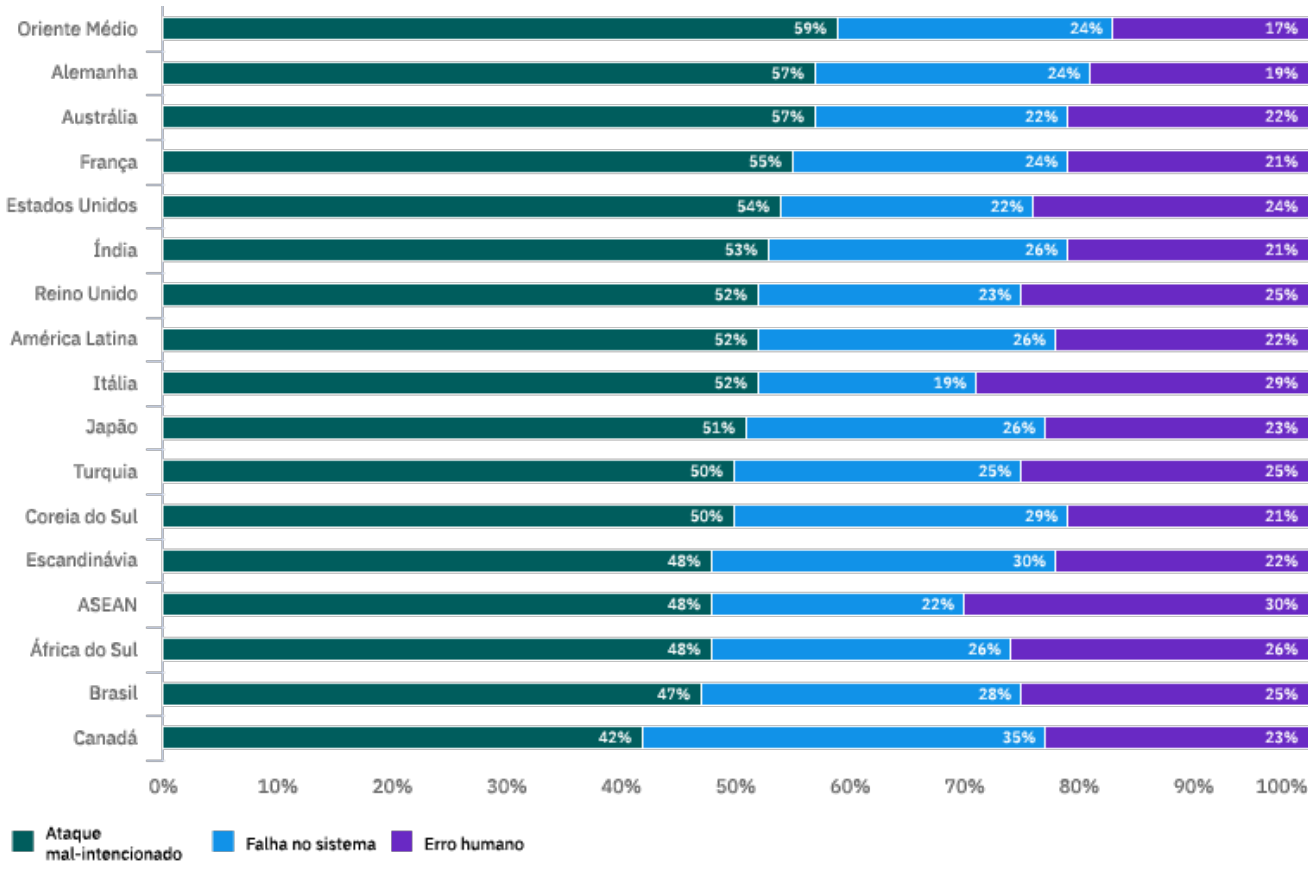


Os vazamentos mal-intencionados continuaram causando o maior prejuízo nos últimos cinco anos.

A Figura 17 mostra o prejuízo total médio das três causas principais do vazamento de dados nos últimos cinco anos. Desde o estudo de 2016, o padrão das causas principais permaneceu bastante constante, com uma ligeira diminuição no prejuízo no estudo de 2020 em comparação com 2019. O prejuízo total médio de um vazamento mal-intencionado aumentou quase 12% desde o estudo de 2016.

Figura 18

Distribuição das principais causas do vazamento de dados por país ou região

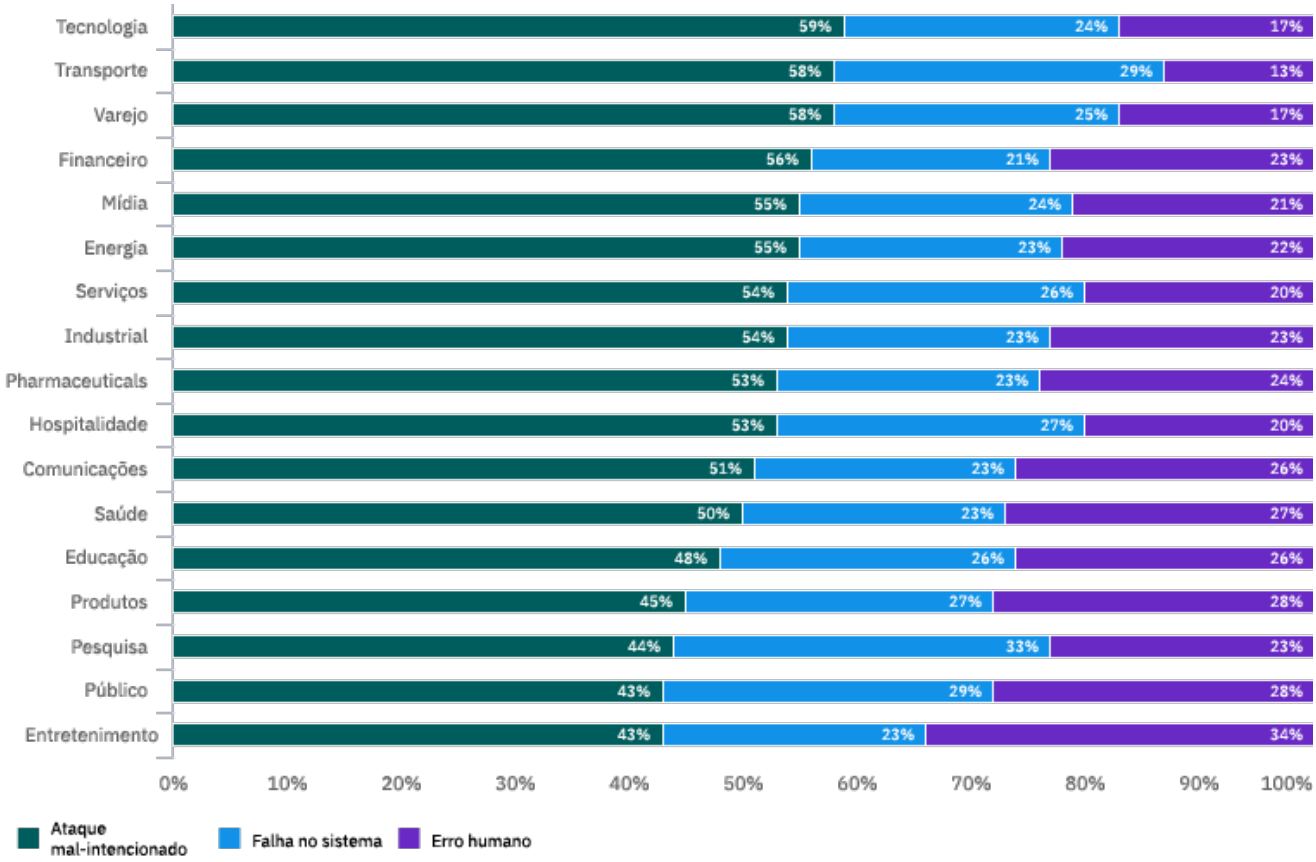


As principais causas do vazamento variaram por localização.

O Oriente Médio, a Alemanha e a Austrália tiveram a maior porcentagem de vazamentos causados por ataques mal-intencionados, enquanto a África do Sul, o Brasil e o Canadá tiveram a menor porcentagem desses ataques, de acordo com a **Figura 18**. Vazamentos de dados causados por falhas no sistema são mais frequentes no Canadá. A ASEAN e a Itália tiveram a maior porcentagem de vazamentos de dados causados por erro humano.

Figura 19

Distribuição das principais causas do vazamento de dados por setor



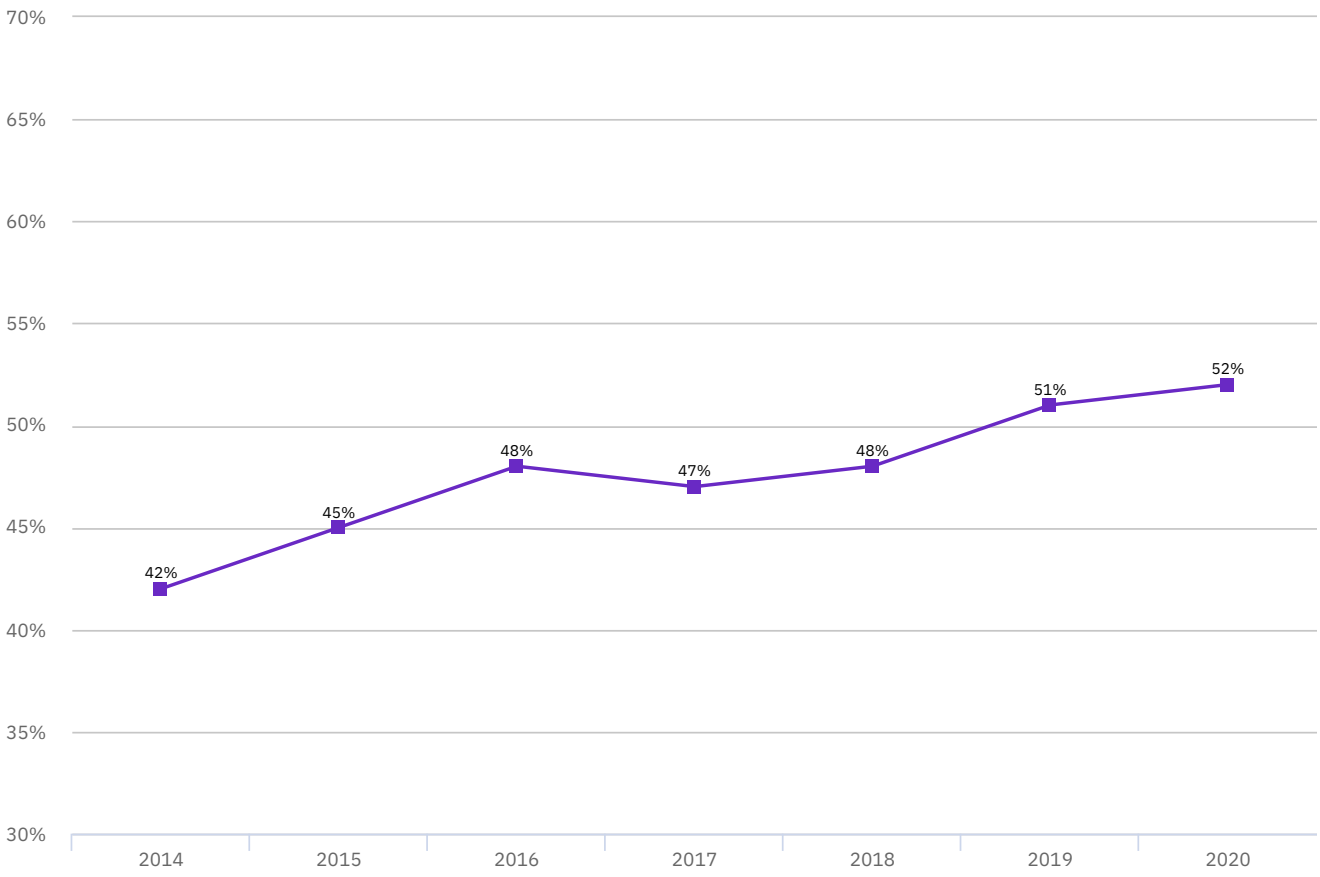
A distribuição das principais causas do vazamento de dados variou por setor.

Como mostra a **Figura 19**, os setores de tecnologia, transporte, varejo e financeiro tiveram a maior porcentagem de ataques mal-intencionados. Os setores de entretenimento, público e de produtos tiveram a maior porcentagem de vazamentos de dados causados por erro humano. Falhas no sistema foram as causas mais frequentes de um vazamento nos setores de pesquisa, público e de transporte.

Figura 20

Tendência no vazamento de dados causado por um ataque mal-intencionado

Porcentagem de todos os vazamentos



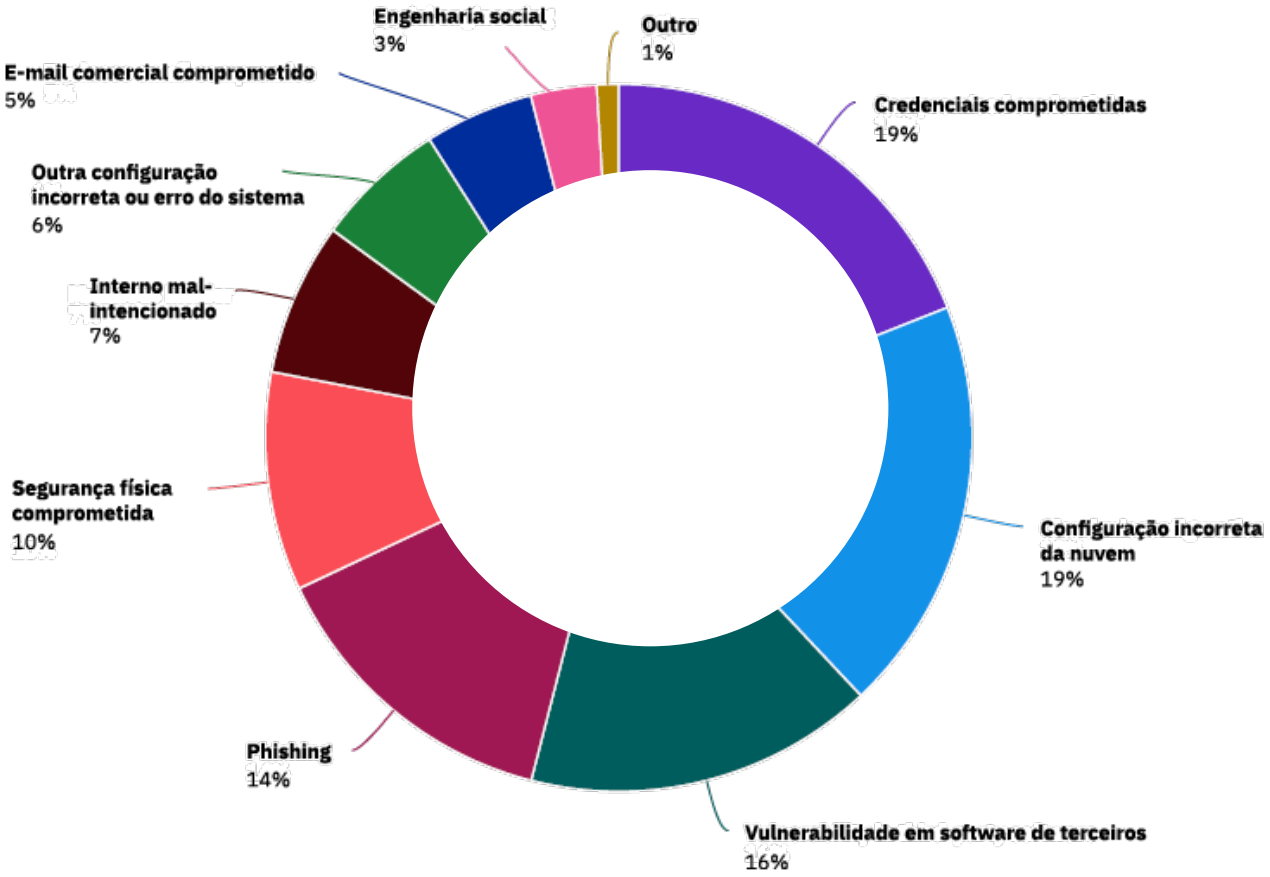
A parcela de vazamentos causados por ataques mal-intencionados aumentou de forma constante ao longo do tempo.

A Figura 20 mostra que a parcela de vazamentos causados por ataques mal-intencionados aumentou de 42%, no relatório de 2014, para 52%, no de 2020. Esse aumento de 10 pontos percentuais representa um aumento de quase 24% (taxa de crescimento) na parcela de vazamentos causados por ataques mal-intencionados.

Figura 21

Distribuição das principais causas do vazamento mal-intencionado de dados por vetor de ameaça

Porcentagem de vazamentos causados por ataque mal-intencionado

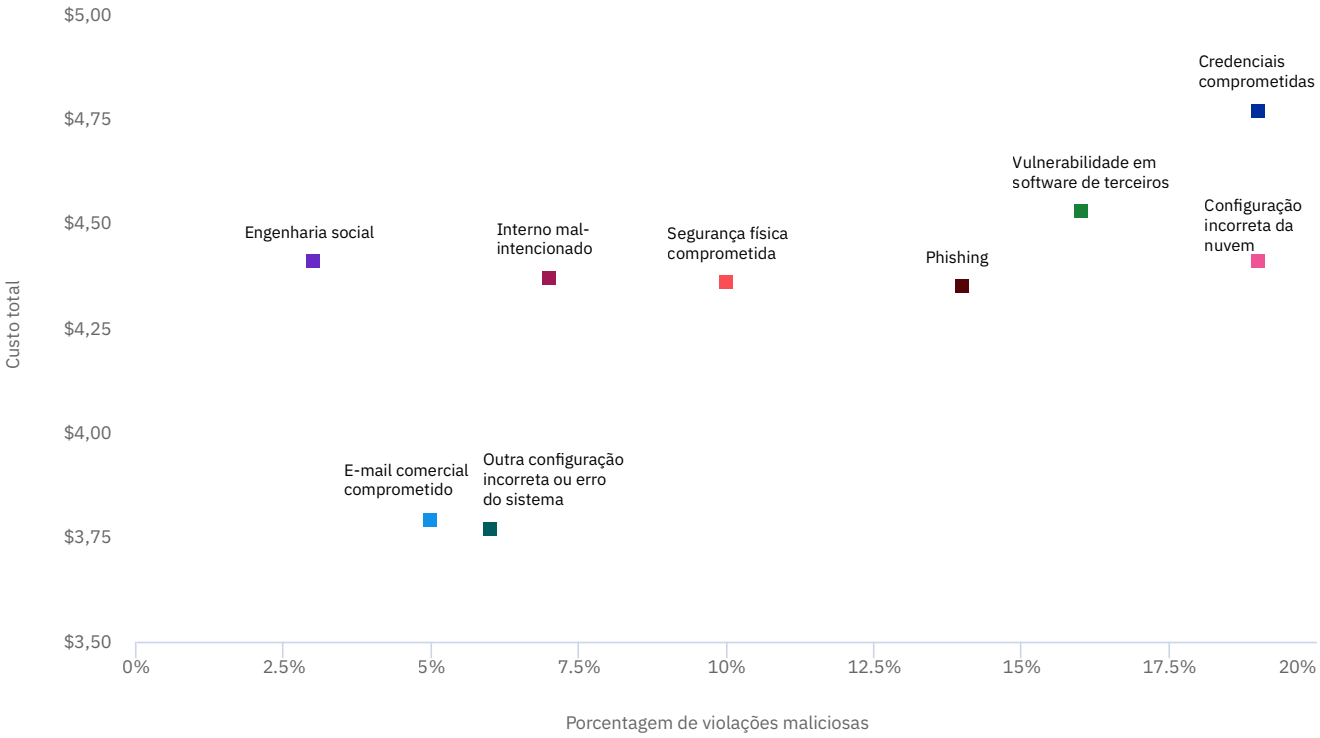


A maioria dos vazamentos mal-intencionados foi causada por credenciais comprometidas, configurações incorretas da nuvem ou vulnerabilidade de software de terceiros.

Credenciais roubadas ou comprometidas e configuração incorreta da nuvem foram os principais vetores de ameaça iniciais, cada um responsável por 19% dos vazamentos mal-intencionados. A vulnerabilidade de software de terceiros foi o vetor de ameaça inicial em 16% dos vazamentos mal-intencionados, de acordo com a **Figura 21**.

