EDIÇÃO 2026 · SETEMBRO DE 2026

SCSDetect

CONTRAINTELIGÊNCIA CORPORATIVA · RELATÓRIO ANUAL

Fraude e espionagem corporativa: **2015–2025**

Dez anos de dados comparáveis, o Brasil na década — e um indicador novo para a ameaça que mais cresceu.

US$ 104 mil

perda mediana por caso de fraude em 2025. Eram US$ 150 mil em 2015.

12 meses

até a fraude ser descoberta. Eram 18 meses em 2015.

87%

das empresas alemãs foram vítimas de espionagem, sabotagem ou roubo de dados. Eram 51% em 2015.

Detectar. Localizar. Neutralizar.

Varredura eletrônica de ambientes, veículos, linhas e dispositivos móveis · São Paulo · Rio de Janeiro · Brasília

SCSDetect — uma empresa do GrupoSCS · scsdetect.com · gruposcs.com.br

RELATÓRIO ANUAL 2026

Fraude e espionagem corporativa

Uma comparação entre 2015 e 2025

SCSDetect
Contrainteligência corporativa
Uma empresa do GrupoSCS

Sumário

RELATÓRIO ANUAL 2026

Apresentação

Dez anos depois, a fraude custa menos por caso e é descoberta mais cedo. O que ela rouba, porém, mudou de natureza.

Em 2015, o Brasil vivia o auge da Lava Jato, a Lei Anticorrupção acabava de ser regulamentada e a palavra *compliance* ainda era novidade em boa parte das empresas. Dez anos depois, o país tem uma autoridade de proteção de dados, mais de R$ 10 bilhões devolvidos por acordos de leniência e operações policiais que revelaram facções controlando distribuidoras de combustível, fintechs e fundos de investimento.

Este relatório mede o que mudou. Ele compara, tema a tema, os dados de 2015 com os de 2025 — sempre com a fonte, o ano e a amostra à vista. A espinha da comparação é a série global de fraude ocupacional da ACFE, que aplica a mesma metodologia há quase trinta anos: duas fotografias com a mesma lente, uma década entre elas.

Alguns resultados surpreendem. A perda mediana por caso caiu de US$ 150 mil para US$ 104 mil e a fraude típica passou a ser descoberta em doze meses, e não mais em dezoito. Detectar melhorou. Mas a corrupção saltou de 35% para 45% dos casos, e o velho *hotline* perdeu para o e-mail e para a web.

E há um movimento que nenhuma dessas estatísticas captura sozinha: ao lado da perda financeira, a informação passou a ser alvo de peso próprio. Na Alemanha, onde existe a série pública mais longa sobre o tema, a proporção de empresas vítimas de espionagem, sabotagem ou roubo de dados saiu de 51% em 2015 para 87% em 2025. O custo anual dos incidentes causados por pessoas de dentro passou de US$ 4,3 milhões para US$ 19,5 milhões por organização.

A SCSDetect atua há 18 anos na contrainteligência corporativa — varredura eletrônica de ambientes, veículos e linhas, verificação de dispositivos móveis e apoio forense a investigações internas. Vemos, em campo, o que as estatísticas mostram em agregado. Este documento é a nossa contribuição para que conselhos, diretorias, compliance, auditoria e segurança decidam com informação, e não com suposição.

Agradecemos a quem produz e publica as pesquisas aqui citadas: sem dados abertos não há gestão de risco possível.

Rodrigo Alves
COO · Responsável pelo relatório
SCSDetect

METODOLOGIA

Sobre este relatório

Duas fotografias com a mesma lente: 2015 e 2025, sempre com fonte, ano e amostra à vista.

Nenhum número foi estimado pela SCSDetect. Onde não existe dado comparável, dizemos isso.

O que este documento é

Um relatório anual de referência sobre fraude e espionagem corporativa, construído sobre três camadas:

- **A comparação 2015 × 2025.** Para cada pergunta, o dado de 2015 e o de 2025, com a fonte de cada um. Sempre que possível, as duas pontas vêm da mesma pesquisa, aplicada com a mesma metodologia nos dois momentos — é o caso da série global da ACFE, da série alemã do Bitkom, do Índice de Percepção da Corrupção e do custo dos incidentes causados por pessoas de dentro.
- **O indicador de espionagem corporativa.** Um capítulo que reúne, em um único painel, os sinais mensuráveis de exposição à espionagem e a leitura da SCSDetect sobre o que eles significam para a empresa brasileira.
- **A cronologia da década.** Os marcos de legislação, enforcement, proteção de dados, crime organizado e tecnologia que ajudam a explicar por que os números se moveram como se moveram.

Como ler as comparações

Onde as duas pontas vêm da mesma pesquisa, a comparação é direta e está identificada como **série**. Onde vêm de pesquisas diferentes — porque nenhuma casa manteve o mesmo levantamento por dez anos no Brasil —, os números aparecem lado a lado, com as amostras declaradas, e o texto comenta a direção do movimento sem tratá-los como série única.

A convenção visual é constante em todo o documento: `CINZA` identifica 2015 e `AZUL` identifica 2025. Cada gráfico traz a fonte em forma curta; a citação completa de cada uma — com amostra, universo, janela de campo e endereço eletrônico — está reunida no capítulo **Fontes e referências**, no fim do documento.

O que não está aqui

Três lacunas merecem registro honesto. Não existe, no Brasil, pesquisa sobre fraude corporativa aplicada de forma comparável em 2015 e em 2025 — por isso a ponta brasileira de alguns capítulos combina levantamentos distintos, sempre identificados. Não existe estatística oficial brasileira de espionagem corporativa, razão pela qual o indicador do capítulo 7 recorre a séries internacionais e a casos documentados. E não existe medida pública da incidência de escutas em empresas brasileiras: é exatamente essa lacuna que a pesquisa SCSDetect 2027 pretende começar a preencher.

PANORAMA

A década em números

Detectar melhorou. O alvo mudou. E a régua de integridade subiu sem que a percepção de corrupção acompanhasse.

Nove indicadores resumem o movimento de 2015 a 2025. Os três primeiros vêm da mesma pesquisa global, aplicada com a mesma metodologia nas duas pontas; os três seguintes medem o deslocamento do alvo para a informação; os três últimos descrevem o Brasil.

A fraude ficou menor e mais curta

US$ 104 mil
é a perda mediana por caso de fraude ocupacional investigado em 2025; eram US$ 150 mil em 2015

12 meses
é a duração típica de uma fraude até ser descoberta; eram 18 meses em 2015

43%
das fraudes são descobertas por denúncia; eram 39% em 2015 — segue sendo o canal número um

Fonte dos três: ACFE, Report to the Nations — edições 2016 e 2026.

Mas o alvo mudou de natureza

45%
dos casos envolvem corrupção, contra 35% em 2015 — o esquema que mais cresceu na década

12%
das empresas alemãs constataram escuta de reuniões ou telefonemas no local em 2025, e outras 20% suspeitam; eram 8% constatados em 2015

US$ 19,5 mi
é o custo anual dos incidentes causados por pessoas de dentro, por organização; eram US$ 4,3 milhões em 2015

Fontes, na ordem: ACFE, Occupational Fraud 2026; Bitkom, Wirtschaftsschutz — edições 2015 e 2025; Ponemon, custo dos incidentes internos — edições 2016 e 2026.

E o Brasil subiu a régua sem mudar a percepção

35 pontos
é a nota do Brasil no Índice de Percepção da Corrupção de 2025, contra 38 em 2015 — de 76º para 107º lugar

128
empresas foram reconhecidas pelo Pró-Ética da CGU no ciclo 2025-2026; eram 19 em 2015

R$ 10 bi
foram devolvidos aos cofres públicos por 32 acordos de leniência assinados desde 2017

Fontes, na ordem: Transparência Internacional, Índice de Percepção da Corrupção — 2015 e 2025; Instituto Ethos e CGU, Pró-Ética — ciclo 2015; CGU, Pró-Ética — ciclo 2025-2026; CGU, acordos de leniência — maio de 2025.

As pesquisas citadas têm amostras, universos e janelas próprios, descritos junto a cada gráfico ao longo do documento. O capítulo final traz a lista completa de fontes.

CAPÍTULO 1

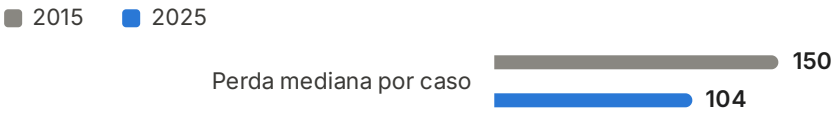
Quanto custa a fraude e quanto tempo ela dura

A boa notícia da década: a fraude típica ficou um terço mais barata e é descoberta seis meses antes.

Entre as duas pontas da série, a perda mediana por caso caiu quase um terço e a duração típica do esquema encolheu de dezoito para doze meses. Os dois movimentos estão ligados: fraude descoberta mais cedo é fraude menor, porque o prejuízo se acumula enquanto o esquema corre.

Quanto custa um caso de fraude

Em milhares de dólares

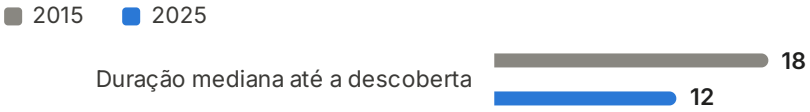


A perda média caiu de US$ 2,7 milhões para US$ 1,46 milhão, e a proporção de casos acima de US$ 1 milhão passou de 23,2% para 20%. A mediana é o indicador mais estável, porque não é distorcida pelos poucos casos de valor extremo.

Fonte: ACFE, Report to the Nations — edições 2016 e 2026

Quanto tempo a fraude fica escondida

Meses entre o início do esquema e a sua descoberta



Fonte: ACFE, Report to the Nations — edições 2016 e 2026

Cada mês de fraude não detectada custa cerca de US$ 9,4 mil. O tempo é a variável mais cara.

Quanto mais tempo escondida, mais cara (2025)

Perda mediana em milhares de dólares, por duração do esquema

Cada mês a mais de fraude não detectada custa, em média, cerca de US$ 9,4 mil. É por isso que reduzir o tempo de detecção rende mais do que endurecer a punição.

Fonte: ACFE, Occupational Fraud 2026

Quanto da receita a fraude consome

2015

5%

da receita anual, na estimativa dos peritos que investigaram os casos

ACFE, Report to the Nations 2016

2025

5%

da receita anual — a estimativa não mudou em dez anos

ACFE, Occupational Fraud 2026

É uma estimativa de opinião dos peritos, repetida sem alteração metodológica ao longo das edições, e não uma medição contábil. Serve como ordem de grandeza.

A melhora, porém, não é homogênea. Um em cada cinco casos ainda supera US$ 1 milhão, e os esquemas que passam de cinco

anos sem detecção custam, na mediana, mais de US$ 1,1 milhão — vinte e sete vezes mais que os descobertos em até seis meses.

No Brasil, recuperar o prejuízo segue sendo exceção: nove em cada dez casos recuperam menos de um quinto.

O Brasil na ponta de 2025

63%

das empresas brasileiras identificaram ao menos uma fraude nos últimos doze meses

Grant Thornton Brasil, Diagnóstico das Fraudes no Brasil, 2025

39%

dos casos no Brasil causaram prejuízo acima de R$ 10 milhões; 46% ficaram até R$ 500 mil

Grant Thornton Brasil, Diagnóstico das Fraudes no Brasil, 2025

93%

das ocorrências no Brasil terminaram com recuperação de menos de 20% do prejuízo

Grant Thornton Brasil, Diagnóstico das Fraudes no Brasil, 2025

Os levantamentos brasileiros não têm série comparável de dez anos, mas dão o retrato de 2025: seis em cada dez empresas identificaram fraude no ano, quatro em cada dez casos passaram de R$ 10 milhões e quase todas as vítimas recuperaram menos de um quinto do que perderam. Em 2015, a leitura disponível — feita com pouco mais de cinquenta executivos brasileiros — registrava que **94%** deles achavam que a exposição à fraude estava aumentando.

> **Leitura SCSDetect**
>
> A queda da perda mediana não significa que a fraude ficou menos grave — indica que a fraude *contábil*, a que deixa rastro em transação e cabe num questionário, está sendo pega mais cedo. O prejuízo de uma proposta comercial interceptada, de uma fórmula copiada ou de uma negociação ouvida por um concorrente não gera lançamento nenhum: gera uma licitação perdida meses depois. Essa perda nunca entra na mediana.