Figura 22

Prejuízo e frequência médios de vazamentos mal-intencionados de dados por vetor de causa principal

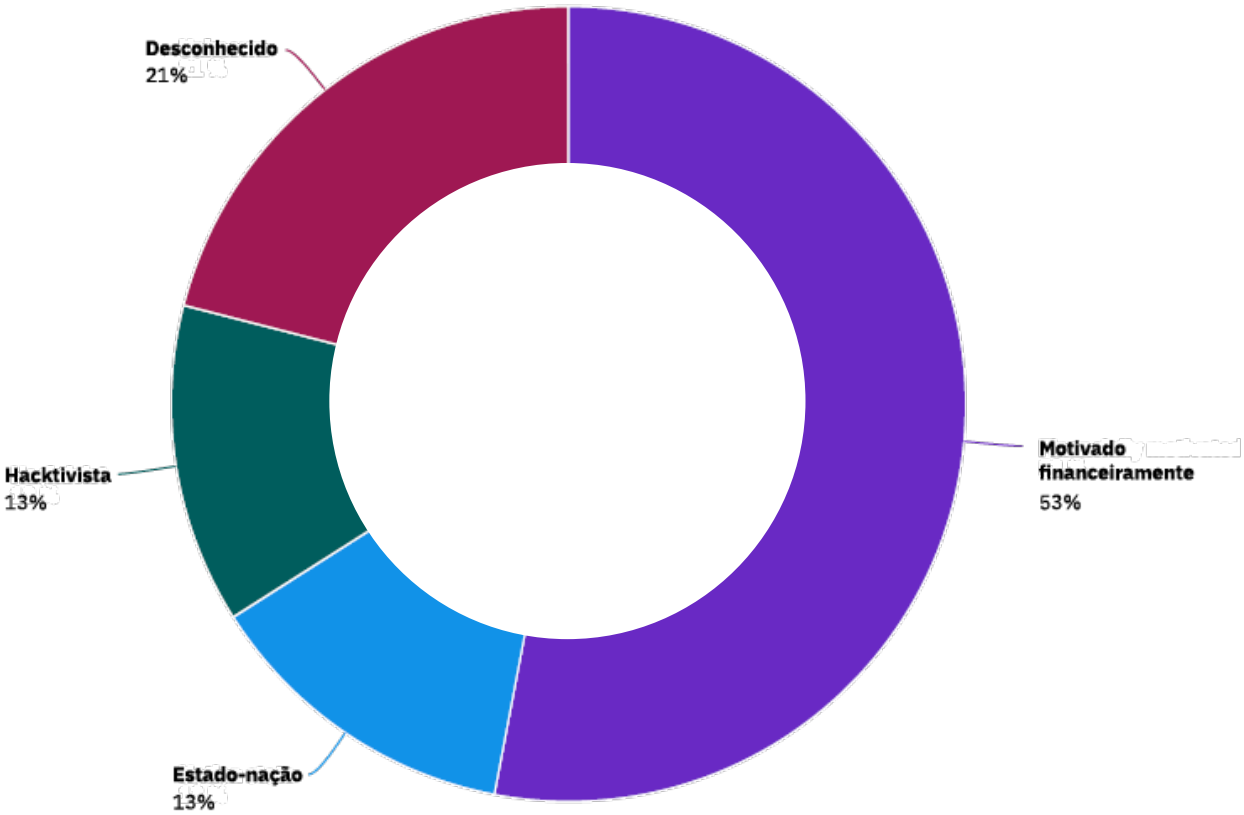


Credenciais comprometidas foram o vetor de ameaça de maior prejuízo e frequência.

A Figura 22 mostra nove vetores iniciais de ameaças em vazamentos mal-intencionados em um gráfico de dispersão, com a porcentagem de vazamentos representada no eixo X e o prejuízo total médio no eixo Y. Credenciais comprometidas são o vetor de ameaça mais à direita no gráfico, mostrando a forte combinação de frequência e prejuízo em vazamentos mal-intencionados de dados.

Figura 23

Vazamentos mal-intencionados de dados organizados por tipo de invasor



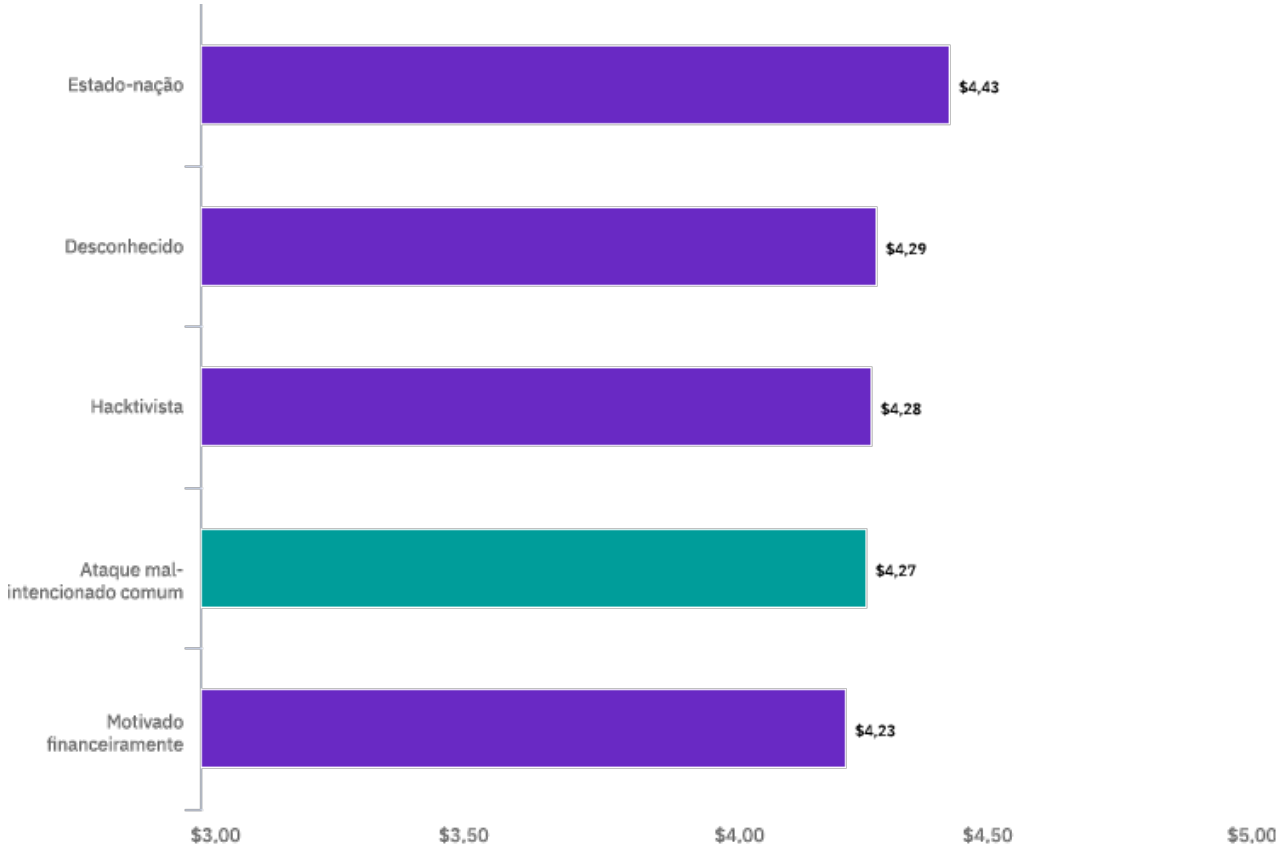
Invasores motivados financeiramente causaram a maioria dos vazamentos mal-intencionados de dados.

De acordo com a **Figura 23**, a maioria dos vazamentos mal-intencionados, 53%, foi causada por invasores motivados financeiramente. Invasores de estado-nação estavam envolvidos em 13% dos vazamentos mal-intencionados, os hacktivistas em 13%, e 21% desse tipo de vazamento foram causados por invasores com motivação desconhecida.

Figura 24

Prejuízo médio de um vazamento mal-intencionado de dados por tipo de invasor

Medido em milhões de dólares (US$)



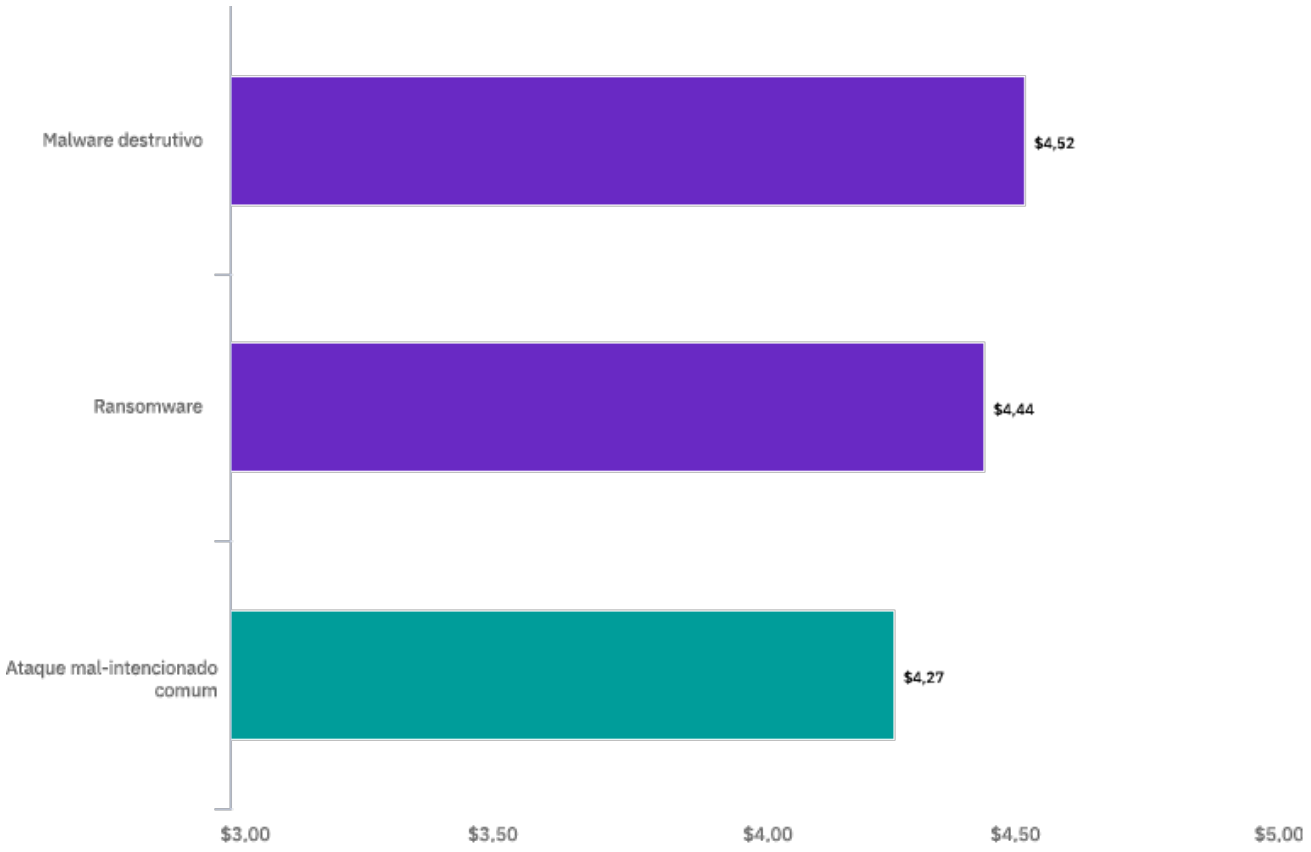
Invasores de estado-nação causaram os vazamentos mal-intencionados de maior prejuízo.

A Figura 24 apresenta o prejuízo de um vazamento de dados por tipo de invasor. Os vazamentos mal-intencionados de maior prejuízo foram causados por invasores de estado-nação, com uma média de US$ 4,43 milhões. Os hacktivistas foram responsáveis por vazamentos mal-intencionados que custaram, em média, US$ 4,28 milhões, enquanto os vazamentos causados por criminosos virtuais motivados financeiramente custaram, em média, US$ 4,23 milhões.

Figura 25

Prejuízo médio de um vazamento por ransomware ou malware destrutivo

Medido em milhões de dólares (US$)



Os vazamentos causados por ransomware e malware destrutivo causam um prejuízo maior em relação aos causados por ataque mal-intencionado comum.

Os ataques mal-intencionados que destruíram dados em ataques destrutivos/do tipo deletério (prejuízo médio de US$ 4,52 milhões) e os ataques de ransomware (US$ 4,44 milhões) foram mais caros do que o vazamento mal-intencionado (US$ 4,27 milhões) ou o vazamento de dados (US$ 3,86 milhões), em média, como mostra a **Figura 25**.

Fatores que influenciam no prejuízo de um vazamento de dados

Esta seção analisa mais detalhadamente uma infinidade de fatores que influenciam o prejuízo de um vazamento de dados, como vários tipos de práticas e tecnologias de segurança, ambientes de TI e envolvimento de terceiros. O estudo deste ano inclui uma análise de 25 fatores exclusivos de prejuízo que tiveram uma influência atenuante, diminuindo o prejuízo total médio de um vazamento, ou amplificadora, aumentando esse prejuízo.

Vários fatores são novos no relatório deste ano: teste de equipe vermelho, teste de vulnerabilidade e serviços de segurança gerenciados (fatores de redução do prejuízo); escassez de especialistas em segurança e trabalho remoto (fatores de aumento do prejuízo).

Esta seção também examina mais profundamente três áreas que demonstraram ter uma influência atenuante no prejuízo de um vazamento de dados: o papel do CISO, o seguro contra ataques virtuais e a resposta a incidentes.

Principais conclusões

US$ 291.870

Aumento do prejuízo total médio de um vazamento de dados associado a sistemas de segurança complexos

51%

Parcela de organizações com seguro contra ataques virtuais que abriram sinistros para cobrir os gastos com consultoria e serviços jurídicos

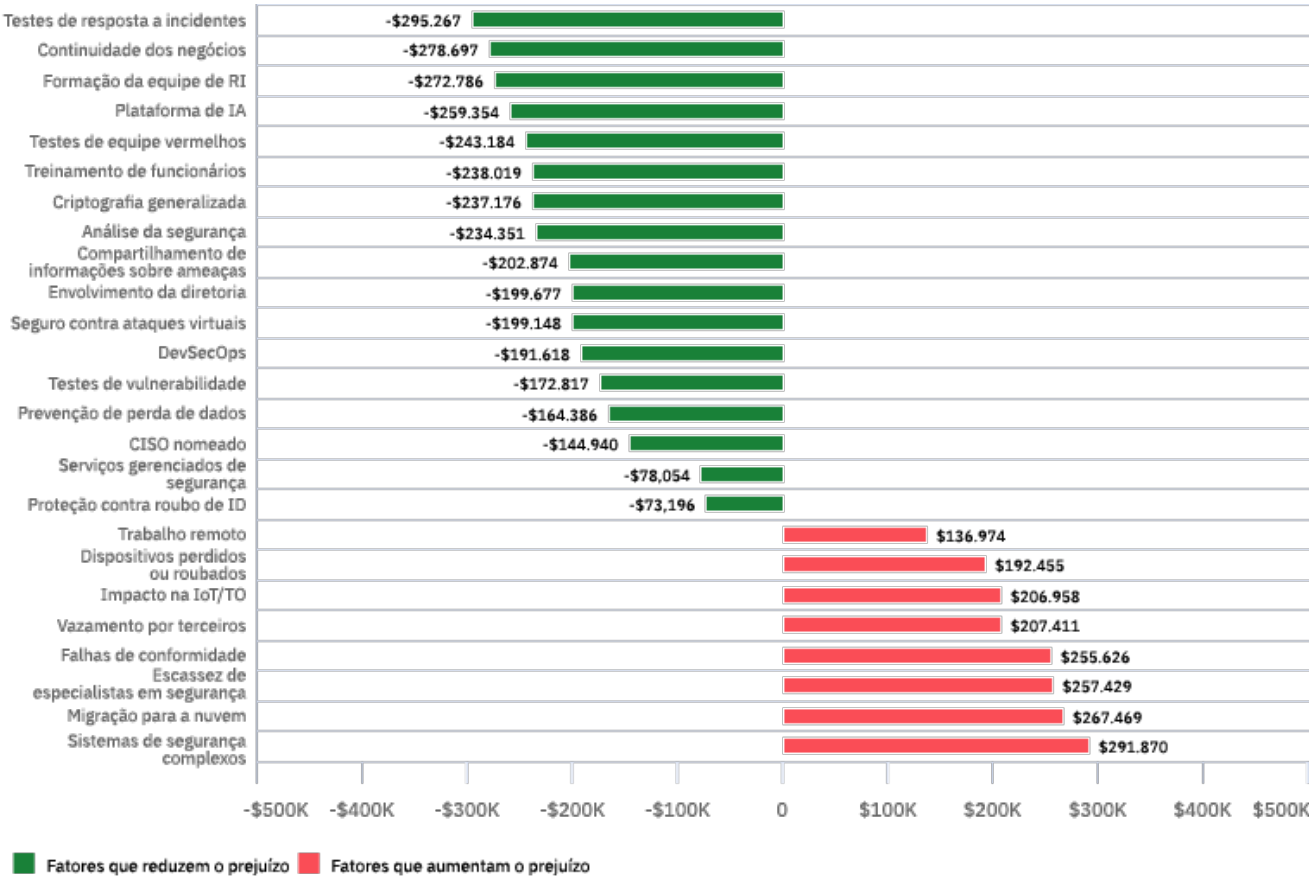
46%

Parcela de entrevistados que disseram que o CISO é o maior responsável pelo vazamento de dados

Figura 26

Impacto dos 25 fatores principais no prejuízo total médio de um vazamento de dados

Diferença em US$ do prejuízo total médio de US$ 3,86 milhões



A complexidade do sistema de segurança e o teste do plano de resposta a incidentes tiveram o maior impacto no prejuízo total de um vazamento de dados.

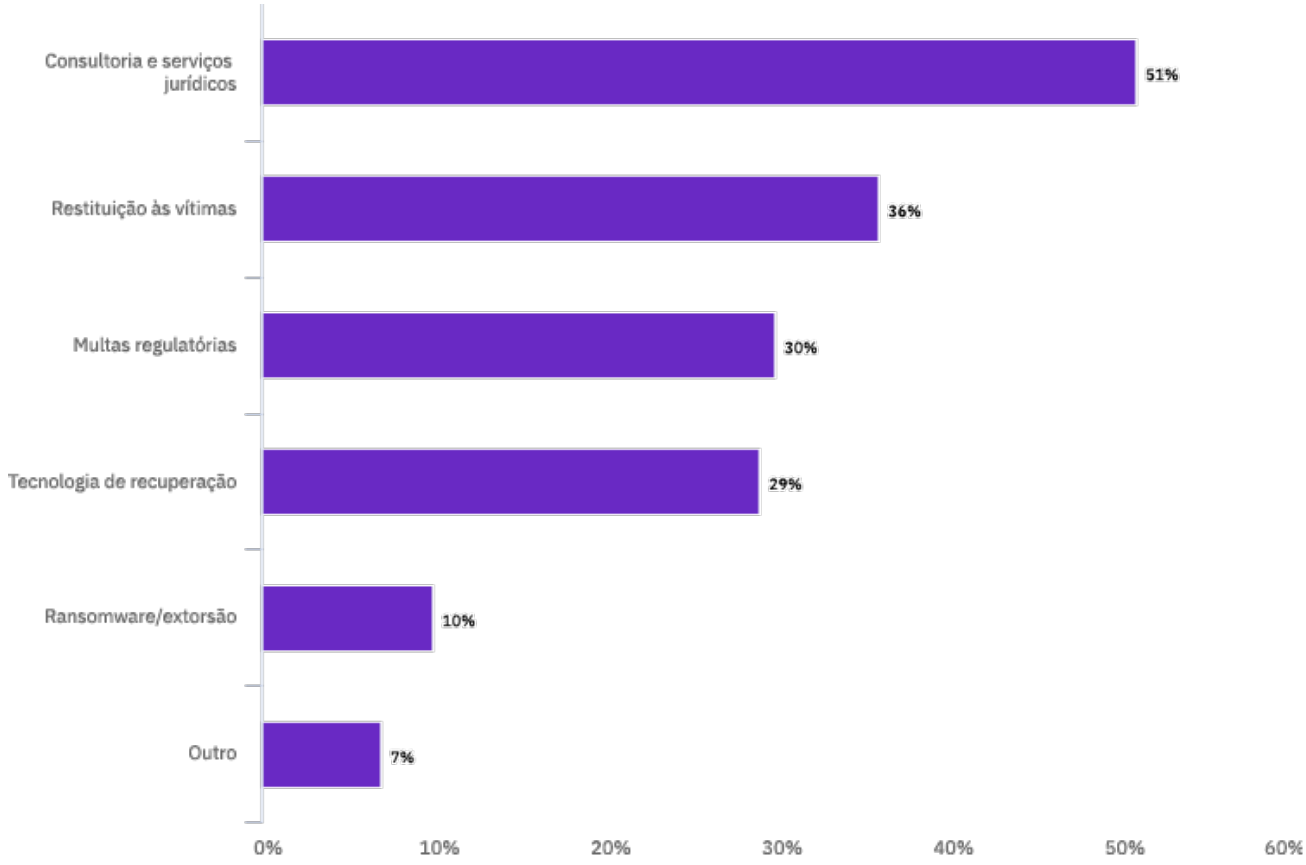
A Figura 26 mostra o impacto no prejuízo médio de 25 fatores no prejuízo total médio de um vazamento de dados de US$ 3,86 milhões. A complexidade do sistema de segurança, criada pelo número de tecnologias facilitadoras e pela falta de conhecimento interno, aumentou o prejuízo total médio de um vazamento de dados, em média, em US$ 291.870. A migração para a nuvem foi associada a prejuízos por vazamentos de dados acima da média, aumentando o prejuízo médio, em média, em US$ 267.469.