CAPÍTULO 2

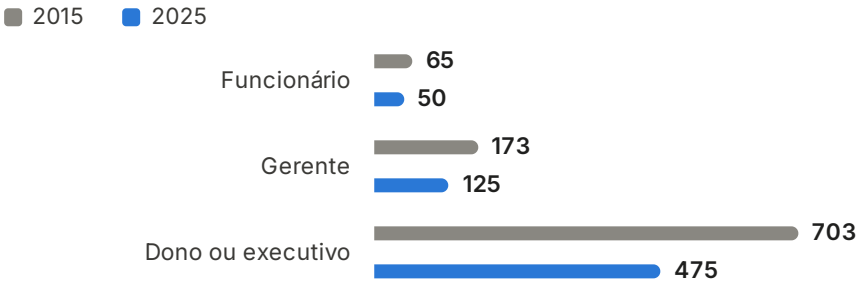
Quem comete e por quê

Funcionários e gerentes dividem os casos meio a meio. Executivos são poucos — e custam nove vezes mais.

O retrato mais estável de toda a série é este: quanto mais alto o cargo, maior o prejuízo. Em 2015, um dono ou executivo causava perda mediana de US$ 703 mil, contra US$ 65 mil de um funcionário. Dez anos depois, os valores caíram — para US$ 475 mil e US$ 50 mil —, mas a proporção entre eles praticamente não se moveu.

Perda mediana por nível hierárquico do fraudador

Em milhares de dólares

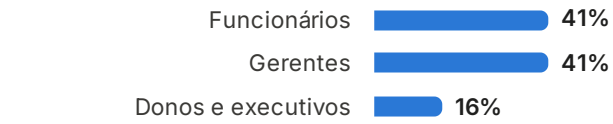


Em 2015, um dono ou executivo causava prejuízo dez vezes maior que um funcionário; em 2025, nove vezes. A desproporção diminuiu pouco — e segue sendo o argumento mais forte para que o controle alcance também quem está no topo.

Fonte: ACFE, Report to the Nations — edições 2016 e 2026

Quem comete a fraude (2025)

Proporção dos casos investigados, por nível hierárquico

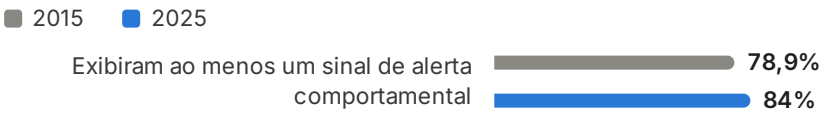


Fonte: ACFE, Occupational Fraud 2026

Nove em cada dez fraudadores são primários. Consultar antecedentes é necessário, mas não é o controle que encontra o fraudador.

Sinais de alerta comportamental

Proporção dos fraudadores que exibiram pelo menos um



Os sinais mais comuns nas duas pontas são os mesmos: viver acima do padrão de renda e enfrentar dificuldades financeiras.

Fonte: ACFE, Report to the Nations — edições 2016 e 2026

O fraudador quase nunca tem ficha

2015

94,8%

dos fraudadores nunca haviam sido condenados por crime relacionado a fraude; apenas 8,3% já haviam sido demitidos por isso

ACFE, Report to the Nations 2016

2025

87%

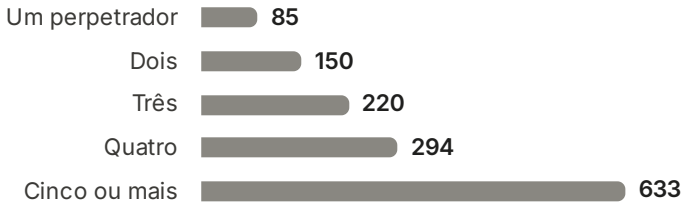
dos fraudadores nunca haviam sido condenados antes do caso investigado

ACFE, Occupational Fraud 2024

Verificar antecedentes continua necessário — mas dez anos de dados mostram que a verificação sozinha não encontra o fraudador, porque ele quase nunca é reincidente.

Quanto o conluio multiplica o prejuízo (2015)

Perda mediana em milhares de dólares, por número de envolvidos



Em 2025, a ACFE registra que quase metade dos casos envolveu mais de um perpetrador. A escada de perdas é o achado que se manteve nas duas pontas: cada pessoa a mais no esquema multiplica o valor desviado.

Fonte: ACFE, Report to the Nations 2016

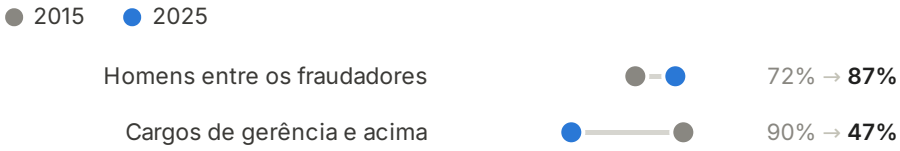
No Brasil, quase metade dos casos envolve alguém de coordenação para cima.

O perfil brasileiro

As duas pontas brasileiras vêm de pesquisas diferentes e não formam série, mas convergem no essencial: o fraudador brasileiro é homem, está na faixa dos 26 aos 45 anos, tem alguns anos de casa e ocupa posição de confiança. Em 2016, um levantamento registrava que quase 90% dos fraudadores internos brasileiros pertenciam à gerência média ou à diretoria — proporção bem acima da média global daquele ano, quando o perpetrador interno típico era descrito como profissional de nível júnior a pleno.

O perfil do fraudador brasileiro

Amostras e definições distintas em cada ponta; leitura indicativa, não série



Homens entre os fraudadores — 2015: série global · 2025: Brasil · **Cargos de gerência e acima** — 2015: Brasil, gerência média ou executiva · 2025: Brasil, de coordenador a presidente

Fonte: ACFE, Report to the Nations 2016; PwC, Crimes Econômicos 2016 — recorte Brasil; Grant Thornton Brasil, Diagnóstico das Fraudes no Brasil, 2025

87%
dos fraudadores brasileiros tinham entre 26 e 45 anos
Grant Thornton Brasil, Diagnóstico das Fraudes no Brasil, 2025

49%
estavam na empresa havia de um a cinco anos
Grant Thornton Brasil, Diagnóstico das Fraudes no Brasil, 2025

73%
agiram por ganho financeiro direto; 10%, para bater metas
Grant Thornton Brasil, Diagnóstico das Fraudes no Brasil, 2025

Leitura SCSDetect

O dado mais relevante para a segurança da informação não é demográfico, é o conluio. A escada de perdas por número de envolvidos atravessou a década sem mudar de forma — e conluio exige comunicação. Comunicação deixa rastro em aplicativos, em registros de acesso e, às vezes, no ar de uma sala de reunião. É por isso que a preservação forense de mensagens e a verificação técnica de dispositivos e ambientes deixaram de ser etapa opcional de uma investigação interna séria.

CAPÍTULO 3

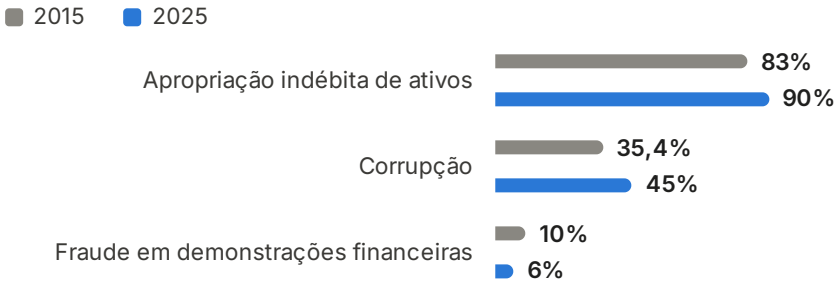
Como a fraude acontece

A apropriação de ativos é a mais comum e a mais barata. A corrupção é a que cresceu. A fraude contábil é a que arruína.

Os três grandes tipos de fraude ocupacional se comportam de maneira inversamente proporcional: quanto mais frequente o esquema, menor o prejuízo típico. A apropriação indébita de ativos aparece em nove de cada dez casos e custa US$ 100 mil na mediana; a fraude em demonstrações financeiras aparece em um caso a cada dezessete e custa dez vezes mais.

Em que proporção dos casos cada esquema aparece

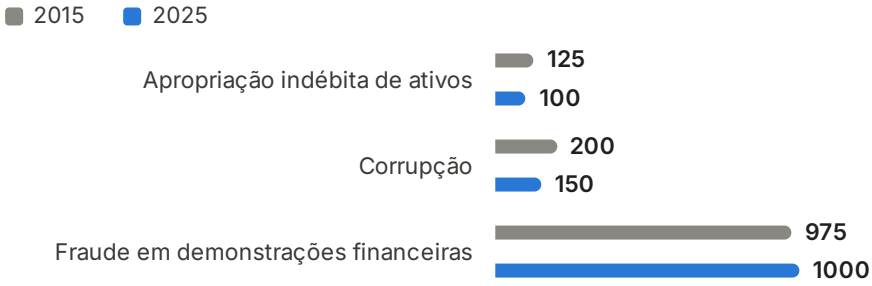
Um mesmo caso pode conter mais de um esquema, por isso a soma passa de 100%



Fonte: ACFE, Report to the Nations — edições 2016 e 2026

Perda mediana de cada esquema

Em milhares de dólares



A fraude em demonstrações financeiras é a mais rara e a mais cara — e foi a única cuja perda mediana subiu na década, de US$ 975 mil para US$ 1 milhão.

Fonte: ACFE, Report to the Nations — edições 2016 e 2026

Corrupção saltou de 10% dos casos em 1996 para 45% em 2025. É o único esquema que cresce década após década.

O esquema que mais cresceu

2015

35,4%

dos casos investigados envolviam corrupção — propina, conflito de interesses, extorsão econômica

ACFE, Report to the Nations 2016

2025

45%

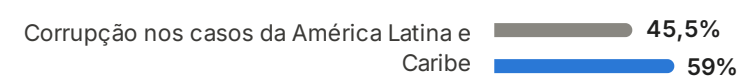
dos casos envolvem corrupção; em 1996, primeira edição da série, eram 10%

ACFE, Occupational Fraud 2026

Corrupção é o esquema em que o conluio é a regra, e não a exceção: por definição, envolve pelo menos duas partes.

Corrupção na América Latina

Proporção dos casos regionais que envolveram corrupção



A região sempre esteve acima da média global — 45,5% contra 35,4% em 2015; 59% contra 48% em 2024. A perda mediana regional também subiu: de US$ 174 mil para US$ 250 mil.

Fonte: ACFE, Report to the Nations 2016; ACFE, Occupational Fraud 2024

O movimento da corrupção é o mais consistente da série e o mais relevante para o Brasil: é o esquema que depende de um terceiro — fornecedor, cliente, intermediário ou agente público — e, portanto, o que mais se apoia em informação trocada fora dos sistemas da empresa.

Um em cada cinco processos de prova em investigações brasileiras já vem de aplicativos de mensagem.

Onde a fraude mora, no Brasil

Compras

é a área mais vulnerável apontada pelas empresas brasileiras, seguida de tesouraria, contas a pagar, faturamento e estoque

Grant Thornton Brasil, Diagnóstico das Fraudes no Brasil, 2025

34%

das provas em investigações brasileiras vêm da análise de transações; 21%, de sistemas de mensagens; 20%, de documentos

Grant Thornton Brasil, Diagnóstico das Fraudes no Brasil, 2025

58%

das fraudes em empresas brasileiras eram cometidas por agente interno em 2016, contra 46% na média global daquele ano

PwC, Crimes Econômicos 2016 — recorte Brasil

Leitura SCSDetect

A corrupção, ao contrário do desvio silencioso, é *negociada*: há reunião, telefonema, conversa em aplicativo. Ela é mais detectável por quem sabe onde procurar — e é por isso que verificação de ambientes e preservação forense deixaram de ser exceção nas apurações internas.

CAPÍTULO 4

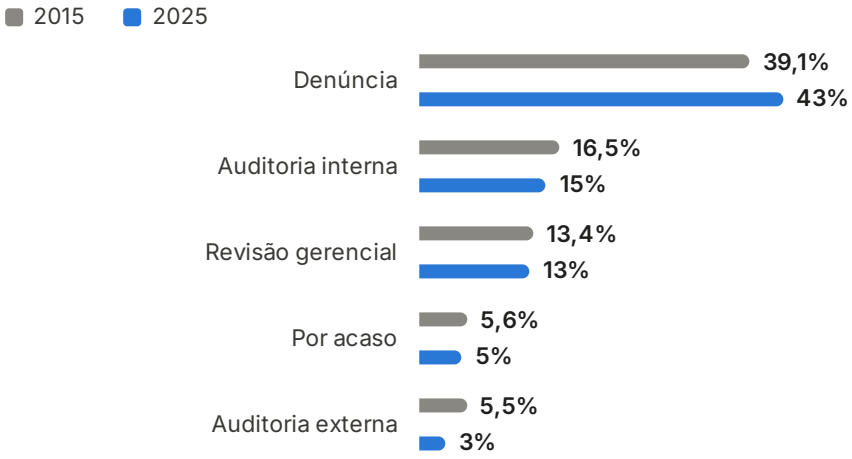
Como a fraude é descoberta

Em 2015, a auditoria externa descobria menos fraudes que o acaso. Dez anos depois, continua descobrindo.