Entre os fatores que reduziram o prejuízo total médio de um vazamento de dados estavam testes extensivos do plano de resposta a incidentes e o gerenciamento da continuidade de negócios, reduzindo o prejuízo médio, em média, em US$ 295.267 e US$ 278.697, respectivamente.

Figura 27

Tipos de prejuízos recuperados com sinistros de seguros de segurança virtual

Porcentagem de respostas, mais de uma resposta permitida



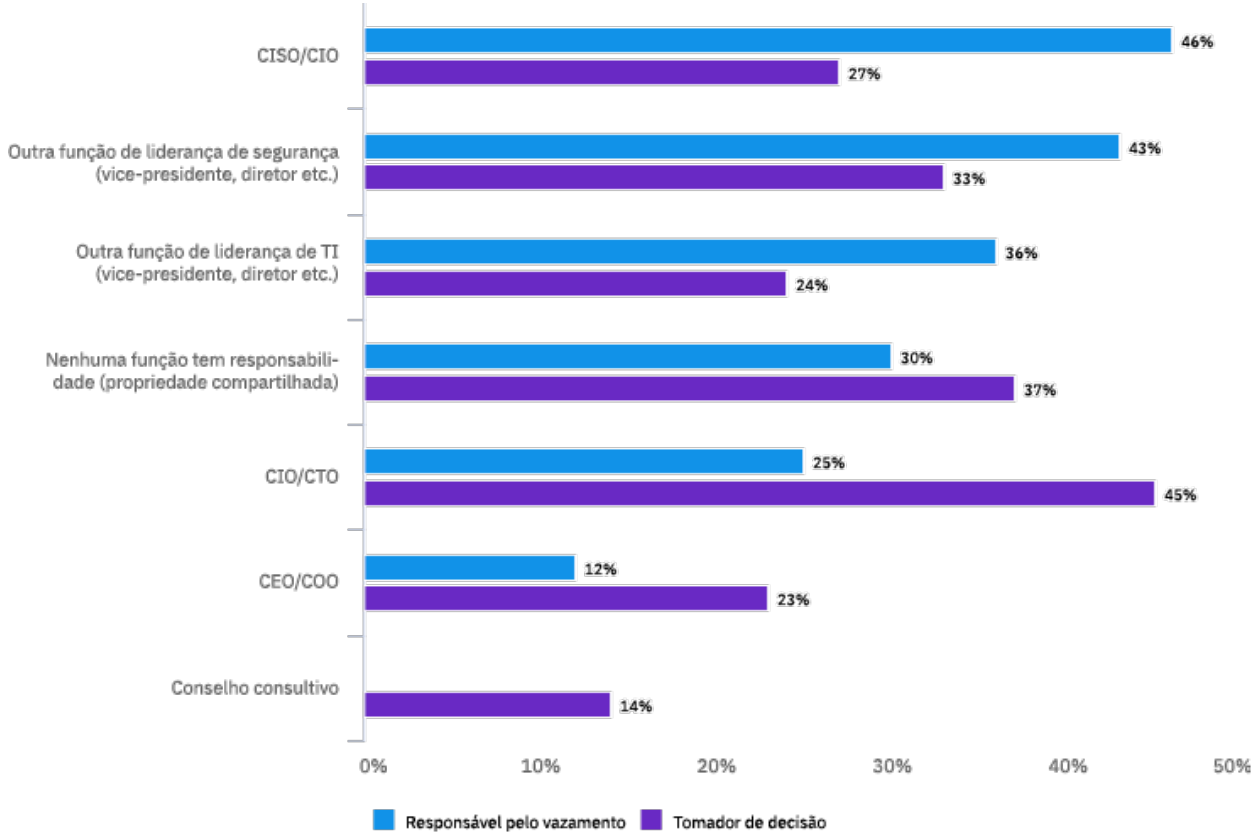
O seguro contra ataques virtuais, na maioria dos casos, cobriu o prejuízo com serviços de terceiros e a restituição das vítimas.

De acordo com a **Figura 27**, 51% das organizações com seguro contra ataques virtuais abriram sinistros para cobrir os gastos com consultoria e serviços jurídicos de terceiros. O custo da restituição das vítimas foi coberto pelo seguro contra ataques virtuais em 36% das organizações. Apenas 10% das organizações com seguro contra ataques virtuais usaram sinistros para cobrir o prejuízo causado por ransomware ou extorsão.

Figura 28

Quem é o maior responsável pela política de segurança virtual e vazamentos e pelas decisões em tecnologia?

Porcentagem de respostas, mais de uma resposta permitida



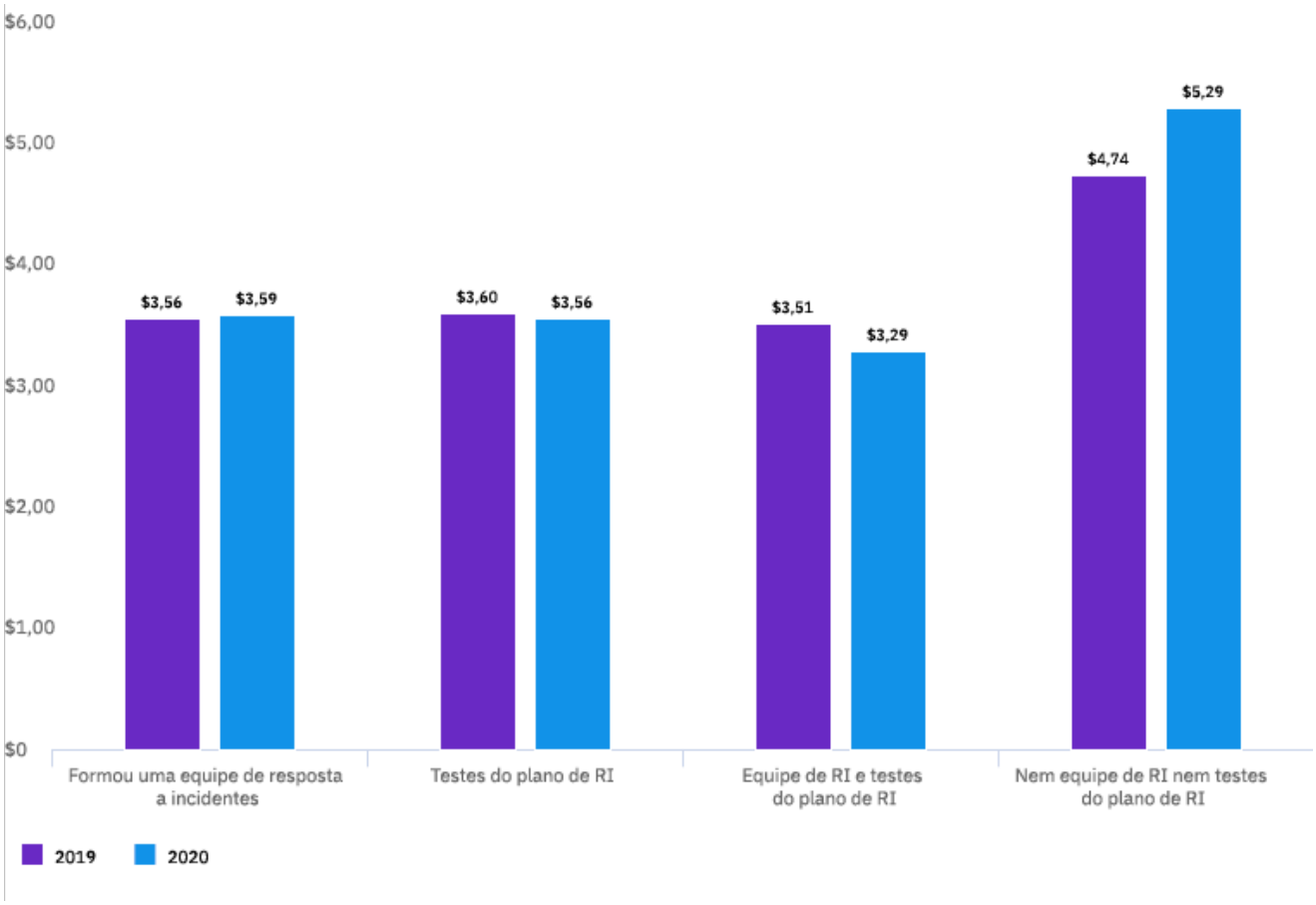
Os CISOs foram os mais responsabilizados pelo vazamento de dados.

Como mostra a **Figura 28**, 46% dos entrevistados disseram que o CISO/CSO seria responsabilizado por um vazamento de dados, mas apenas 27% disseram que o CISO/CSO foi o maior responsável pela política de segurança virtual e pela tomada de decisões em tecnologia. Os CEOs e COOs foram os menos responsabilizados por um vazamento de dados, enquanto a função de CIO/CTO foi mais frequentemente considerada a principal tomadora de decisões das políticas e tecnologias de segurança virtual.

Figura 29

Prejuízo total médio de um vazamento de dados com equipe de resposta a incidentes e testes do plano de RI

Medido em milhões de dólares (US$)



As equipes de resposta a incidentes, combinadas com testes do plano de resposta a incidentes, reduziram bastante o prejuízo de um vazamento de dados.

Como mostra a **Figura 29,** as organizações que formaram uma equipe de resposta a incidentes e testaram extensivamente um plano de resposta a incidentes tiveram um prejuízo médio de vazamento de dados de US$ 3,29 milhões. Por outro lado, as organizações que não adotaram nenhuma dessas etapas tiveram um prejuízo total médio de US$ 5,29 milhões, uma diferença de US$ 2 milhões.

Tendências e eficácia da automação da segurança

Este foi o terceiro ano em que examinamos a relação entre o prejuízo de um vazamento de dados e a automação da segurança. Neste contexto, a automação da segurança se refere à implantação de tecnologias de segurança que aumentam ou substituem a intervenção humana na identificação e na contenção de invasões ou vazamentos virtuais. Elas dependem de inteligência artificial, aprendizado de máquina, análise e orquestração automatizada.

Principais conclusões

21%

Parcela de organizações em 2020 com automação da segurança totalmente implantada, aumento em relação aos 15% em 2018

US$ 3,58 milhões

Diferença no prejuízo total médio de um vazamento de dados para organizações sem automação da segurança em relação àquelas com automação totalmente implantada

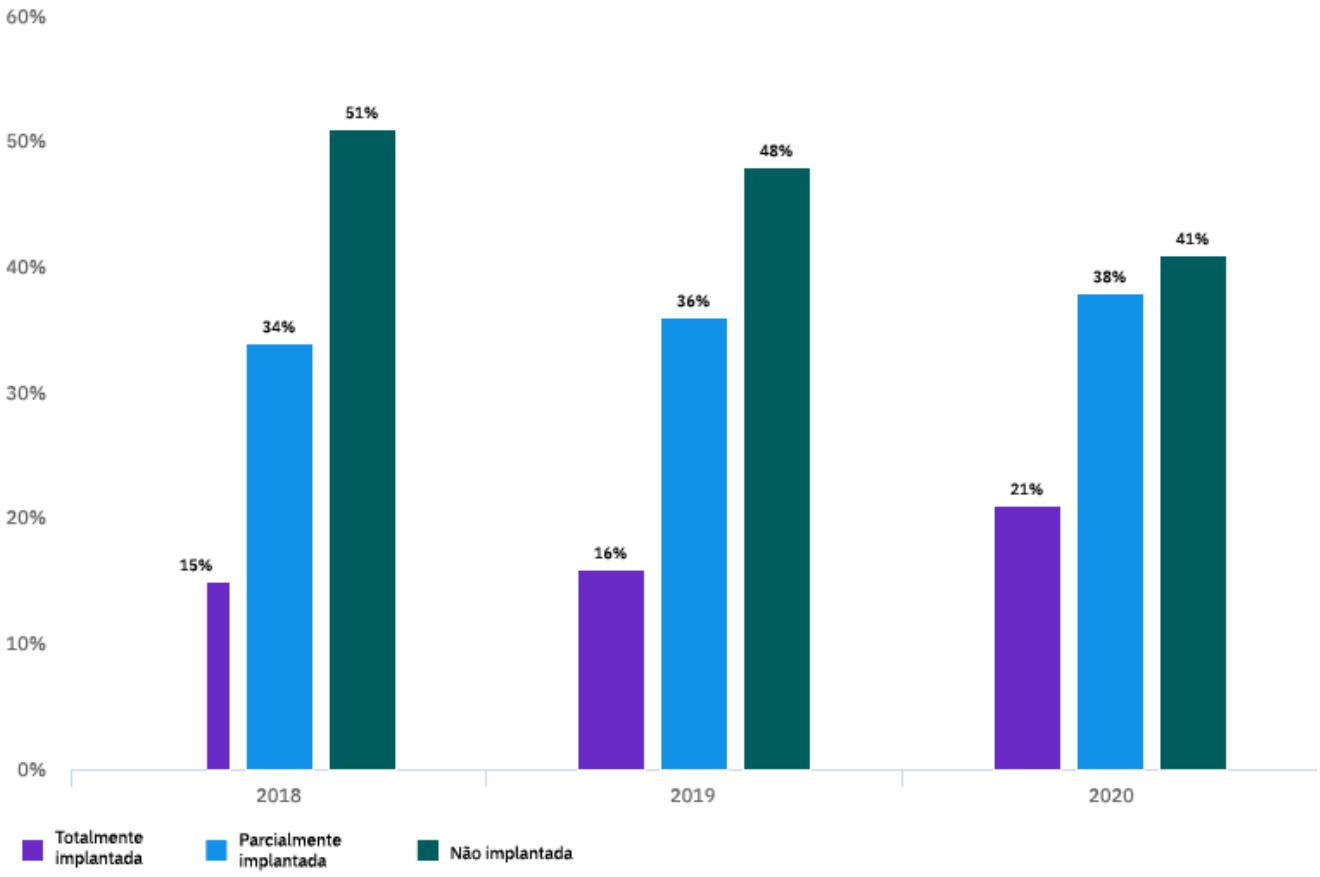
30%

Parcela de organizações na Alemanha com automação da segurança totalmente implantada, a maior em relação aos outros países/regiões

Figura 30

Cenário da automação da segurança comparando três níveis de implantação

Porcentagem de organizações por nível de automação



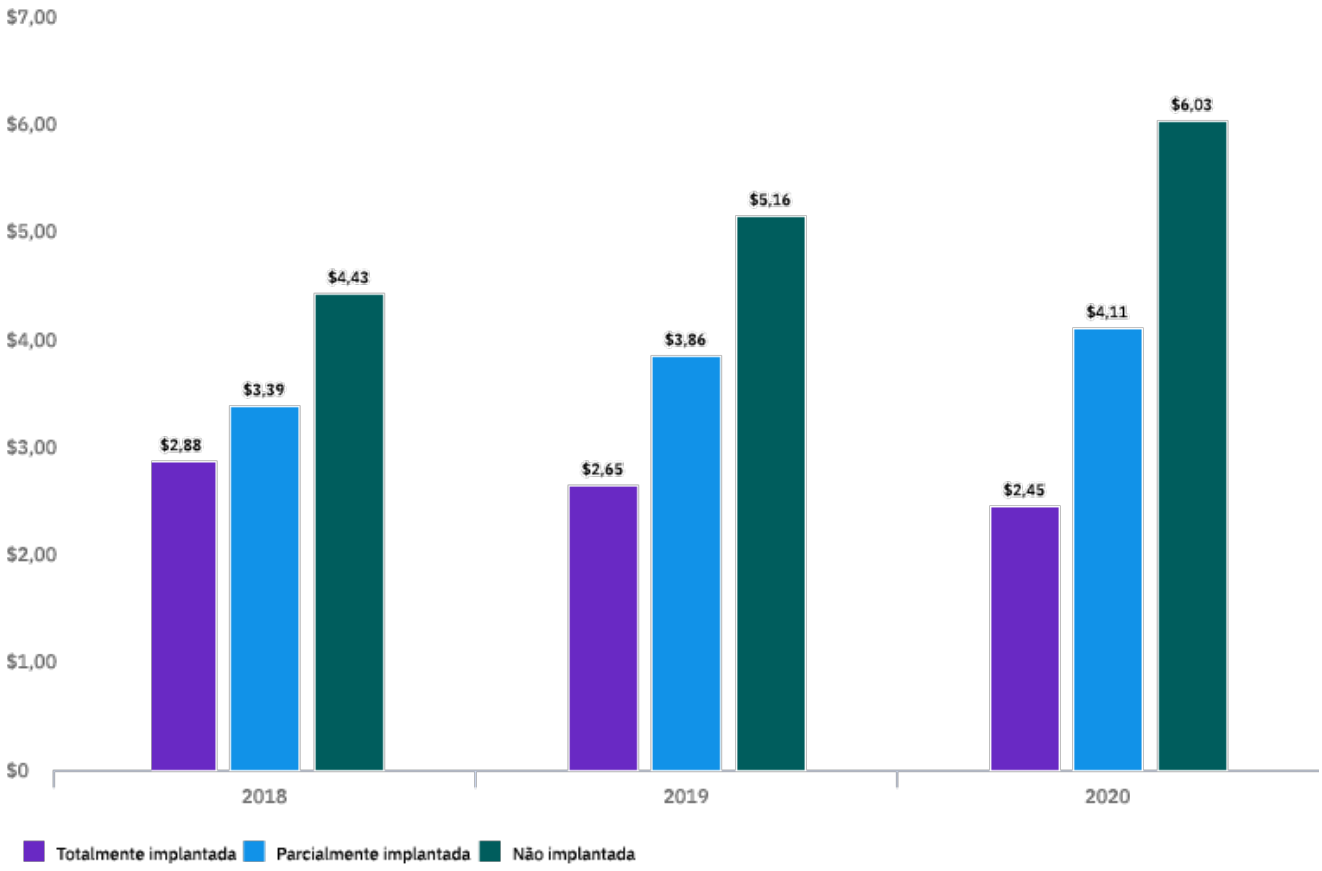
A implantação completa da automação aumentou nos últimos três anos.

Como mostra a **Figura 30**, apenas 21% das empresas informaram que implantaram completamente a automação da segurança no estudo de 2020, mas houve um aumento em relação aos 15% de 2018 e aos 16% de 2019. No estudo de 2020, outros 38% informaram que implantaram parcialmente a automação, e 41% informaram que a automação não foi implantada.