A denúncia era o principal meio de detecção em 2015 e reforçou a posição em 2025. Nenhum outro canal chega perto: auditoria interna e revisão gerencial, somadas, descobrem dois terços do que a denúncia sozinha descobre, e a auditoria externa das demonstrações financeiras — o controle mais caro e mais universal — descobre menos de uma fraude em trinta.

Como as fraudes são descobertas

Proporção dos casos investigados; valores de 2025 para “por acaso” e “auditoria externa” são da edição 2024

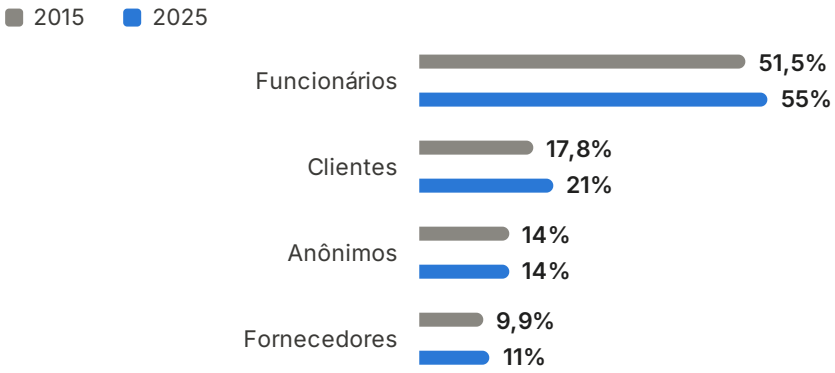


Em 2015, a auditoria externa descobria menos fraudes que o acaso. Dez anos depois, continua descobrindo.

Fonte: ACFE, Report to the Nations — edições 2016 e 2026; ACFE, Occupational Fraud 2024

Quem faz a denúncia

Proporção das denúncias recebidas



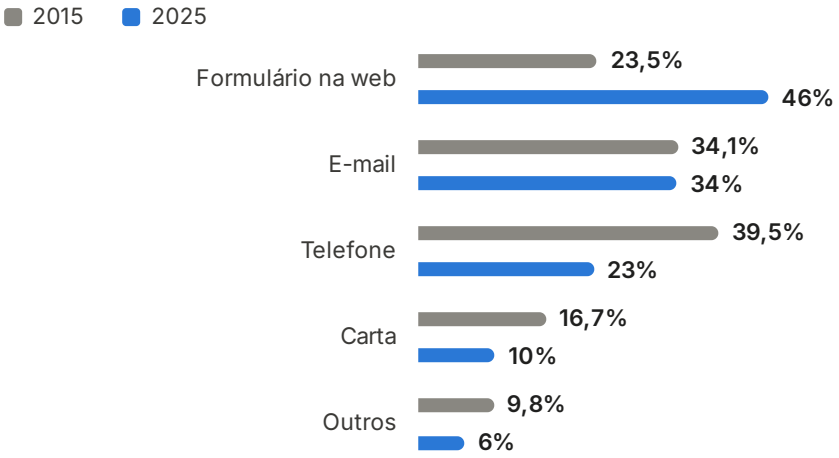
Quase um terço das denúncias vem de fora da empresa: 21% de clientes e 11% de fornecedores. Um canal aberto só a funcionários perde essa parcela.

Fonte: ACFE, Report to the Nations — edições 2016 e 2026

Quase um terço das denúncias vem de fora: de clientes e fornecedores. Um canal fechado a eles perde essa parcela.

O canal de denúncia trocou de meio

Meio usado pelo denunciante, entre as denúncias feitas por canal formal



Cada barra é independente: o denunciante podia usar mais de um meio, por isso a soma passa de 100% nas duas pontas. O telefone caiu de primeiro para terceiro lugar e o formulário na web dobrou de peso. Vale para as denúncias que passaram por canal formal — pouco mais da metade do total; as demais chegam informalmente, ao chefe direto ou à auditoria.

Fonte: ACFE, Report to the Nations — edições 2016 e 2026

O que muda quando existe canal de denúncia

2015

47,3%

das fraudes eram descobertas por denúncia nas organizações com canal formal, contra 28,2% nas que não tinham

ACFE, Report to the Nations 2016

2025

US$ 100 mil

é a perda mediana nas organizações com canal, contra US$ 150 mil sem canal; a detecção cai de 17 para 11 meses

ACFE, Occupational Fraud 2026

Em 2015, apenas 60,1% das organizações vítimas tinham canal de denúncia. Em 2025, o canal está presente em 85% das organizações com mais de cem funcionários — mas em apenas 24% das menores.

A troca de meio não é detalhe operacional. O denunciante que escreve deixa registro, anexa documento e pode permanecer anônimo com mais conforto do que ao telefone — e o volume de relatos anônimos cresceu junto. A contrapartida é que a apuração passa a depender de evidência digital preservada corretamente desde o primeiro momento.

No Brasil, dois em cada três relatos são anônimos — e mais da metade dos denunciados são gestores.

O canal de denúncia brasileiro em 2025

59%

das fraudes no Brasil só foram descobertas depois de uma denúncia

Grant Thornton Brasil, Diagnóstico das Fraudes no Brasil, 2025

64,7%

dos relatos recebidos pelos canais brasileiros em 2025 foram anônimos — o maior índice desde 2021

Aliant, 11ª Pesquisa Nacional de Canais de Denúncias, 2026

42 dias

é o tempo médio de apuração de uma denúncia no Brasil; 38 dias nos casos críticos

Aliant, 11ª Pesquisa Nacional de Canais de Denúncias, 2026

245.518

relatos foram recebidos pelos canais de denúncia analisados no Brasil em 2025

Aliant, 11ª Pesquisa Nacional de Canais de Denúncias, 2026

49,2%

dos relatos tratam de relacionamento interpessoal — assédio, discriminação, práticas abusivas

Aliant, 11ª Pesquisa Nacional de Canais de Denúncias, 2026

56,6%

dos denunciados são líderes e gestores; 66,8% dos denunciantes são colaboradores

Aliant, 11ª Pesquisa Nacional de Canais de Denúncias, 2026

O perfil dos relatos mudou junto com a década. Quando as pesquisas nacionais de canais de denúncia começaram, em 2015, o foco dos relatos era corrupção e fraude. Em 2025, quase metade do volume trata de relacionamento interpessoal — assédio moral, assédio sexual, discriminação e práticas abusivas. Parte da mudança é do fenômeno; parte é da lei, que passou a exigir canal para esse tipo de relato.

> **Leitura SCSDetect**
>
> Um canal de denúncia bem construído é o controle com melhor relação entre custo e resultado: as organizações que o tinham registraram perda mediana um terço menor e detecção seis meses mais rápida. Mas ele produz um efeito colateral que poucas empresas planejam: a apuração passa a depender de prova digital. Conversa em aplicativo, arquivo apagado, registro de acesso. Sem extração e preservação com método, a denúncia procedente vira demissão contestada na Justiça em vez de responsabilização.

CAPÍTULO 5

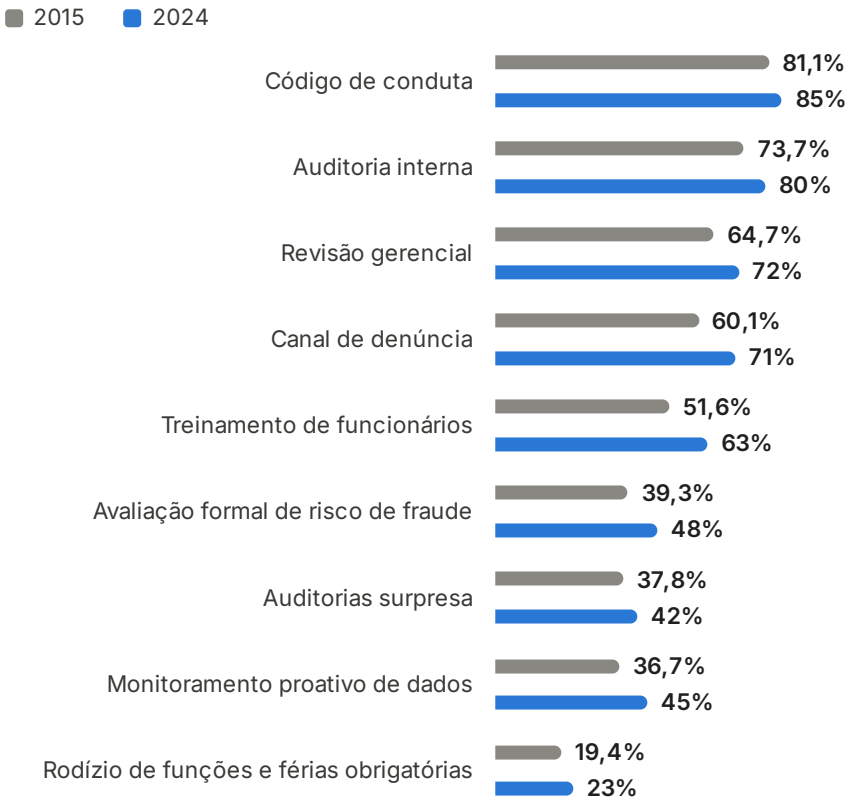
O que realmente funciona

Os controles mais difundidos não são os mais eficazes. Essa distorção atravessou a década inteira.

A pesquisa mede, para cada controle, a diferença de perda entre as organizações que o tinham e as que não o tinham. O resultado é o mesmo nas duas pontas da década — e é desconfortável: os controles que mais reduzem o prejuízo estão entre os menos adotados, enquanto o mais universal de todos é o que menos ajuda.

Quais controles antifraude as organizações têm

Prevalência nas organizações que sofreram fraude; valores de 2025 referentes à edição 2024 da pesquisa



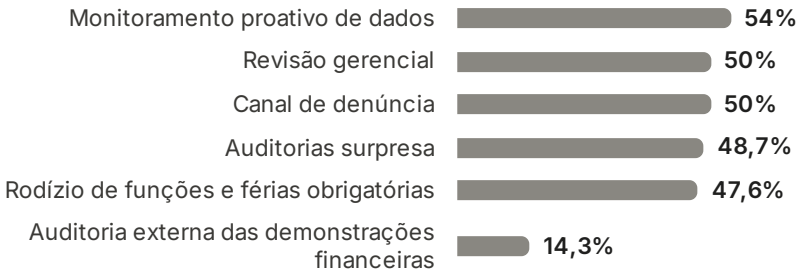
Todos os controles avançaram na década. Os que mais avançaram em pontos percentuais foram o treinamento de funcionários e o canal de denúncia.

Fonte: ACFE, Report to the Nations 2016; ACFE, Occupational Fraud 2024

A auditoria externa das demonstrações financeiras reduz a perda por fraude em 14%. Ela não foi desenhada para isso.

Quais controles mais reduziam a perda (2015)

Redução da perda mediana nas organizações que tinham o controle

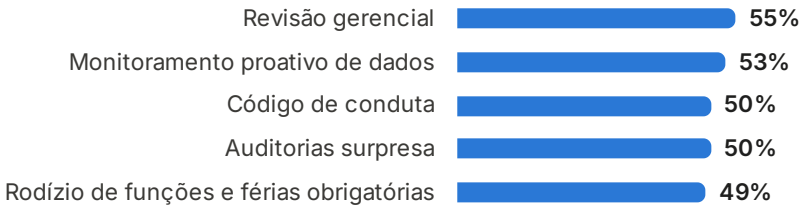


A ordem praticamente não mudou em dez anos. O controle mais caro e mais difundido — a auditoria externa das demonstrações financeiras — é o que menos reduz a perda por fraude, porque não foi desenhado para isso.

Fonte: ACFE, Report to the Nations 2016

Quais controles mais reduzem a perda (2025)

Redução da perda mediana nas organizações que tinham o controle



Fonte: ACFE, Occupational Fraud 2026

O efeito do treinamento

2015

51,6%

das organizações treinavam funcionários contra fraude

ACFE, Report to the Nations 2016

2025

US$ 84 mil

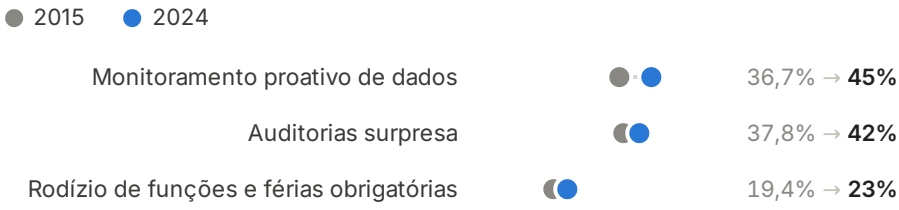
é a perda mediana onde há treinamento, contra US$ 150 mil onde não há — 44% menos

ACFE, Occupational Fraud 2026

Dez anos e a lacuna não fechou: o que funciona continua sendo o que menos se faz.