Figura 31

Prejuízo total médio de um vazamento de dados por nível de implantação da automação da segurança

Medido em milhões de dólares (US$)



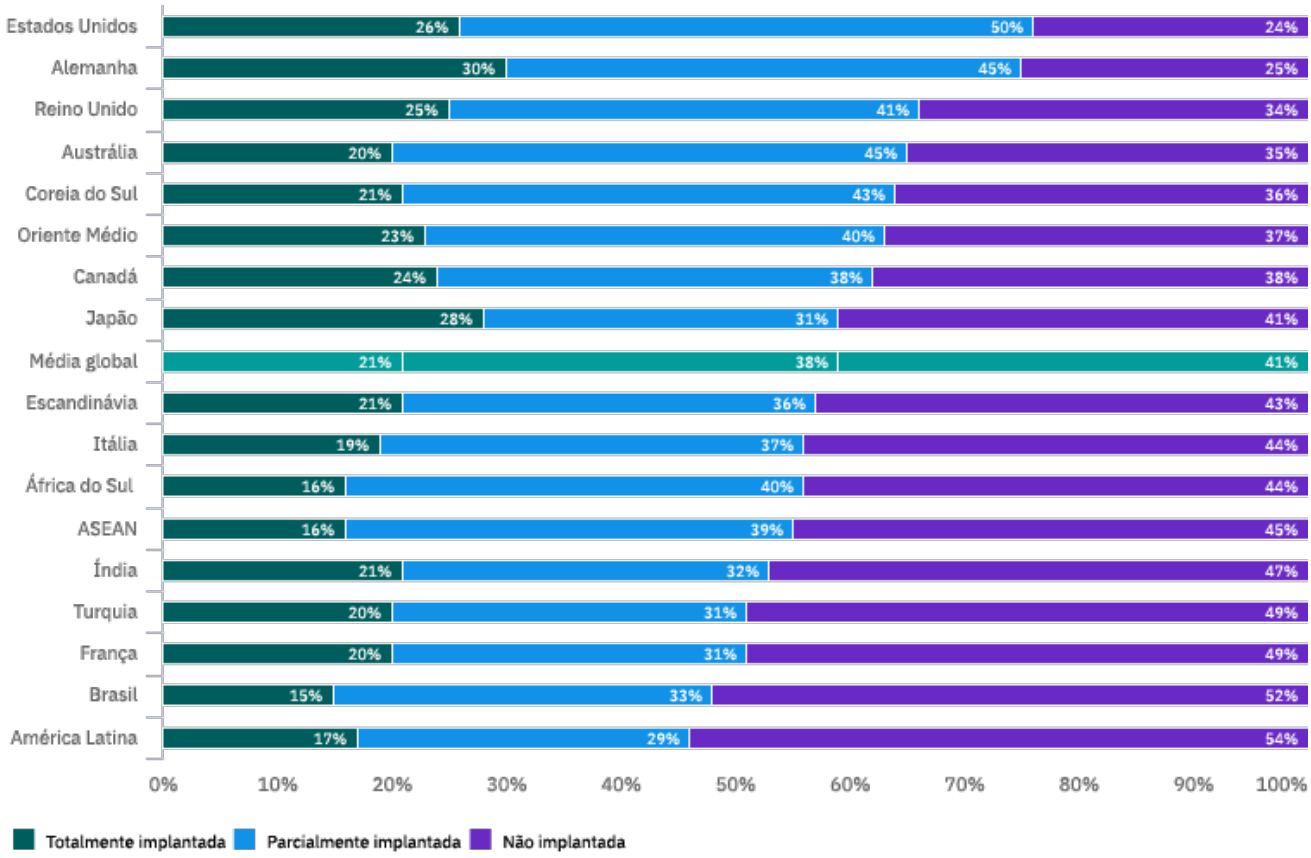
O impacto da automação da segurança no prejuízo de um vazamento de dados aumentou nos últimos três anos.

Como mostra a **Figura 31**, o prejuízo total médio do vazamento de dados foi de US$ 2,45 milhões para as organizações no estudo de 2020 que implantaram totalmente a automação da segurança, US$ 3,58 milhões a menos do que o prejuízo médio das organizações sem a automação da segurança implantada. No estudo de 2018, a diferença entre o prejuízo médio de um vazamento em organizações com automação totalmente implantada e sem automação implantada foi de US$ 1,55 milhão e, em 2019, essa diferença foi de US$ 2,51 milhões.

Figura 32

Média de implantação de automação da segurança por país

Porcentagem de organizações em três níveis de automação



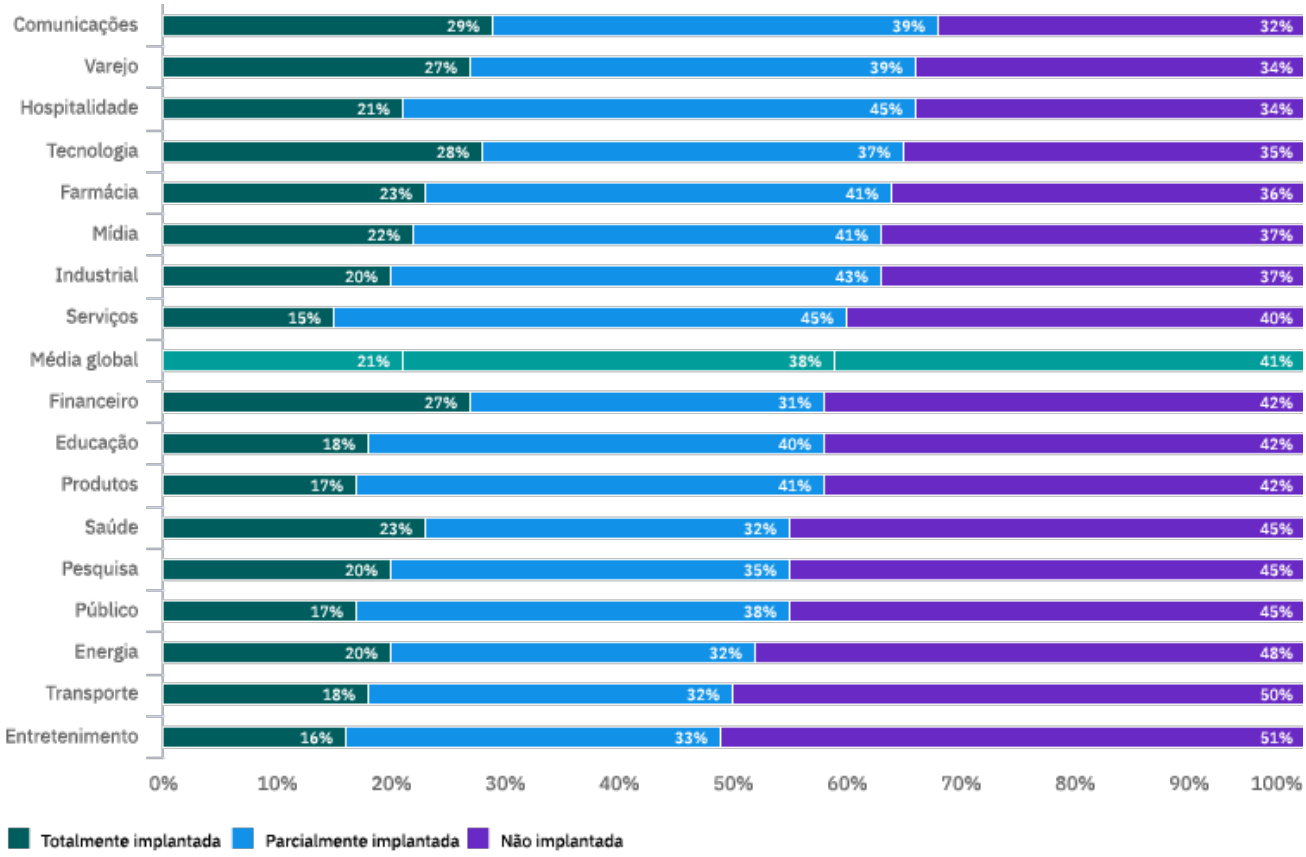
O cenário de automação da segurança variou entre países e regiões.

De acordo com a **Figura 32**, os Estados Unidos e a Alemanha tiveram percentuais mais altos de organizações com automação total ou parcialmente implantada (76% nos Estados Unidos e 75% na Alemanha). A automação da segurança totalmente implantada foi de 26% nos Estados Unidos e 30% na Alemanha. A América Latina e o Brasil tiveram os maiores percentuais de organizações sem automação implantada (54% e 52%, respectivamente).

Figura 33

Nível médio de implantação de automação da segurança por setor

Porcentagem de organizações em três níveis de automação



O nível de automação da segurança implantado varia de acordo com o setor.

Como mostra a **Figura 33**, os setores de comunicação, tecnologia e varejo tiveram as maiores porcentagens de organizações com automação total ou parcialmente implantada. As organizações financeiras tiveram uma parcela acima da média de organizações com automação da segurança totalmente implantada (27%). Mas sua parcela relativamente baixa de organizações com implantação parcial da automação (31%) significa que a parcela combinada do setor financeiro de automação total e parcialmente implantada ficou abaixo da média global (58% vs. a média global de 59%). Entretenimento e transporte tiveram as maiores porcentagens de organizações que não implantaram a automação.

Tempo para identificar e conter um vazamento de dados

Em anos anteriores, esta pesquisa mostrou que quanto mais rapidamente o vazamento de dados for identificado e contido, menor será o prejuízo. O tempo médio de identificação descreve o tempo necessário para detectar que um incidente ocorreu. O tempo para conter refere-se ao tempo que leva para uma organização resolver uma situação depois que ela foi detectada e, finalmente, restaurar o serviço.

O tempo decorrido entre a detecção do vazamento e sua contenção é chamado de ciclo de vida do vazamento de dados. Essas métricas podem ser usadas para determinar a eficácia dos processos de resposta a incidentes e de contenção de uma organização. Pela primeira vez, o estudo deste ano examinou o impacto da automação da segurança na direção do ciclo de vida do vazamento de dados.

Principais conclusões

280 dias

Tempo médio para detectar e conter um vazamento de dados

315 dias

Tempo médio para detectar e conter um vazamento de dados causado por um ataque mal-intencionado

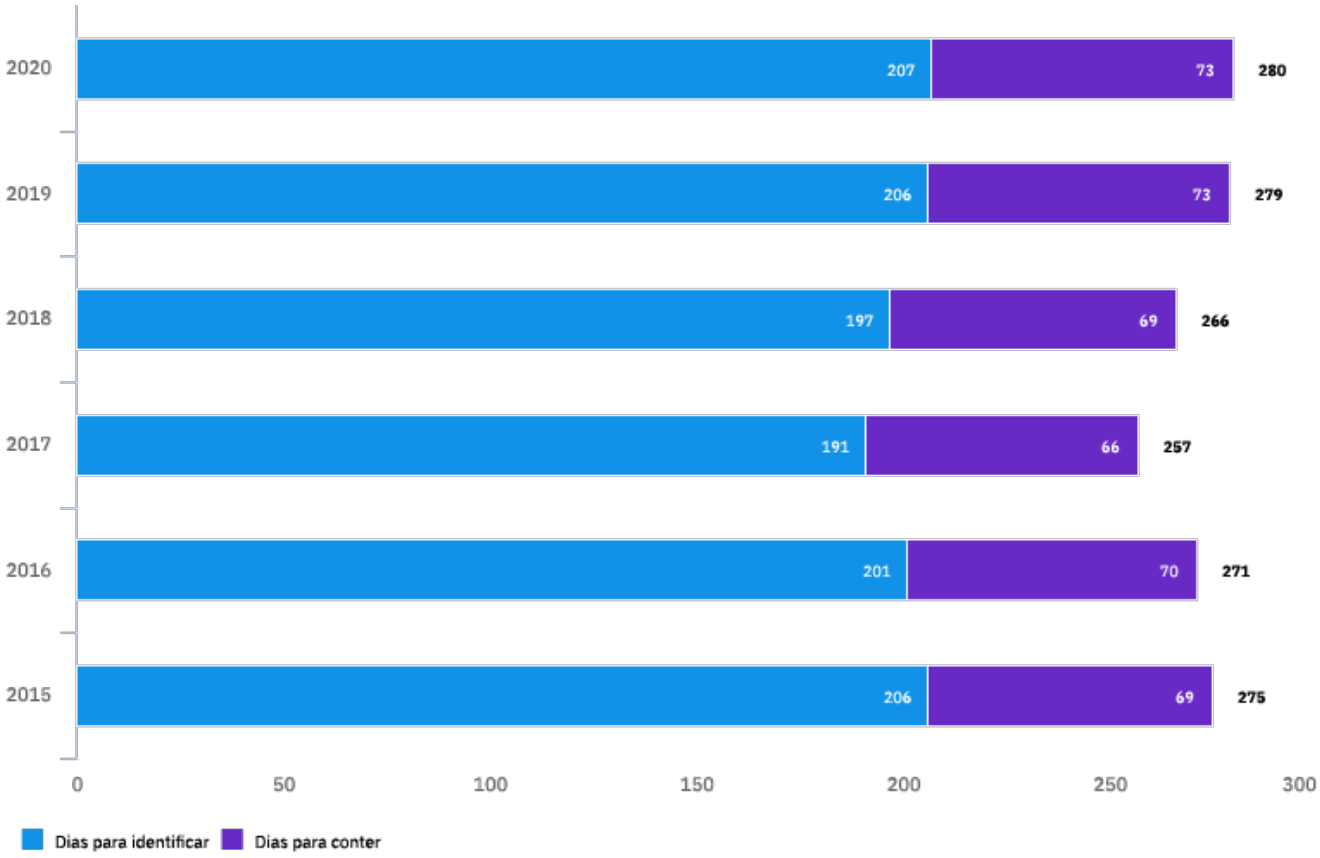
US$ 1,12 milhão

Economia média por conter um vazamento em menos de 200 dias vs. mais de 200 dias

Figura 34

Tempo médio para identificar e conter um vazamento de dados

Medido em dias



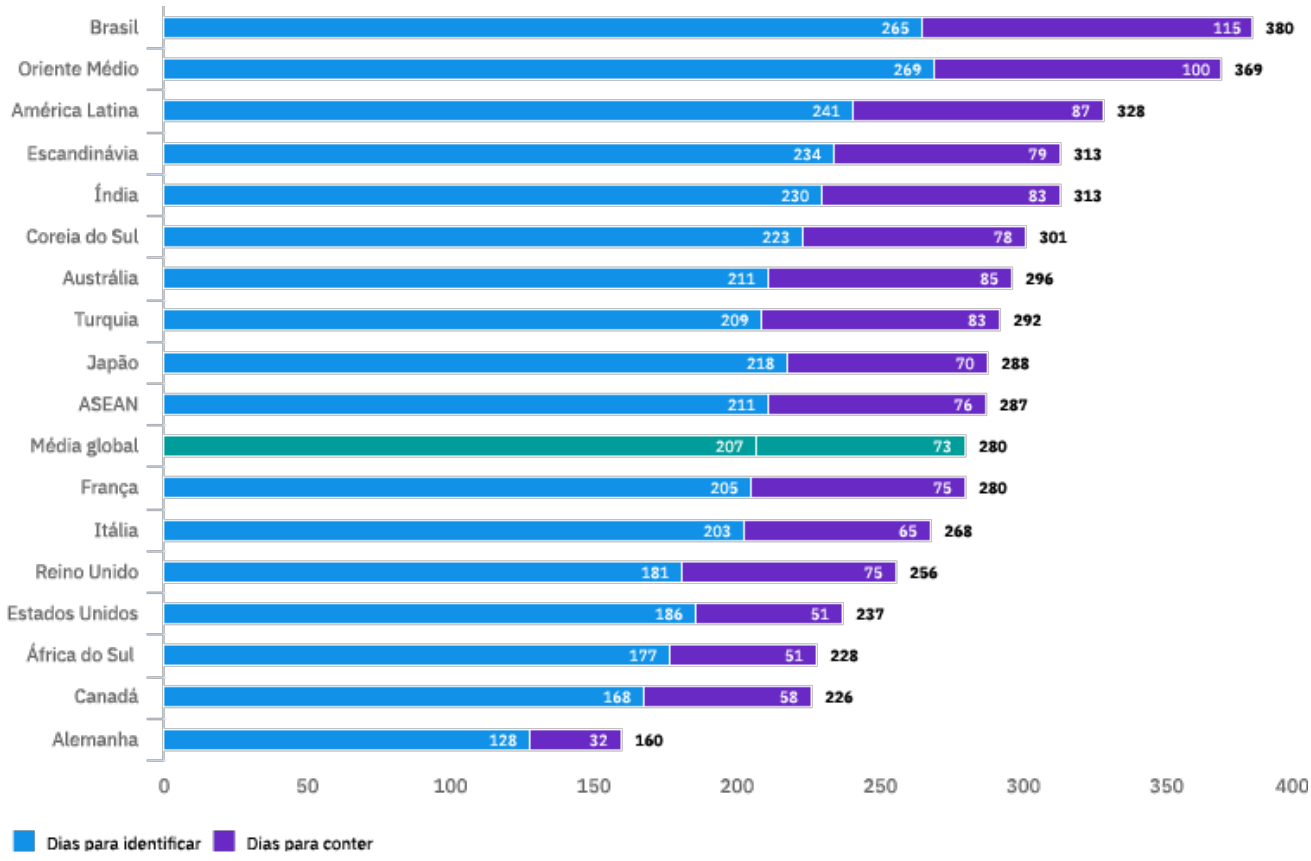
O tempo médio para identificar e conter um vazamento permaneceu consistente.

Como mostra a **Figura 34**, o tempo para identificar e o tempo para conter um vazamento de dados não variaram muito nos últimos relatórios. No estudo de 2020, o tempo médio de identificação foi de 207 dias, e o tempo médio de contenção foi de 73 dias, somando 280 dias. Em 2019, o ciclo de vida combinado do vazamento de dados foi de 279 dias.

Figura 35

Tempo médio para identificar e conter um vazamento de dados por país ou região

Medido em dias



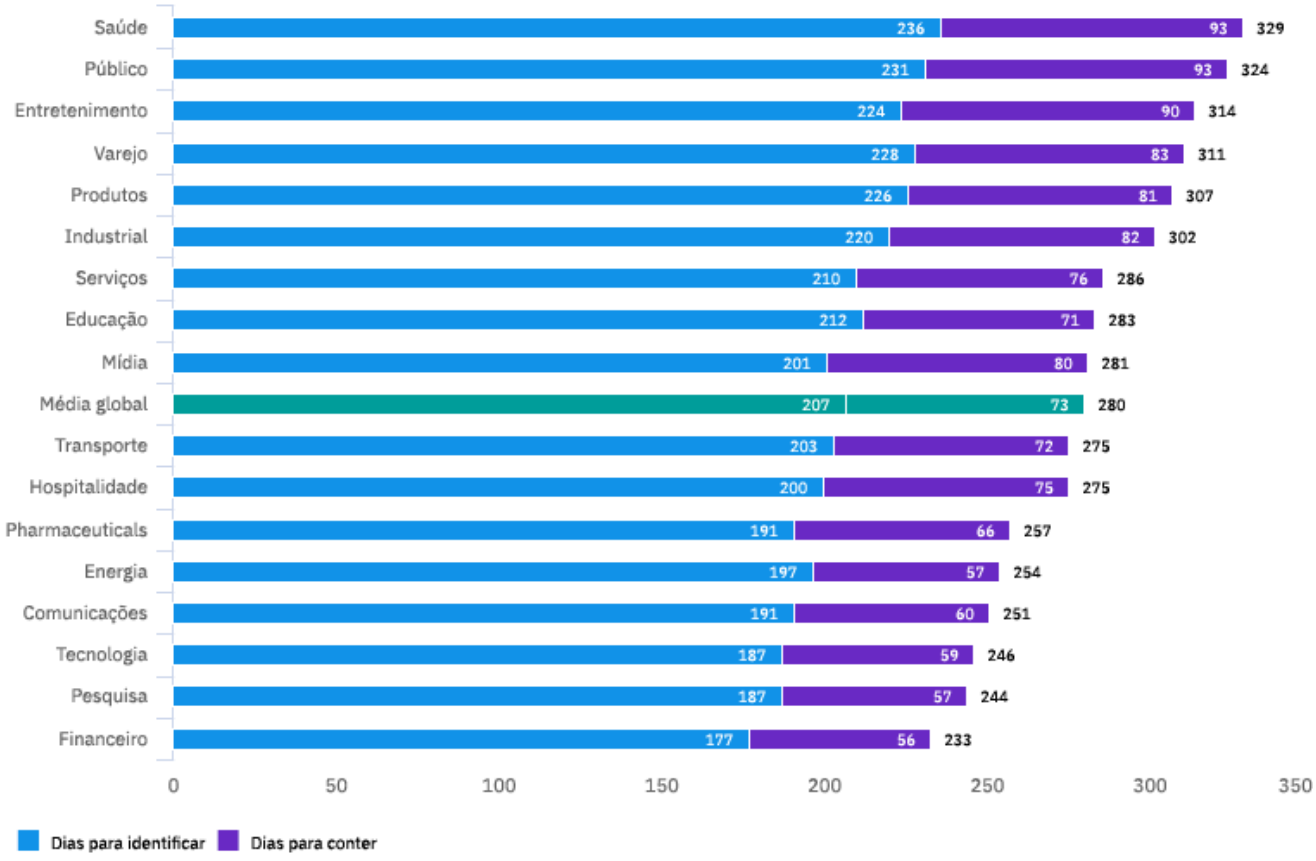
As diferenças entre países/regiões no ciclo de vida médio dos vazamentos foram significativas.