A lacuna que não fechou

Os três controles de maior efeito sobre a perda continuam entre os menos adotados



Monitoramento proativo de dados — o segundo controle mais eficaz, presente em menos da metade das organizações · **Auditorias surpresa** — corta a perda pela metade; quatro em cada dez organizações o adotam · **Rodízio de funções e férias obrigatórias** — o mais eficaz por real investido e o menos adotado de todos

Fonte: ACFE, Report to the Nations 2016; ACFE, Occupational Fraud 2024

Rodízio de funções e férias obrigatórias é o exemplo mais claro. É um controle que não exige sistema, licença nem consultoria — exige decisão. Reduz a perda mediana em quase metade e, em dez anos, saiu de 19% para 23% de adoção. O monitoramento proativo de dados, segundo controle mais eficaz, ainda não alcança metade das organizações.

> **Leitura SCSDetect**
>
> A lista dos controles eficazes tem um traço em comum: todos criam imprevisibilidade. Auditoria surpresa, rodízio de função, férias obrigatórias e monitoramento contínuo funcionam porque tiram do fraudador a certeza de que o esquema não será olhado hoje. A varredura eletrônica periódica opera pela mesma lógica no plano físico — e é o único controle capaz de responder à pergunta que nenhum sistema de *analytics* responde: alguém está ouvindo esta sala?

CAPÍTULO 6

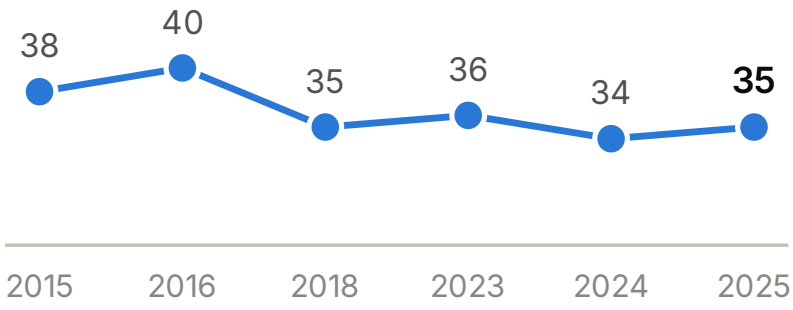
O Brasil na década

A infraestrutura de integridade cresceu sete vezes. A percepção de corrupção piorou três pontos.

Os dois movimentos brasileiros da década correm em direções opostas. De um lado, a régua de integridade subiu: a Lei Anticorrupção foi regulamentada em 2015, os acordos de leniência devolveram mais de R$ 10 bilhões e o número de empresas reconhecidas pelo programa de integridade do governo federal saiu de 19 para 128. De outro, a percepção de corrupção do país piorou: 38 pontos em 2015, 35 em 2025, sempre abaixo da média mundial.

Índice de Percepção da Corrupção — Brasil

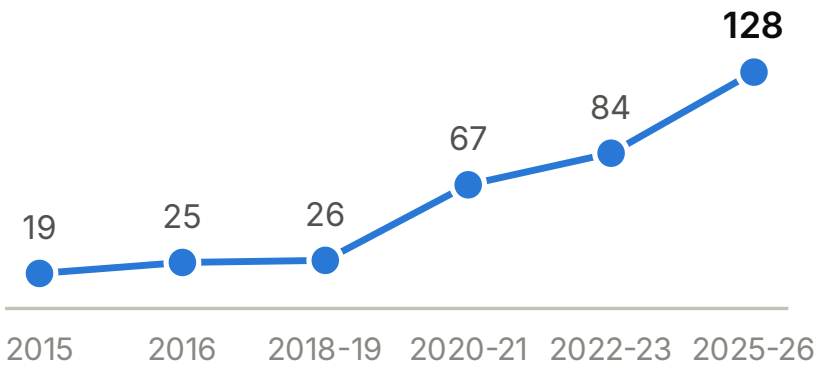
Pontuação de 0 a 100; a média mundial em 2025 foi 42



Fonte: Transparência Internacional, Índice de Percepção da Corrupção — 2015 e 2025

Empresas reconhecidas pelo Pró-Ética

Número de empresas aprovadas por ciclo de avaliação da CGU



Fonte: Instituto Ethos e CGU, Pró-Ética — ciclo 2015; CGU, Pró-Ética — ciclo 2025-2026

Sete vezes mais empresas com selo de integridade em dez anos — e ainda assim um universo pequeno para o tamanho da economia.

A posição do Brasil no ranking mundial

2015

76ª

posição entre 168 países avaliados, com 38 pontos — o Brasil foi o país que mais perdeu pontos naquele ano

Transparência Internacional, IPC 2015

2025

107ª

posição entre 182 países, com 35 pontos — abaixo da média mundial e da média das Américas, ambas em 42

Transparência Internacional, IPC 2025

A própria Transparência Internacional desaconselha comparar posições entre anos, porque o número de países avaliados muda. A nota é o indicador comparável: 38 em 2015, 35 em 2025.

32

acordos de leniência foram assinados pela CGU e pela AGU desde 2017 — o primeiro deles em julho daquele ano

CGU, acordos de leniência — maio de 2025

R$ 10 bi

foram efetivamente devolvidos aos cofres públicos por esses acordos até maio de 2025

CGU, acordos de leniência — maio de 2025

126

processos administrativos de responsabilização foram instaurados pela CGU só em 2025, num total de 539 desde 2020

CGU, balanço de processos administrativos de responsabilização, 2025

O enforcement também mudou de forma. O ciclo concentrado nas forças-tarefa penais encerrou-se em 2021; o que ficou foi o processo administrativo, mais silencioso e dirigido diretamente à empresa. Só em 2025 a Controladoria-Geral da União instaurou 126 processos de responsabilização, sendo as infrações mais frequentes a fraude em licitação, a obstrução à fiscalização e a oferta de vantagem indevida.

O risco de contraparte deixou de ser documental. Virou verificação de origem.