De acordo com a **Figura 35**, o Brasil e o Oriente Médio demoraram muito mais que a média para identificar e conter um vazamento de dados, com média de 380 e 369 dias, respectivamente. A África do Sul, o Canadá e a Alemanha tiveram um ciclo de vida de vazamento de dados muito mais curto, com as organizações na Alemanha levando uma média de apenas 160 dias para conter o vazamento.

Figura 36

Tempo médio para identificar e conter um vazamento de dados por setor

Medido em dias



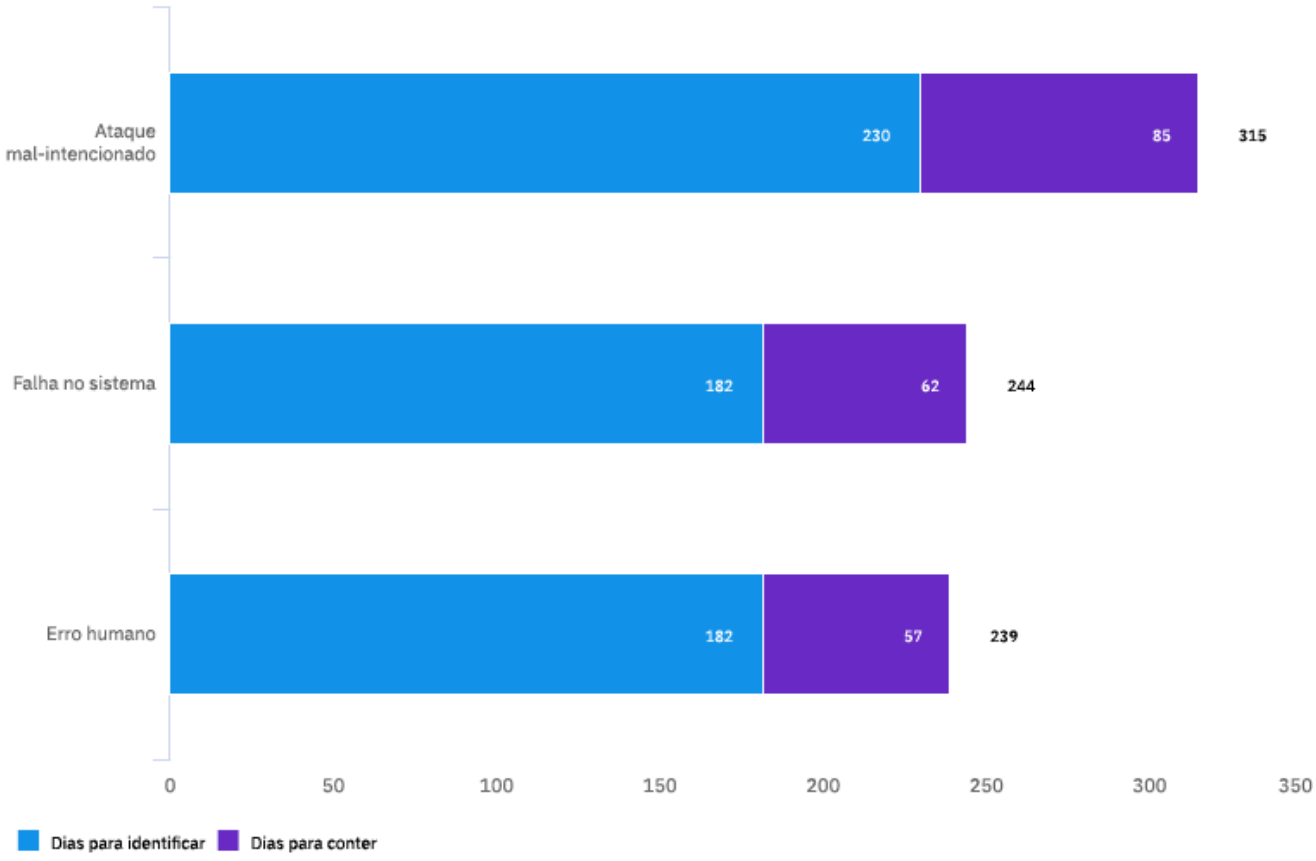
Os setores financeiro e de saúde tiveram tempos para conter um vazamento bastante distantes.

Como mostra a **Figura 36**, o setor de saúde teve o tempo médio mais alto para identificar e conter um vazamento, com 329 dias. O financeiro teve o menor tempo médio para identificar e conter um vazamento, com 233 dias. Nove setores ficaram acima e oito ficaram abaixo do ciclo de vida médio global dos vazamento, de 280 dias.

Figura 37

Tempo médio para identificar e conter um vazamento de dados por causa principal

Medido em dias



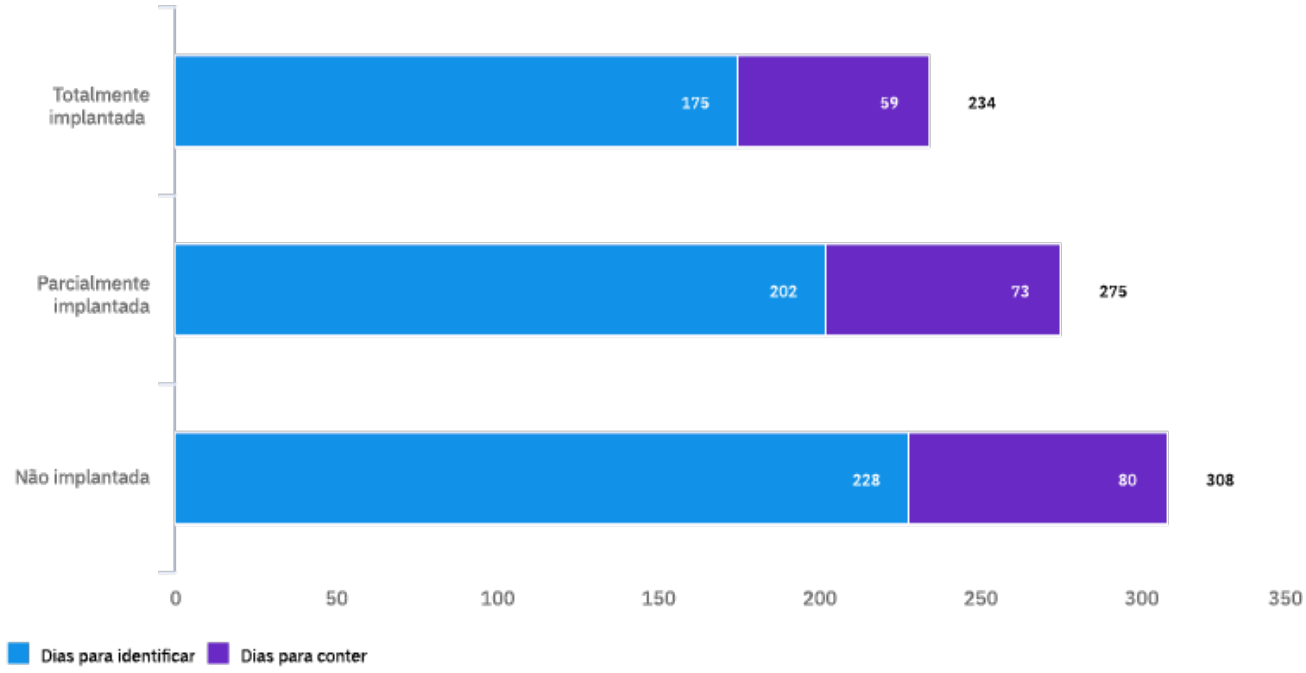
Os vazamentos causados por ataques mal-intencionados levaram mais tempo para serem identificados e contidos.

No estudo de 2020, os vazamentos mal-intencionados levaram, em média, 315 dias para serem identificados e contidos, em comparação com os vazamentos por outras causas, como mostra a **Figura 37**. Demorou, em média, 244 dias para identificar e conter um vazamento por falha no sistema, e 239 dias para identificar e conter um vazamento causado por erro humano. Os vazamentos mal-intencionados levaram 23 dias a mais para serem identificados do que os vazamentos de dados comuns. Em média, foram necessários 230 dias para identificar um vazamento mal-intencionado, em comparação com a média geral de 207 dias.

Figura 38

Tempo médio para identificar e conter um vazamento de dados por nível de segurança da automação

Medido em dias



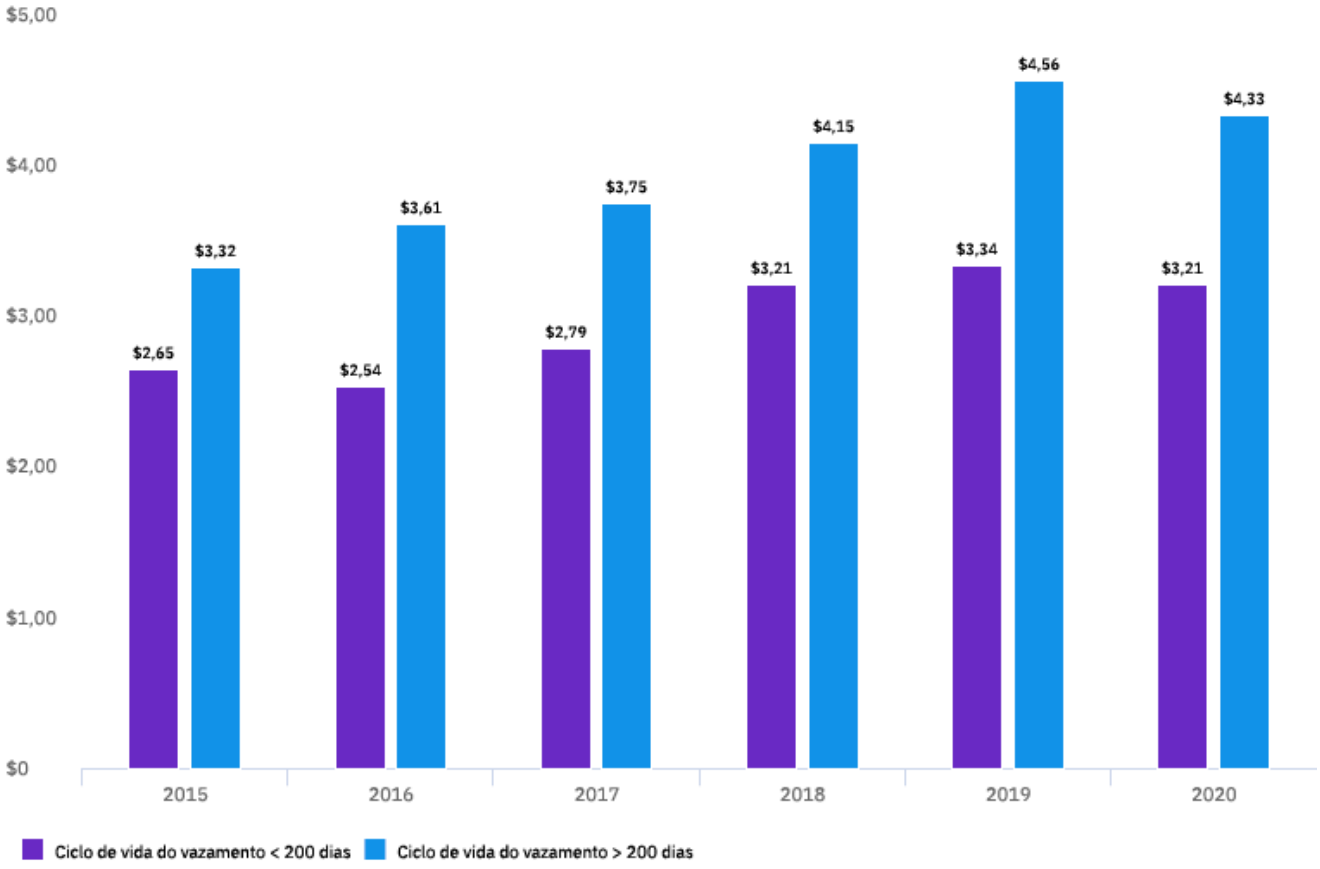
A automação da segurança reduziu o tempo necessário para identificar e conter um vazamento de dados.

Pela primeira vez, este estudo examinou o impacto da automação no ciclo de vida do vazamento de dados. **A Figura 38** mostra que, quando a automação foi totalmente implantada, em média, o tempo de identificação foi de 175 dias, e o tempo de contenção, 59 dias. Sem automação, o tempo aumentou significativamente para, em média, 228 dias para identificar e 80 dias para conter um vazamento, totalizando 308 dias.

Figura 39

Prejuízo total médio de um vazamento de dados com base no ciclo de vida médio do vazamento de dados

Medido em milhões de dólares (US$)



O ciclo de vida do vazamento de dados influenciou o prejuízo médio de um vazamento.

Nos últimos seis anos, a pesquisa foi consistente em mostrar que os vazamentos com ciclo de vida (tempo para identificar somado ao tempo para conter um vazamento) de mais de 200 dias tiveram um prejuízo muito maior do que aqueles com um ciclo de vida com menos de 200 dias. Como mostra a **Figura 39**, no estudo de 2020, os vazamentos com um ciclo de vida superior a 200 dias custaram, em média, US$ 1,12 milhão a mais do que aqueles com um ciclo de vida inferior a 200 dias (US$ 4,33 milhões para mais de 200 dias vs. US$ 3,21 milhões para menos de 200 dias).

Prejuízo duradouro de um vazamento de dados

As consequências do prejuízo de um vazamento de dados podem continuar nos anos seguintes ao evento. No estudo do ano passado, examinamos primeiro como as organizações podem ser impactadas pelo prejuízo do vazamento de dados em um período de dois ou mais anos. A análise mostrou que o prejuízo foi mais alto no primeiro ano após o vazamento, mas com tendência a subir novamente após dois anos.

Em seguida, analisamos a diferença entre esses "prejuízos duradouros" em vazamentos em organizações de setores altamente regulados em comparação com aquelas de setores com normas de proteção de dados menos rigorosas. Consideramos setores altamente regulados os de energia, saúde, produtos, financeiro, tecnologia, farmácia, comunicação, público e educação. As organizações dos setores de varejo, industrial, entretenimento, mídia, serviços de pesquisa e hospitalidade foram consideradas pouco reguladas. Na análise de setores nas categorias de alta vs. baixa regulação, concluímos que os gastos com serviços regulatórios e jurídicos podem ter contribuído para o aumento do prejuízo nos anos seguintes a um vazamento

No estudo de 2020, examinamos uma amostra de 101 empresas que registraram dois ou mais anos de prejuízo de um vazamento de dados.

Principais conclusões

61%

Parcela média do prejuízo de um vazamento de dados incorrido no primeiro ano

44%

Parcela média do prejuízo de um vazamento de dados incorrido no primeiro ano em setores altamente regulados

92%

Parcela média do prejuízo de um vazamento de dados incorrido nos primeiros dois anos em setores menos regulados

Figura 40

Distribuição média dos prejuízos de um vazamento de dados em mais de dois anos

Porcentagem de prejuízo acumulado em intervalos de três meses

	2019	2020
Tempo decorrido	Porcentagem do prejuízo total	
1º ano	67%	61%
2º ano	22%	24%
Mais de 2 anos	11%	15%

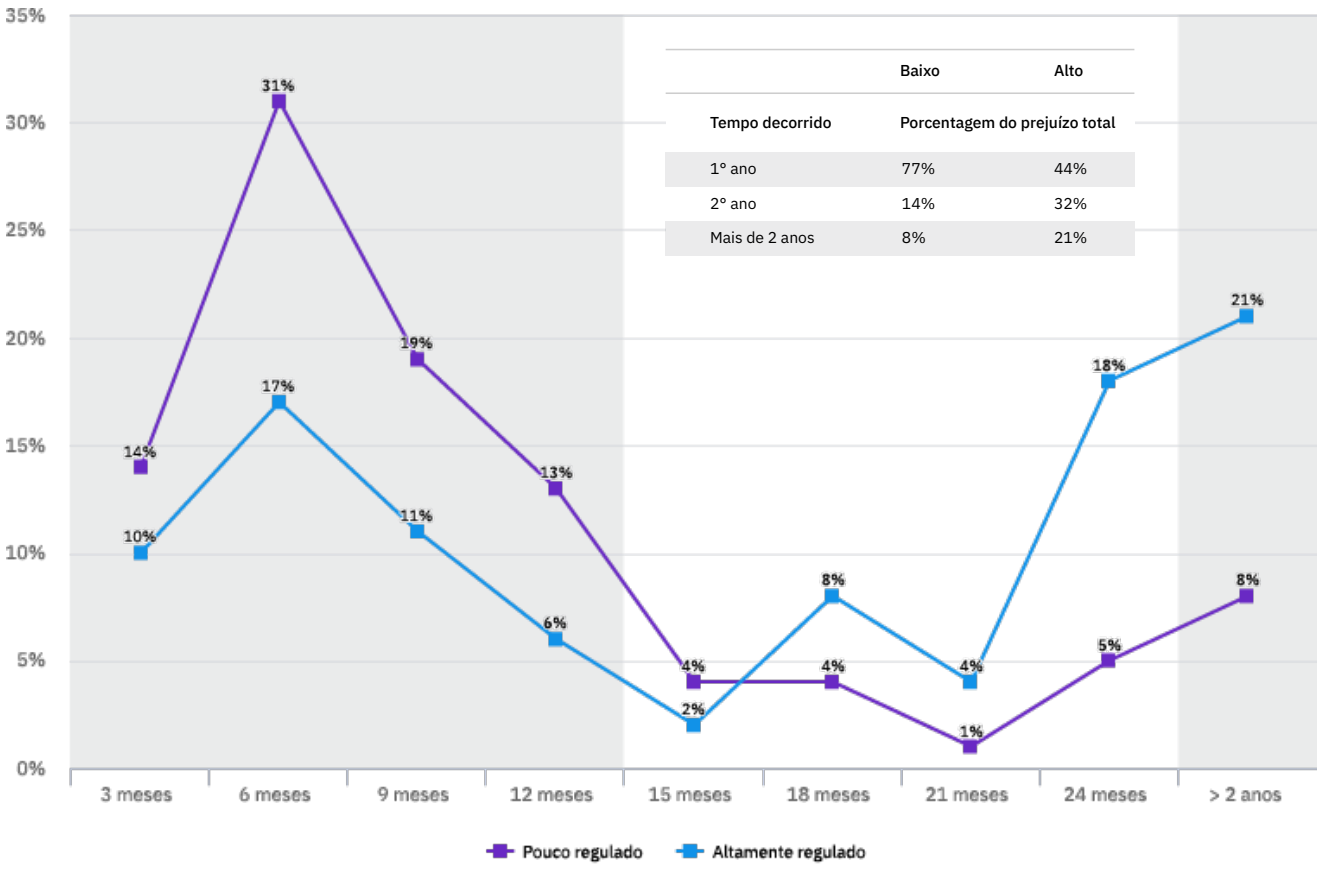
A parcela de prejuízos de vazamentos incorridos após dois anos aumentou no estudo de 2020.

De acordo com a **Figura 40**, a análise de prejuízo duradouro constatou que, em média, 61% do prejuízo de um vazamento de dados incorreu durante o primeiro ano, 24% durante o segundo ano e 15% após dois anos. Esse foi um pequeno aumento no prejuízo mais de dois anos após o vazamento, em comparação com 11% na análise de 2019.

Figura 41

Distribuição média dos prejuízos de um vazamento de dados ao longo do tempo em ambientes altamente vs. pouco regulados

Porcentagem do prejuízo total acumulado em intervalos de três meses



	Baixo	Alto
Tempo decorrido	Porcentagem do prejuízo total	
1º ano	77%	44%
2º ano	14%	32%
Mais de 2 anos	8%	21%

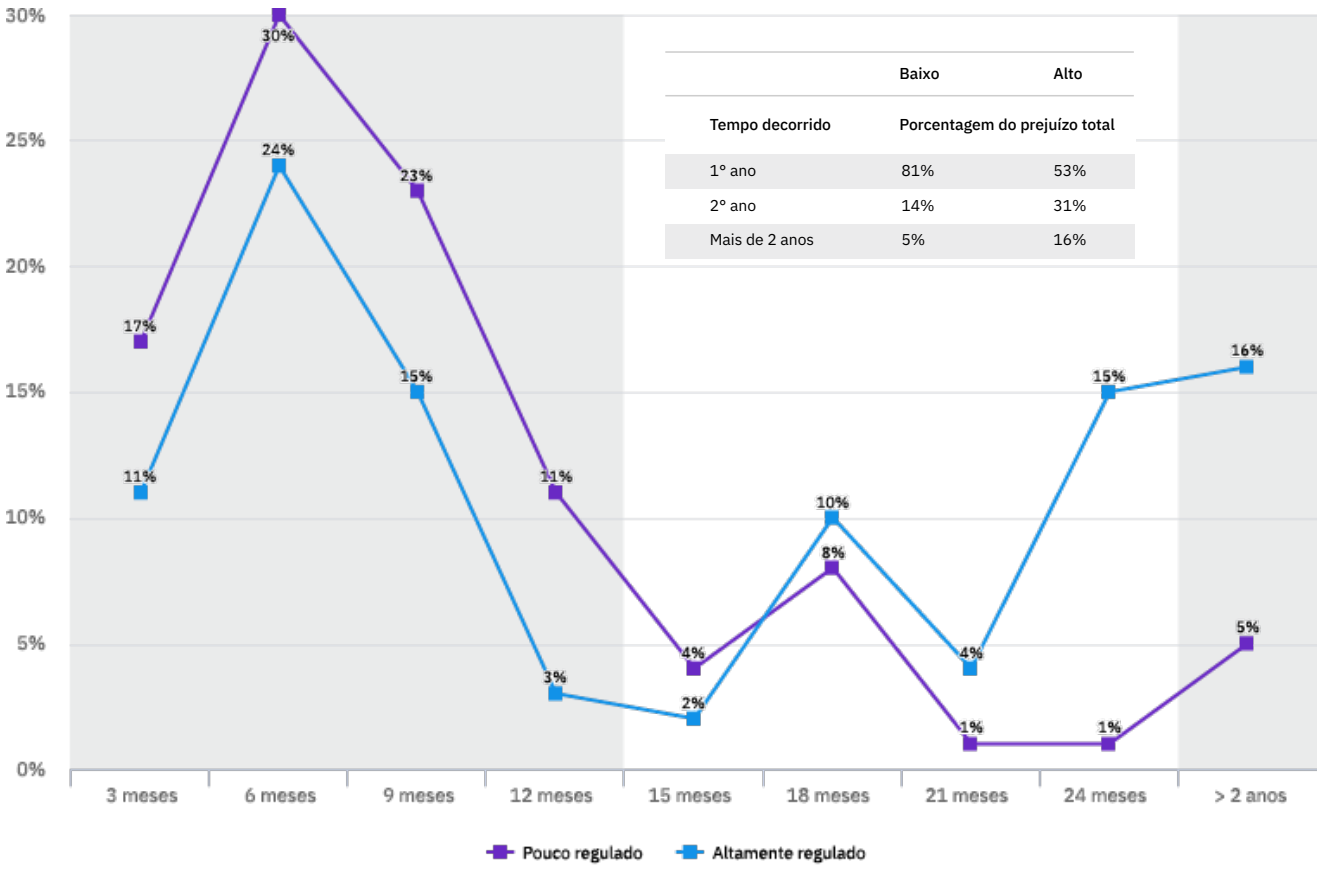
Os vazamentos em setores altamente regulados causaram o maior prejuízo após o primeiro ano.

De acordo com a **Figura 41**, as organizações em ambientes pouco regulados tiveram muito mais chance de perceber o prejuízo total do vazamento de dados durante o primeiro ano. Em setores menos regulados, houve uma média de 77% dos prejuízos durante o primeiro ano, em comparação com uma média de 44% dos prejuízos durante o primeiro ano para vazamentos em organizações altamente reguladas.

Figura 42

Distribuição média dos prejuízos de um vazamento de dados ao longo do tempo em ambientes altamente vs. pouco regulados no relatório de 2019

Porcentagem do prejuízo total acumulado em intervalos de três meses



	Baixo	Alto
Tempo decorrido	Porcentagem do prejuízo total	
1º ano	81%	53%
2º ano	14%	31%
Mais de 2 anos	5%	16%

A análise de 2019 de ambientes com alta vs. baixa regulação mostrou que uma menor proporção do prejuízo ocorreu mais de dois anos após um vazamento.

A Figura 42 mostra o prejuízo duradouro de um vazamento em ambientes regulados de baixa vs. alta proteção de dados no estudo de 2019. No estudo de 2019, uma média de 16% dos prejuízos em setores altamente regulados incorreram após dois anos. Isso se compara a 21% dos prejuízos incorridos após dois anos em setores altamente regulados no estudo de 2020 (Figura 41).

Possíveis impactos da COVID-19

A pandemia de COVID-19 teve um enorme impacto na forma como muitas organizações fazem negócios, com um grande número de pessoas trabalhando em casa e uma crescente demanda por videoconferências, aplicativos em nuvem e recursos de rede. Para entender essa nova realidade, adicionamos várias perguntas à pesquisa para reunir as opiniões dos participantes do estudo sobre os possíveis impactos da COVID-19 no prejuízo de um vazamento de dados.

Principais conclusões

54%

Parcela de organizações que exigiram trabalho remoto em resposta à COVID-19

76%

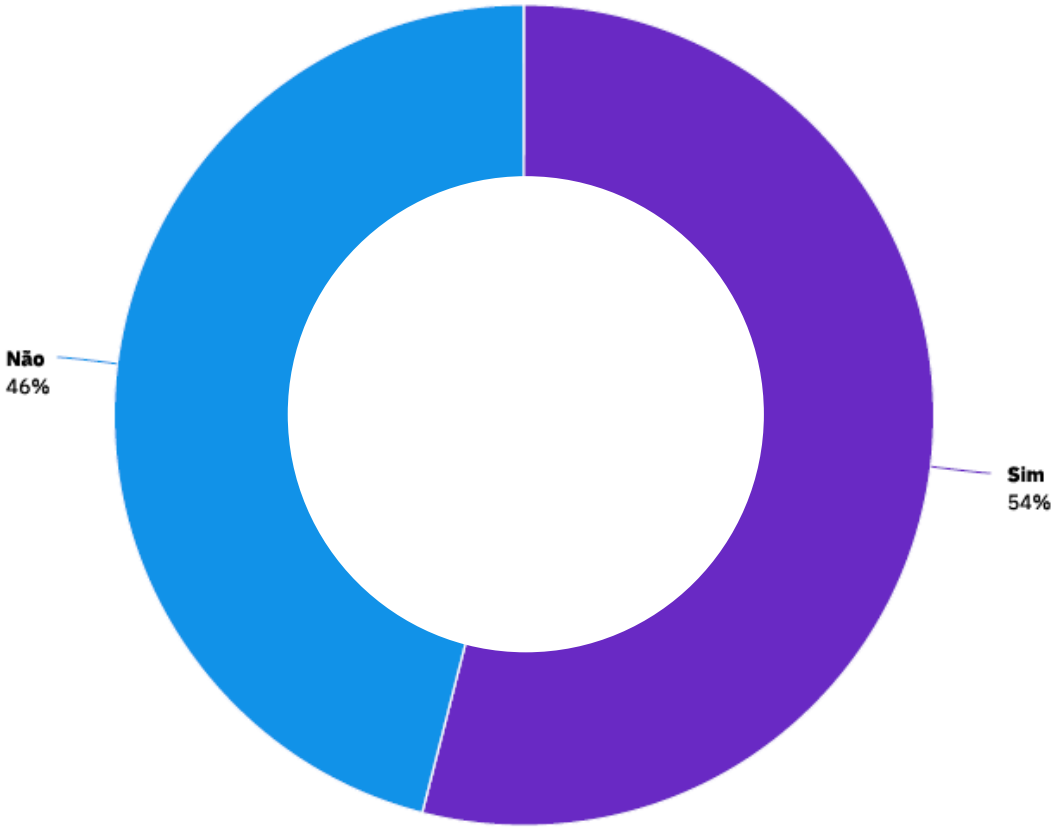
Parcela de participantes que disse que o trabalho remoto aumentaria o tempo para identificar e conter um vazamento de dados

70%

Parcela de participantes que disse que o trabalho remoto aumentaria o prejuízo de um vazamento de dados

Figura 43

Sua organização exigiu que os funcionários trabalhassem remotamente em resposta à COVID-19?

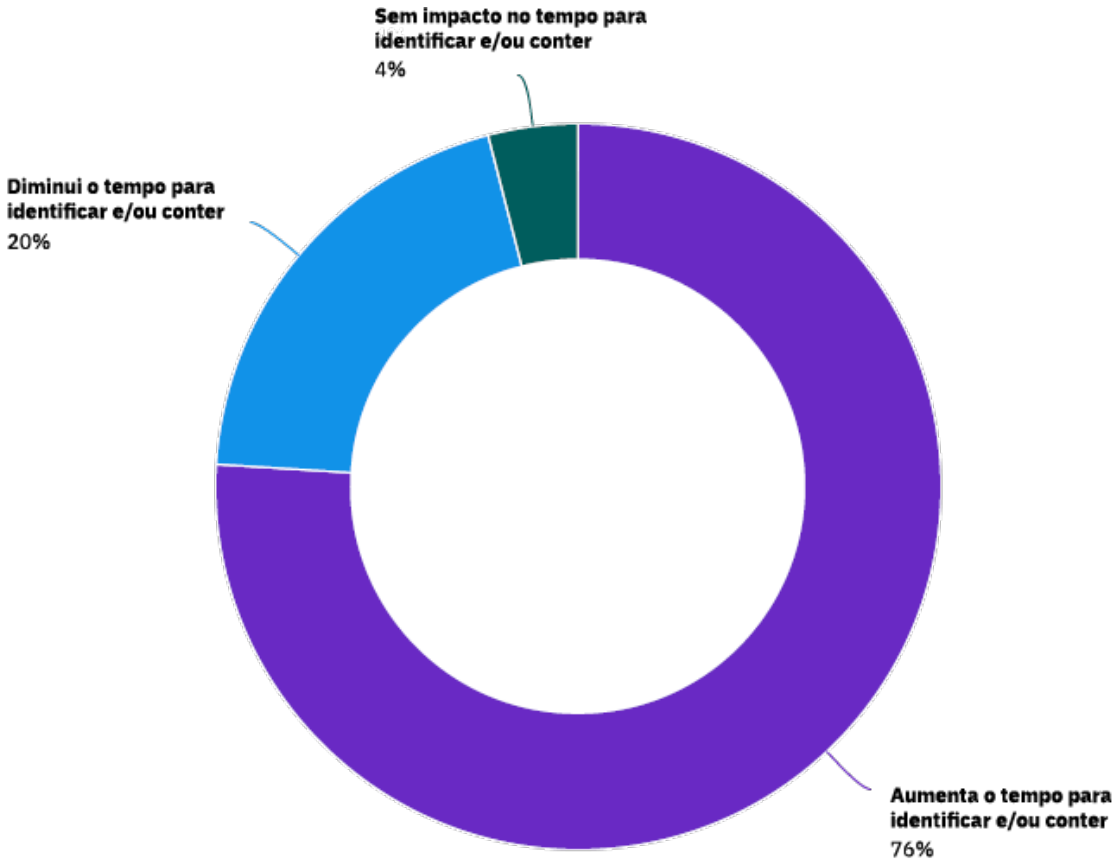


A maioria das organizações exigiu trabalho remoto em resposta à COVID-19.

Como mostra a **Figura 43**, a maioria das organizações no estudo (54%) exigiu trabalho remoto em resposta à pandemia de COVID-19.

Figura 44

Como o trabalho remoto afetaria sua capacidade de responder a um vazamento de dados?

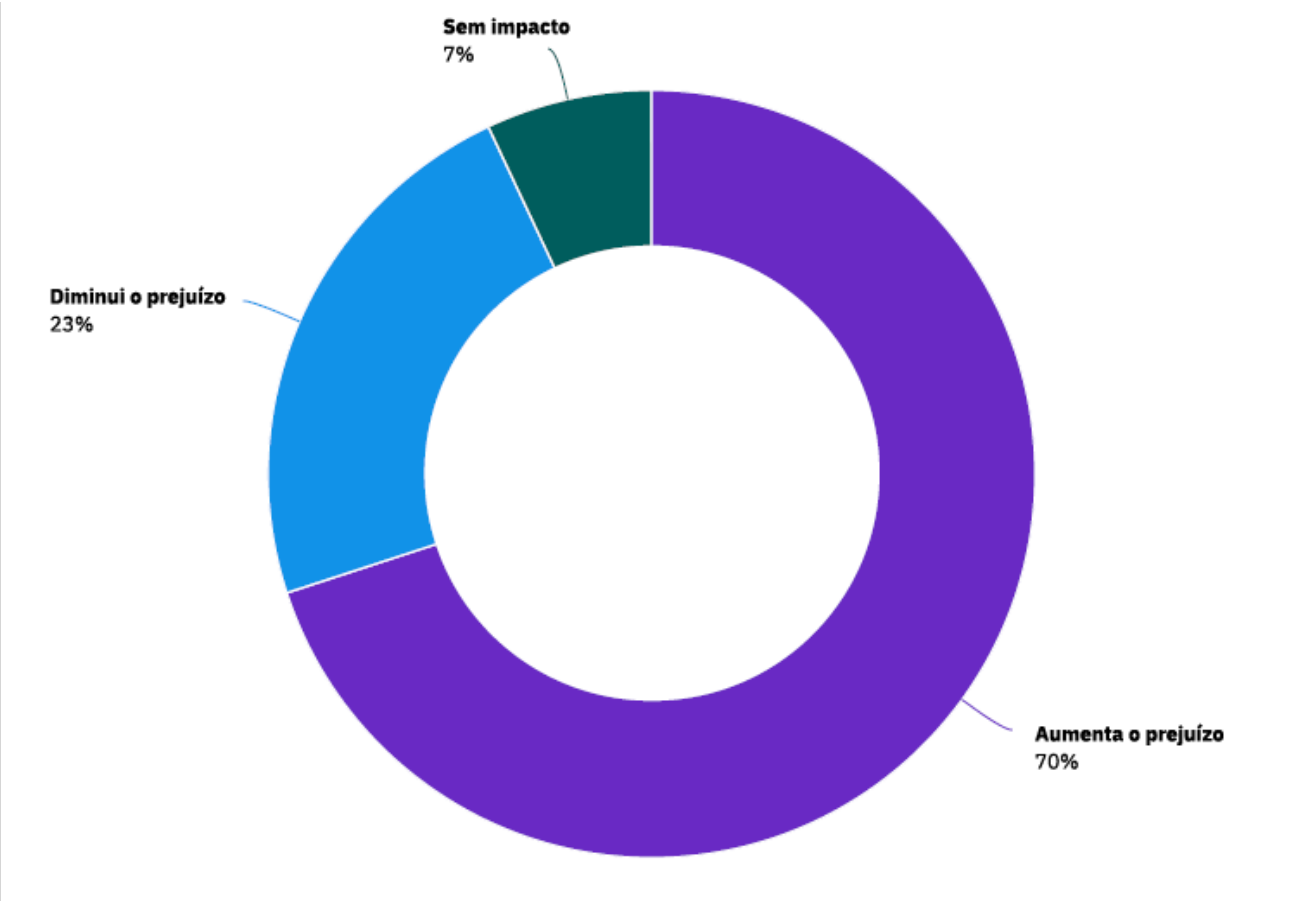


Três quartos dos participantes esperavam que um vazamento de dados levasse mais tempo para ser identificado e contido.

Dos participantes que disseram que suas organizações exigiam trabalho remoto em resposta à COVID-19, mais de três quartos (76%) disseram que isso aumentaria o tempo para identificar e conter um vazamento de dados, 20% disseram que isso diminuiria o tempo para identificar e conter um vazamento e 4% disseram que não haveria impacto, de acordo com a **Figura 44**.

Figura 45

Como o trabalho remoto afetaria o prejuízo de um vazamento de dados?



Os participantes esperavam que o trabalho remoto aumentasse o prejuízo de um possível vazamento de dados.

Dos participantes que disseram que suas organizações exigiam trabalho remoto em resposta à COVID-19, 70% disseram que isso aumentaria o prejuízo de um possível vazamento de dados, de acordo com a **Figura 45**. Outros 23% disseram que o trabalho remoto diminuiria o prejuízo de um vazamento de dados e 7% disseram que não haveria impacto.

O prejuízo de um megavazamento de dados

Este é o terceiro ano em que examinamos o prejuízo de megavazamentos, que são aqueles com mais de 1 milhão de registros comprometidos. Eles não são comuns para a maioria das empresas, mas os megavazamentos têm um impacto enorme nos consumidores e nos setores. O prejuízo médio de um megavazamento continuou crescendo desde que introduzimos essa análise no estudo de 2018.

A investigação deste ano se baseia na análise de 17 empresas que sofreram com um vazamento de dados envolvendo a perda ou o roubo de 1 milhão ou mais de registros. A explicação completa da metodologia usada está disponível nas perguntas frequentes sobre o prejuízo de um vazamento de dados, no final deste relatório.

Principais conclusões

US$ 392 milhões

Prejuízo médio de um vazamento de mais de 50 milhões de registros

100x

Diferença entre os prejuízos médios de um vazamento superior a 50 milhões de registros e um vazamento comum de dados

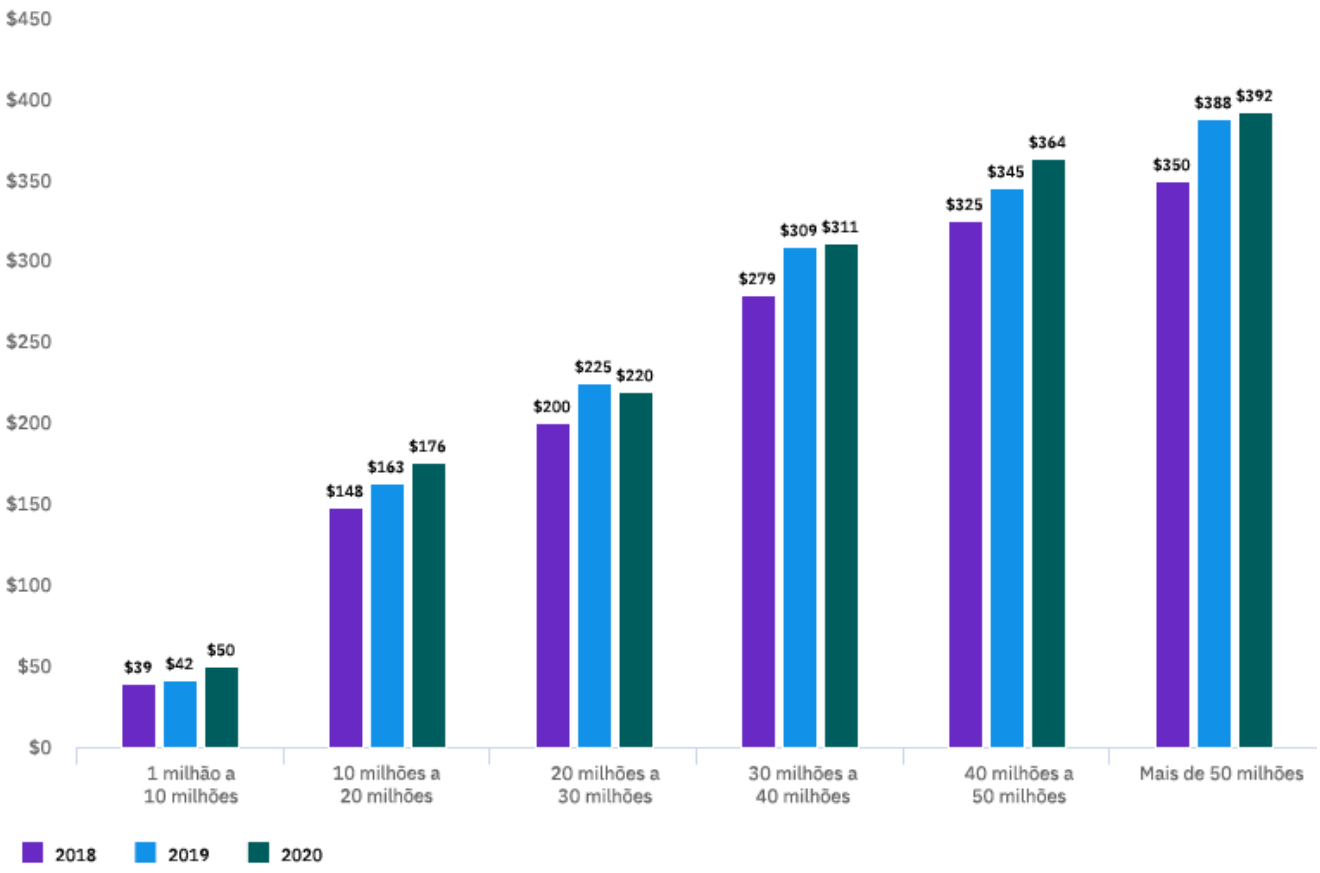
US$ 19 milhões

Aumento no prejuízo médio de um vazamento de 40 a 50 milhões de registros entre o estudo de 2019 e o de 2020

Figura 46

Prejuízo total médio de um megavazamento por número de registros perdidos

Medido em milhões de dólares (US$)



O prejuízo de um megavazamento de dados disparou.

Como mostra a **Figura 46**, vazamentos de 1 milhão a 10 milhões de registros custam, em média, US$ 50 milhões, mais de 25 vezes o custo médio de US$ 3,86 milhões para vazamentos de menos de 100 mil registros. O tamanho de vazamento de 1 milhão a 10 milhões de registros teve a maior taxa de crescimento, aumentando 22%, passando de US$ 39 milhões em 2018 para US$ 50 milhões em 2020.

Em vazamentos de mais de 50 milhões de registros, o prejuízo médio foi de US$ 392 milhões, mais de 100 vezes o prejuízo médio de um vazamento de dados. O maior aumento de prejuízo absoluto ocorreu em vazamentos de mais de 50 milhões de registros, que aumentaram de uma média de US$ 350 milhões em 2018 para US$ 392 milhões em 2020.

Etapas para minimizar os impactos financeiros e na reputação da marca de um vazamento de dados

*Nesta seção, a IBM Security descreve as etapas adotadas pelas organizações no estudo para reduzir o prejuízo financeiro e as consequências à reputação da marca decorrentes de um vazamento de dados.**

Invista em orquestração, automação e resposta de segurança (SOAR) para ajudar a melhorar os tempos de detecção e resposta.

No estudo sobre o prejuízo de um vazamento de dados, a automação da segurança reduz significativamente o tempo médio para identificar e responder a um vazamento, bem como o prejuízo médio. Software e serviços de SOAR podem ajudar sua organização a acelerar a resposta a incidentes com automação, padronização de processos e integração com as suas ferramentas de segurança. As tecnologias de automação, como inteligência artificial, análise e orquestração automatizada, foram todas associadas a prejuízos de um vazamento de dados abaixo da média.

Adote um modelo de segurança de confiança zero para impedir o acesso não autorizado a dados confidenciais.

Os resultados do estudo mostraram que credenciais perdidas e roubadas, juntamente com configurações incorretas da nuvem, foram as causas mais comuns de vazamentos de dados. Agora que as organizações passaram a incorporar o trabalho remoto e ambientes multicloud híbridos mais desconectados, uma estratégia de confiança zero pode ajudar a proteger dados e recursos, tornando-os acessíveis apenas com restrições e no contexto certo.

Teste seu plano de resposta a incidentes para aumentar a resiliência virtual.

As organizações do estudo que formaram equipes de resposta a incidentes (RI) e que testaram seus planos de resposta a incidentes reduziram o prejuízo total médio de um vazamento de dados em US$ 2 milhões, em comparação com organizações sem equipes de RI e que não testaram um plano de RI. O mantra “treine como você luta e lute como você treina” significa desenvolver e testar manuais de resposta a incidentes para ajudar a otimizar a capacidade da sua empresa de responder de forma rápida e eficaz a ataques.

*As recomendações de práticas de segurança são para fins de orientação e não garantem resultados.

Use ferramentas que ajudem a proteger e monitorar endpoints e funcionários remotos.

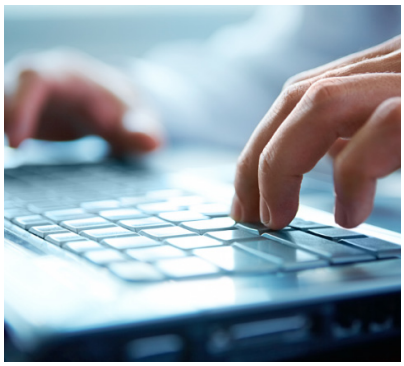
No estudo, 70% das organizações que exigiram trabalho remoto em resposta à pandemia de COVID-19 acreditavam que isso aumentaria o prejuízo de um vazamento de dados. Os produtos e serviços de gerenciamento unificado de endpoint (UEM) e gerenciamento de identidade e acesso (IAM) podem fornecer às equipes de segurança uma visibilidade mais profunda de atividades suspeitas em laptops, desktops, tablets, dispositivos móveis e de IoT, da empresa e dos funcionários (BYOD), inclusive de endpoints a que a organização não tem acesso físico, agilizando a investigação e o tempo de resposta para isolar e conter os danos.

Invista em programas de governança, gerenciamento de riscos e conformidade.

Atrás apenas do prejuízo causado pela perda de negócios, detecção e encaminhamento foi a categoria com o segundo maior prejuízo relacionado a um vazamento neste estudo. Uma estrutura interna para auditorias que avalia os riscos em toda a empresa e monitora a conformidade com os requisitos de governança pode melhorar a capacidade de uma organização de detectar um vazamento de dados e aumentar as medidas de contenção.

Minimize a complexidade dos ambientes de TI e segurança.

No estudo deste ano, a complexidade dos sistemas de segurança foi o fator que mais contribuiu para o elevado prejuízo de um vazamento de dados, em uma lista de 25 fatores. Vazamentos de dados causados por terceiros, ampla migração para a nuvem e ambientes de IoT/TO também foram associados a prejuízos mais altos de um vazamento de dados. As ferramentas de segurança com a capacidade de compartilhar dados entre sistemas diferentes podem ajudar as equipes de segurança a detectar incidentes em ambientes multicloud híbridos complexos.

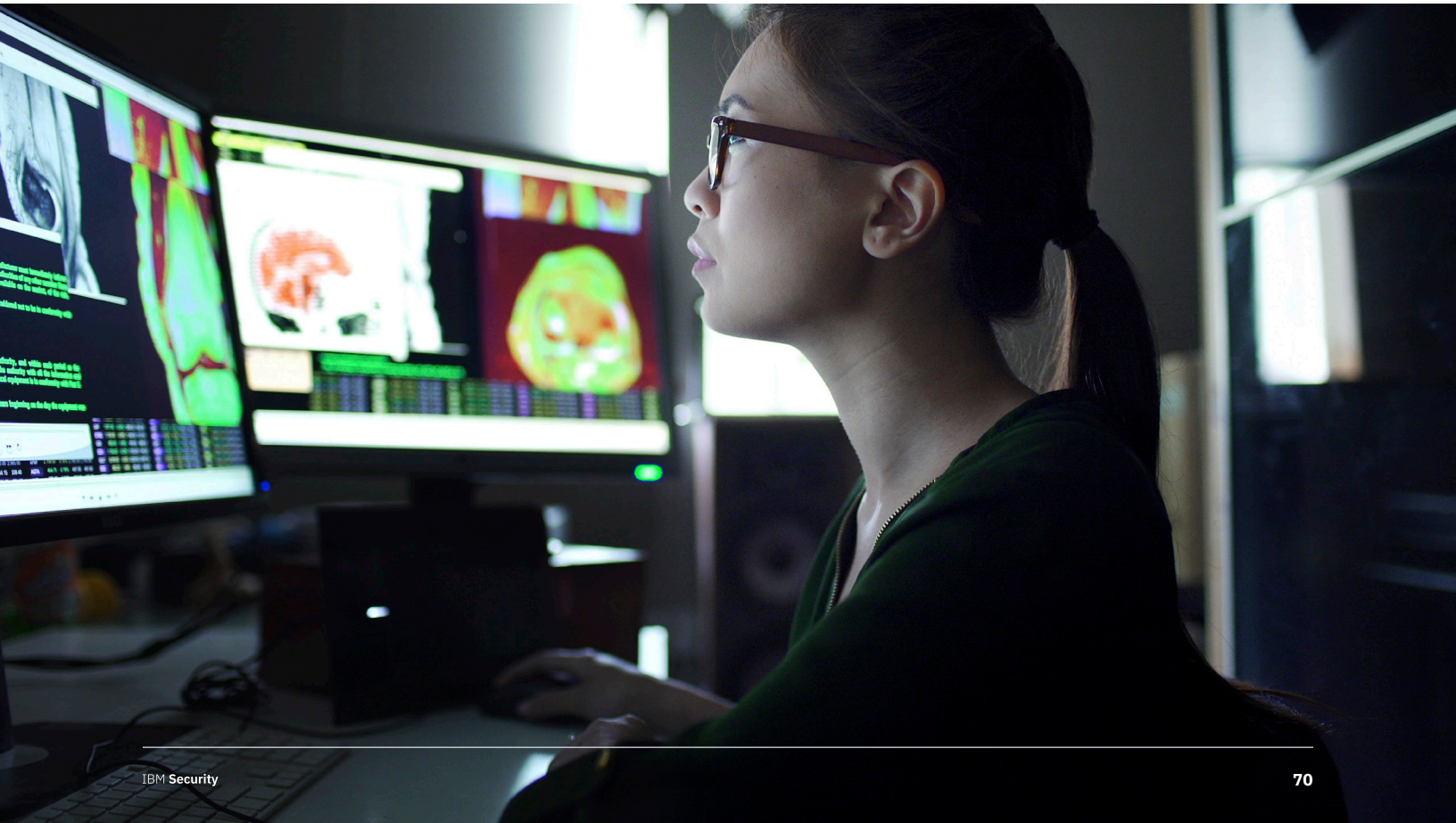


Proteja dados confidenciais em ambientes em nuvem usando políticas e tecnologia.

Com a crescente quantidade e o valor dos dados hospedados em ambientes em nuvem, as organizações devem tomar medidas para proteger os bancos de dados hospedados na nuvem. Use um esquema de classificação de dados e programas de retenção para ajudar a trazer visibilidade e reduzir o volume das informações confidenciais vulneráveis a um vazamento e protegê-las usando criptografia. Use verificação de vulnerabilidades, testes de penetração e equipes de alerta para ajudar a identificar exposições e configurações incorretas de vulnerabilidades de banco de dados hospedadas na nuvem. Todas essas soluções foram associadas no estudo com prejuízos médios mais baixos de um vazamento de dados.

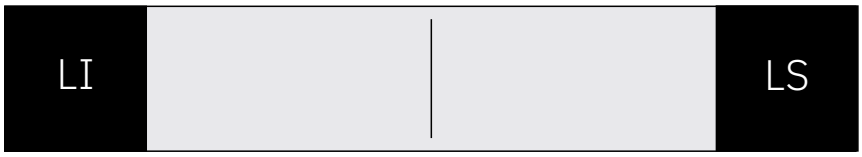
Use serviços de segurança gerenciados para compensar a falta de especialistas em segurança.

As organizações participantes do estudo identificaram a escassez de especialistas em segurança como um dos principais fatores que contribuem para o aumento do prejuízo de um vazamento de dados, enquanto os serviços de segurança gerenciados foram associados a prejuízos médios mais baixos de um vazamento de dados. Um provedor de serviços de segurança gerenciados pode ajudar a simplificar a segurança e os riscos com monitoramento contínuo e soluções e serviços integrados.



Metodologia de pesquisa

Para preservar a confidencialidade, o instrumento de referência não capturou nenhuma informação específica da empresa. Os métodos de coleta de dados não incluíram informações contábeis reais, mas basearam-se na estimativa que os participantes fizeram do prejuízo direto, marcando uma variável de intervalo em uma linha numérica. Os participantes foram instruídos a marcar a linha numérica em um ponto entre os limites inferior e superior de um intervalo para cada categoria de prejuízo.



O valor numérico obtido da linha numérica, em vez de uma estimativa pontual para cada categoria de prejuízo apresentada, preservou a confidencialidade e garantiu uma maior taxa de resposta. O instrumento de referência também exigiu que os profissionais fornecessem uma segunda estimativa para os prejuízos indiretos e de oportunidade, separadamente.

Para garantir um tamanho gerenciável para o processo de referência, limitamos cuidadosamente os itens apenas aos centros de atividades de custo que consideramos cruciais para a medição do prejuízo do vazamento de dados. Com base em discussões com especialistas, o conjunto final de itens incluía um conjunto fixo de atividades de custo. Após a coleta das informações de referência, cada instrumento foi reexaminado cuidadosamente quanto a consistência e integridade.

O escopo dos itens de prejuízo de um vazamento de dados contidos no nosso instrumento de referência foi limitado a categorias de custo conhecidas que se aplicavam a um amplo conjunto de operações comerciais que lidam com informações pessoais. Acreditamos que um estudo focado em processos de negócios, não em atividades de proteção de dados ou conformidade de privacidade, traria melhores resultados de qualidade.

Perguntas frequentes sobre o prejuízo de um vazamento de dados

O que é um vazamento de dados?
Um vazamento é definido como um evento em que o nome de uma pessoa e um registro médico e/ou um registro financeiro ou cartão de débito estão potencialmente em risco, seja em formato eletrônico ou em papel. Os vazamentos incluídos no estudo variaram de 3.400 a 99.730 registros comprometidos.

O que é um registro comprometido?
Registro são informações que identificam uma pessoa individualmente e que foram perdidas ou roubadas em um vazamento de dados. Entre os exemplos estão um banco de dados com o nome de um indivíduo, informações de cartão de crédito e outras informações de identificação pessoal (PII) ou um registro de saúde com o nome do segurado e informações de pagamento.

Como vocês coletam os dados?
Nossos pesquisadores coletaram dados qualitativos detalhados por meio de mais de 3.200 entrevistas separadas com indivíduos em 524 organizações que sofreram com um vazamento de dados entre agosto de 2019 e abril de 2020. As organizações começaram a ser recrutadas em outubro de 2019, e as entrevistas foram concluídas em 21 de abril de 2020. Participaram das entrevistas profissionais de TI, conformidade e segurança da informação que conhecem bem o vazamento de dados da organização e o prejuízo associado à resolução desse incidente. Por motivo de privacidade, não coletamos informações específicas da organização.

Como vocês calculam o prejuízo?
Para calcular o prejuízo médio de um vazamento de dados, coletamos as despesas diretas e indiretas arcadas pela organização. As despesas diretas incluem contratar especialistas forenses, terceirizar o suporte de linha direta e fornecer assinaturas gratuitas de monitoramento de crédito e descontos para futuros produtos e serviços. Os custos indiretos incluem investigações e comunicações internas, bem como o valor extrapolado da perda de clientes resultante de rotatividade ou diminuição das taxas de aquisição de clientes.

Somente eventos diretamente relevantes para a experiência de vazamento de dados são representados nesta pesquisa. Por exemplo, novos regulamentos, como o GDPR (General Data Protection Regulation, ou Regulamento Geral sobre a Proteção de Dados) e a CCPA (California Consumer Privacy Act, ou Lei de Privacidade do Consumidor da Califórnia), podem incentivar as organizações a aumentar os investimentos em tecnologias de governança da segurança virtual, mas não afetam diretamente o prejuízo de um vazamento de dados, como apresentamos nesta pesquisa.

Para manter a consistência com anos anteriores, usamos o mesmo método de conversão de moeda em vez de ajustar os custos contábeis.

Como a pesquisa de referência difere da pesquisa de opinião?
A unidade de análise do relatório "Prejuízo de um vazamento de dados" é a organização. Na pesquisa de opinião, a unidade de análise é o indivíduo. Recrutamos 524 organizações para participar deste estudo.

O prejuízo médio por registro pode ser usado para calcular o prejuízo de vazamentos envolvendo milhões de registros perdidos ou roubados?
Nesta pesquisa, o prejuízo médio de um vazamento de dados não se aplica a megavazamentos ou vazamentos catastróficos, como Equifax, Capital One ou Facebook. Esses vazamentos não são comuns à maioria das organizações.

Portanto, para tirar conclusões úteis no entendimento do comportamento do prejuízo do vazamento de dados, selecionamos os incidentes que não excedem cem mil registros. Não é consistente com esta pesquisa usar o prejuízo por registro para calcular o prejuízo de vazamentos únicos ou múltiplos, totalizando milhões de registros. No entanto, o estudo usa uma estrutura de simulação para medir o impacto no prejuízo de um "megavazmento" envolvendo 1 milhão ou mais de registros, com base em uma amostra de 17 violações muito grandes desse tamanho.

Por que vocês usam métodos de simulação para estimar o prejuízo de um megavazamento de dados?
O tamanho da amostra de 17 empresas que passaram por um megavazamento é muito pequeno para realizar uma análise estatisticamente significativa usando métodos de custo baseados em atividades. Para solucionar esse problema, implantamos a simulação de Monte Carlo para estimar uma série de resultados possíveis (aleatórios) por meio de ensaios repetidos.

No total, realizamos mais de 150 mil ensaios. A média geral de todas as médias da amostra oferece um resultado mais provável para cada tamanho de vazamento de dados, variando de 1 a 50 milhões de registros comprometidos.

Vocês acompanham as mesmas organizações todos os anos?
Cada estudo anual envolve uma amostra diferente de empresas. Para ser consistente com os relatórios anteriores, recrutamos e associamos empresas a cada ano com características semelhantes, como setor, número de funcionários, presença geográfica e tamanho do vazamento de dados. Desde o início desta pesquisa em 2005, estudamos as experiências de vazamento de dados de 3.940 organizações.

Características da organização

O estudo deste ano incluiu 524 organizações de vários tamanhos, amostradas em uma grande variedade de localidades e setores. O estudo 2020 foi realizado em amostras de 17 países ou regiões e 17 setores.

Pela primeira vez, o estudo examinou um grupo de organizações na América Latina, que inclui México, Argentina, Chile e Colômbia.

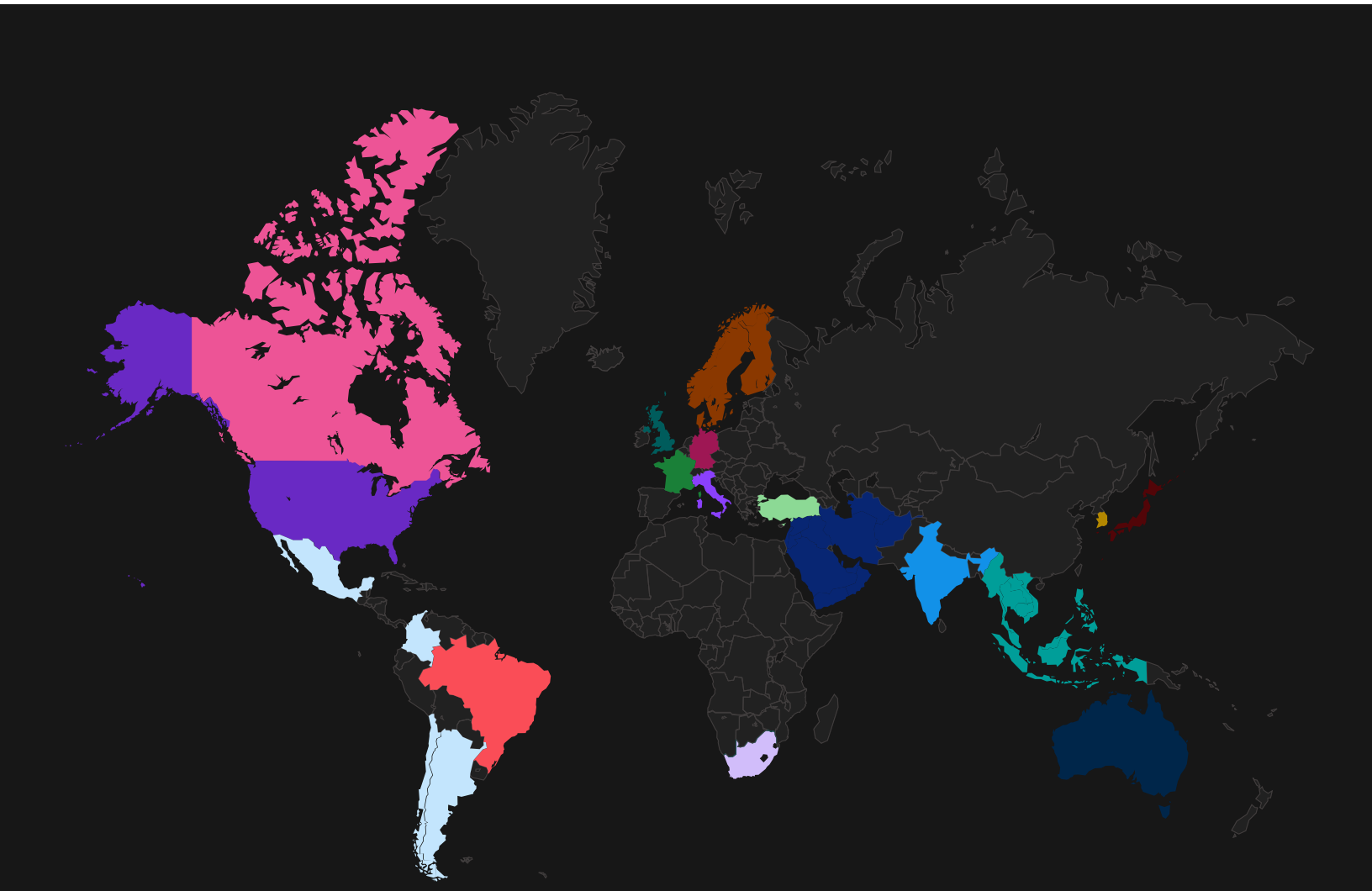
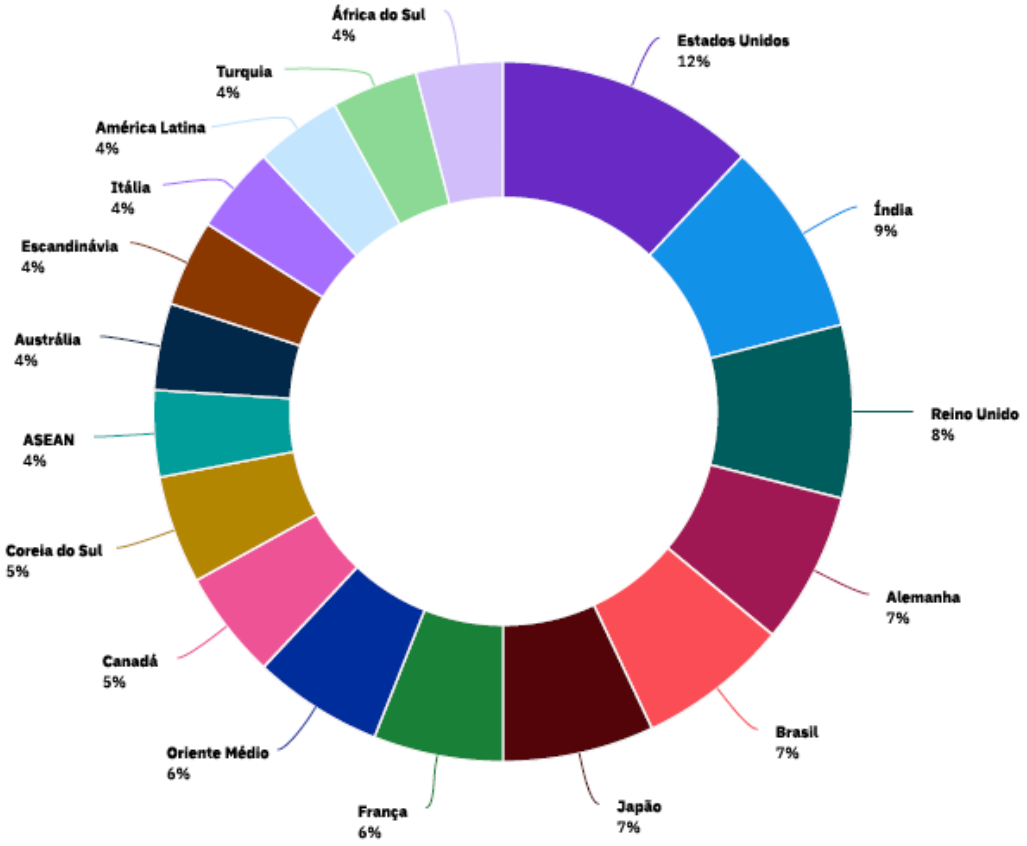


Figura 47

Distribuição da amostra por país ou região



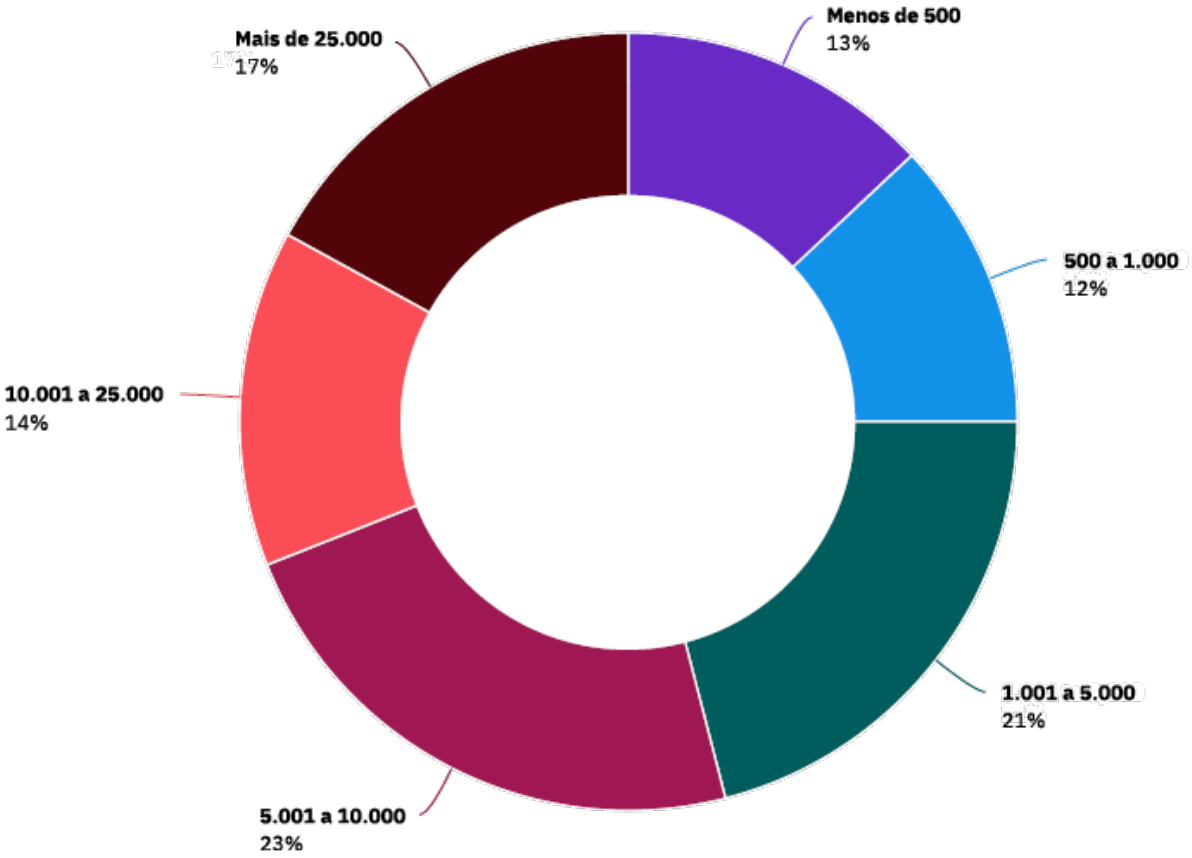
Países/regiões de seis continentes foram representados no estudo.

A Figura 47 mostra a distribuição das organizações de referência por país ou região. Os Estados Unidos tiveram a maior representação com 12%, seguidos pela Índia, com 9%, e o Reino Unido, com 8%. Os países/regiões com a menor representação foram ASEAN, Austrália, Escandinávia, Itália, América Latina, Turquia e África do Sul.

Figura 48

Distribuição da amostra por tamanho da empresa

Medido por número de funcionários

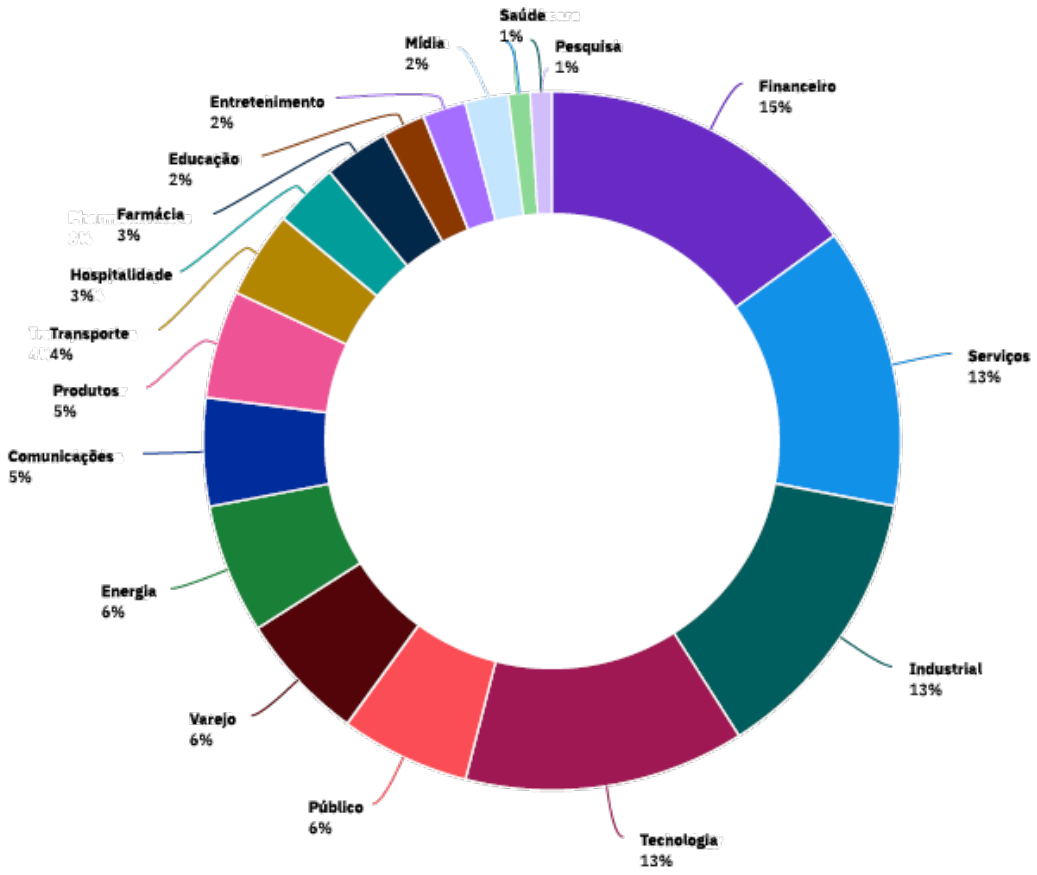


Pequenas, médias e grandes organizações foram representadas.

A Figura 48 mostra a distribuição das 524 organizações da amostra por número de funcionários, o que representa o tamanho da empresa. A amostra teve um peso um pouco maior nas organizações de médio porte, com 58% das organizações entre 1.001 e 25.000 funcionários, enquanto 25% tinham menos de 1.000 e 17% tinham mais de 25.000 funcionários.

Figura 49

Distribuição da amostra por setor



A representação se inclinou para alguns setores importantes.

A Figura 49 mostra a distribuição das organizações de referência por setor. Dezessete setores foram representados no estudo deste ano. Os maiores setores foram o financeiro, de serviços, industrial e de tecnologia. As definições de setor são explicadas separadamente.

Definições de setores

Saúde
Hospitais, clínicas

Financeiro
Empresas bancárias, de seguros e de investimento

Energia
Empresas de petróleo e gás, empresas de serviços públicos, produtores e fornecedores de energia alternativa

Farmacêutico
Farmacêutica, inclusive ciências biomédicas

Industrial
Empresas de processos químicos, engenharia e fabricação

Tecnologia
Empresas de software e hardware

Educação
Universidades e faculdades públicas e privadas, empresas de treinamento e desenvolvimento

Serviços
Serviços profissionais, como empresas jurídicas, contábeis e de consultoria

Entretenimento
Produção de filmes, esportes, jogos e cassinos

Transporte
Companhias aéreas, ferrovias, caminhões e empresas de entrega

Comunicações
Jornais, editoras de livros, agências de relações públicas e publicidade

Produtos
Fabricantes e distribuidores de bens de consumo

Mídia
Televisão, satélite, redes sociais, Internet

Hospitalidade
Hotéis, redes de restaurantes, linhas de cruzeiro

Varejo
Lojas físicas e comércio eletrônico

Pesquisa
Pesquisa de mercado, grupos de ideias, P&D

Público
Órgãos federais, estaduais e municipais e ONGs

Limitações da pesquisa

Nosso estudo usa um método de referência confidencial e proprietário que foi implantado com êxito em pesquisas anteriores. No entanto, existem limitações inerentes a esta pesquisa de referência que precisam ser cuidadosamente consideradas antes de se tirar conclusões dos resultados.

Resultados não estatísticos
Nosso estudo baseia-se em uma amostra representativa e não estatística de entidades globais. Inferências estatísticas, margens de erro e intervalos de confiança não podem ser aplicados a esses dados, uma vez que nossos métodos de amostragem não são científicos.

Não resposta
O viés de não resposta não foi testado, portanto, é possível que as empresas que não participaram sejam substancialmente diferentes em termos do prejuízo do vazamento de dados subjacente.

Viés do quadro de amostragem
Como nosso quadro de amostragem é crítico, a qualidade dos resultados é influenciada pelo grau em que o quadro é representativo da população de empresas em estudo. É nossa convicção que o atual quadro de amostragem é tendencioso para empresas com programas mais maduros de privacidade ou segurança da informação.

Informações específicas da empresa
O estudo comparativo não captura informações de identificação da empresa. Ele permite que as pessoas usem variáveis de resposta categórica para divulgar informações demográficas sobre a empresa e a categoria do setor.

Fatores não medidos
Omitimos variáveis de nossas análises, como principais tendências e características organizacionais. A extensão em que variáveis omitidas podem explicar os resultados da referência não pode ser determinada.

Resultados de custo extrapolados
Embora certas verificações e balanços possam ser incorporados ao processo de referência, é sempre possível que os entrevistados não tenham fornecido respostas precisas ou verdadeiras. Além disso, o uso de métodos de extrapolação de custos, em vez de dados reais, pode inadvertidamente introduzir viés e imprecisões.

Resultados de custo extrapolados
Este ano, um dólar norte-americano forte influenciou significativamente a análise de prejuízos globais. A conversão de moedas locais em dólar norte-americano diminuiu as estimativas por registro e prejuízo total médio. Para fins de consistência com os anos anteriores, decidimos continuar usando o mesmo método contábil, em vez de ajustar o custo.

Sobre o Ponemon Institute e a IBM Security

O relatório *"Prejuízo de um vazamento de dados"* é produto da parceria entre o Ponemon Institute e a IBM Security. A pesquisa é conduzida de forma independente pelo Ponemon Institute, e os resultados são patrocinados, analisados, relatados e publicados pela IBM Security.

Em caso de dúvidas ou para fazer comentários sobre este relatório de pesquisa, inclusive sobre a permissão para citar ou reproduzir o relatório, entre em contato por carta, telefone ou e-mail:

Ponemon Institute LLC

Attn: Research Department
2308 US 31 NorthTraverse
City, Michigan 49686 USA

1.800.887.3118

research@ponemon.org

Ponemon INSTITUTE

O Ponemon Institute se dedica a pesquisa e educação independentes que aprimoram as práticas responsáveis de gerenciamento de informações e privacidade nas empresas e no governo. Nossa missão é conduzir estudos empíricos de alta qualidade sobre questões críticas que afetam o gerenciamento e a segurança de informações confidenciais sobre pessoas e organizações.

O Ponemon Institute mantém rigorosos padrões de confidencialidade de dados, privacidade e pesquisa ética e não coleta nenhuma informação pessoal identificável de indivíduos (ou informações identificáveis da empresa em pesquisa comercial). Além disso, rígidos padrões de qualidade garantem que os participantes não sejam solicitados a responder perguntas estranhas, irrelevantes ou impróprias.

IBM **Security**

A IBM Security oferece os mais avançados e integrados portfólios de produtos e serviços de segurança corporativa. O portfólio, com respaldo da pesquisa IBM X-Force® de renome mundial, fornece soluções de segurança para ajudar as organizações a melhorar a segurança na própria estrutura de negócios, para que possam prosperar diante da incerteza.

A IBM opera uma das mais amplas e profundas organizações de pesquisa, desenvolvimento e entrega de segurança. Monitorando mais de dois trilhões de eventos por mês em mais de 130 países, a IBM conta com mais de 3.000 patentes de segurança. Para saber mais, acesse https://www.ibm.com/br-pt/security.

Seu próximo passo

Serviços de segurança virtual

Reduza os riscos com serviços de consultoria, nuvem e segurança gerenciada

Saiba mais →

Gerenciamento de identificação e acesso

Conecte todos os usuários, APIs e dispositivos a todos os aplicativos com segurança

Saiba mais →

Segurança dos dados

Descubra, classifique e proteja dados corporativos confidenciais

Saiba mais →

Informações de segurança e gerenciamento de eventos

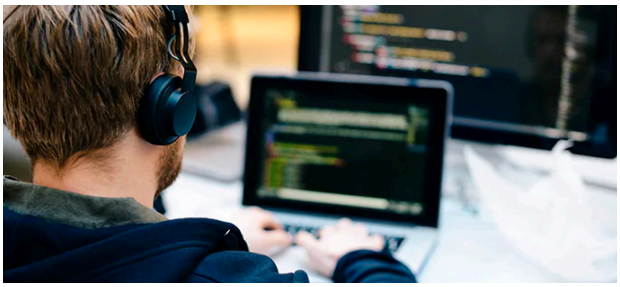
Ganhe visibilidade para detectar, investigar e responder a ameaças

Saiba mais →

Orquestração, automação e resposta de segurança

Acelere a resposta a incidentes com orquestração e automação

Saiba mais →



Segurança da nuvem

Integre a segurança na sua jornada para a multicloud híbrida

Saiba mais →

© Copyright IBM Corporation 2020

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produzido nos Estados Unidos da América
Julho de 2020

IBM, o logotipo da IBM e ibm.com são marcas comerciais da International Business Machines Corp. registradas em vários países no mundo todo. Os nomes de outros produtos e serviços podem ser marcas comerciais da IBM ou de outras empresas. Uma lista atualizada das marcas registradas IBM encontra-se disponível na Web em “Copyright and trademark information” (“Informações de copyright e marca registrada”), em ibm.com/legal/copytrade.shtml

Este documento é atual na data de publicação e pode ser alterado pela IBM a qualquer momento. Nem todas as ofertas estão disponíveis em todo país em que a IBM opera. Os dados de desempenho e os exemplos de clientes citados estão presentes apenas para propósitos ilustrativos. Os resultados reais de desempenho podem variar de acordo com as configurações específicas e as condições de funcionamento.

AS INFORMAÇÕES NESTE DOCUMENTO SÃO FORNECIDAS “COMO ESTÃO”, SEM QUALQUER GARANTIA, EXPRESSA OU IMPLÍCITA, INCLUSIVE SEM QUAISQUER GARANTIAS DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UM PROPÓSITO EM PARTICULAR E QUALQUER GARANTIA OU CONDIÇÃO DE NÃO VIOLAÇÃO.

Os produtos da IBM são garantidos de acordo com os termos e condições dos acordos sob os quais são fornecidos. O cliente é responsável por garantir a conformidade para com as leis e regulamentações a ele aplicáveis. A IBM não fornece nenhum aconselhamento jurídico, representa ou garante que seus serviços ou produtos garantirão que o cliente esteja em conformidade com qualquer lei ou regulamento. Declarações em relação à direção futura da IBM e da intenção estão sujeitas a mudança ou retirada sem aviso prévio, e representam apenas metas e objetivos.

IBM **Security**