O crime organizado entrou na economia formal

R$ 146,8 bi

por ano é o faturamento estimado do crime organizado com produtos lícitos — combustíveis, bebidas, ouro e tabaco

Fórum Brasileiro de Segurança Pública, Follow the Products, 2025

R$ 107 bi

por ano é o que o crime custa à indústria brasileira: R$ 68,8 bi em prevenção e R$ 39,1 bi em perdas diretas

CNI, sondagem com 1.398 empresas — nov. de 2025

96%

dos profissionais de compliance veem o avanço do crime organizado como problema crescente; 57% têm controle específico para esse risco

Transparência Internacional Brasil, dez. de 2025

É a mudança mais brusca do período, e ela aconteceu quase toda nos últimos dois anos da década. Até 2024, a infiltração do crime organizado em empresas formais era tratada como hipótese. Em agosto de 2025, uma força-tarefa de Receita Federal, Polícia Federal e Ministério Público de São Paulo mostrou a cadeia inteira funcionando.

Operação Carbono Oculto e desdobramentos	O que foi apurado
28 de agosto de 2025 Receita Federal, Polícia Federal e MPSP	Mais de mil servidores cumpriram mais de 400 mandados em pelo menos oito estados. Foram bloqueados R$ 3,2 bilhões em bens nas operações Carbono Oculto, Quasar e Tank, com movimentação ilícita apurada de cerca de R$ 140 bilhões.
Setores alcançados	Cerca de mil postos de combustíveis, quatro refinarias, vinte e uma carteiras de fundos de investimento bloqueadas, 255 pessoas jurídicas e uma fintech operando como banco paralelo.
Resposta regulatória	No mesmo dia, a Receita Federal publicou instrução normativa que passou a exigir das fintechs as mesmas obrigações de informação das instituições financeiras tradicionais.
O que significa para a empresa	Fornecedor, cliente, distribuidor e até fundo de investimento passaram a ser pontos possíveis de contágio. A diligência de contraparte deixou de ser formalidade documental e virou verificação de origem.

Leitura SCSDetect

Para a empresa que não está no setor de combustíveis, a lição da Carbono Oculto não é sobre combustíveis. É sobre o que acontece quando a contraparte é fachada: a informação interna — rotas, estoques, contratos, condições comerciais, propostas em concorrência — passa a circular para fora junto com o relacionamento comercial. O risco de espionagem e o risco de infiltração deixaram de ser dois assuntos.

CAPÍTULO 7 · NOVO NESTA EDIÇÃO

Indicador 2026: exposição à espionagem corporativa

Não existe estatística oficial brasileira de espionagem corporativa. Existem sinais mensuráveis — e todos apontam na mesma direção.

Quatro sinais, uma leitura: a espionagem saiu da exceção estatística para a rotina operacional.

Este é o capítulo que a comparação 2015 × 2025 torna possível. Nenhum órgão brasileiro mede espionagem corporativa, e nenhuma pesquisa nacional pergunta a uma empresa se ela encontrou um dispositivo de escuta. O que existe são séries internacionais aplicadas com a mesma metodologia nas duas pontas da década, e elas permitem medir a direção e a velocidade do movimento. Reunimos as quatro mais consistentes.

SINAL 1 · ESCUTA NO LOCAL

8% → 12%

das empresas alemãs **constataram** escuta de reuniões ou telefonemas no próprio local. Outras 20% suspeitam ter sofrido — somadas, 32%. É a única série pública que mede o fenômeno de forma direta, mas as duas pontas não são estritamente comparáveis: 2015 conta só o que foi constatado, em janela de dois anos; 2025 conta doze meses e separa constatação de suspeita.

Bitkom, Wirtschaftsschutz — edições 2015 e 2025

SINAL 2 · INCIDÊNCIA GERAL

51% → 87%

das empresas alemãs foram vítimas de espionagem, sabotagem ou roubo de dados. O prejuízo estimado para a economia do país saiu de € 51 bilhões por ano para € 289,2 bilhões.

Bitkom, Wirtschaftsschutz — edições 2015 e 2025

SINAL 3 · PESSOAS DE DENTRO

4,5×

foi o aumento do custo anual dos incidentes causados por pessoas de dentro: de US$ 4,3 milhões por organização em 2015 para US$ 19,5 milhões em 2025, com média de 25 incidentes por organização no ano.

Ponemon, custo dos incidentes internos — edições 2016 e 2026

SINAL 4 · QUEM ESTÁ POR TRÁS

3% → 28%

das empresas alemãs atacadas atribuíram ao menos um ataque a um serviço de inteligência estrangeiro. Em 2015, os autores apontados eram sobretudo funcionários e ex-funcionários, com 52%.

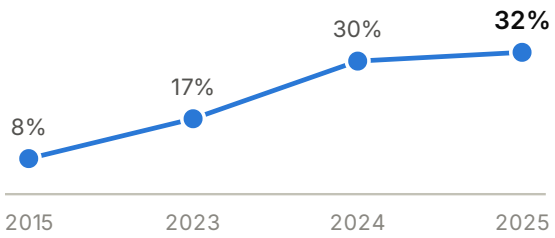
Bitkom, Wirtschaftsschutz — edições 2015 e 2025

Tendências

Nenhum dos quatro sinais aponta para baixo. Dois deles mais que triplicaram.

Alvos de escuta de reuniões ou telefonemas no local

% de empresas alemãs; de 2023 em diante inclui suspeita, e em 2025 a constatação isolada é 12%

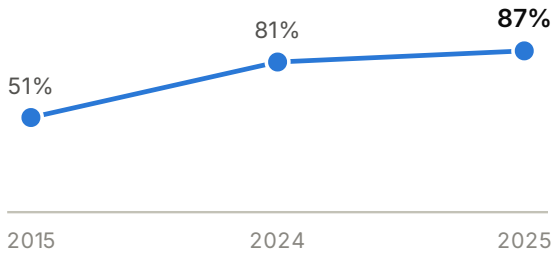


A edição de 2015 registrava apenas o que as empresas constataram, em janela de dois anos; as recentes somam constatação e suspeita em doze meses. A linha indica direção, não é série estritamente comparável.

Fonte: Bitkom, Wirtschaftsschutz — edições 2015 e 2025; edições de 2023 e 2024

Empresas vítimas de espionagem, sabotagem ou roubo de dados

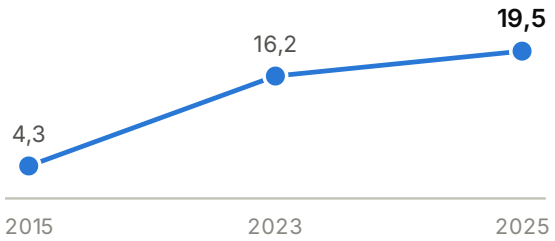
% do total, Alemanha



Fonte: Bitkom, Wirtschaftsschutz — edições 2015 e 2025

Custo anual dos incidentes por pessoas de dentro

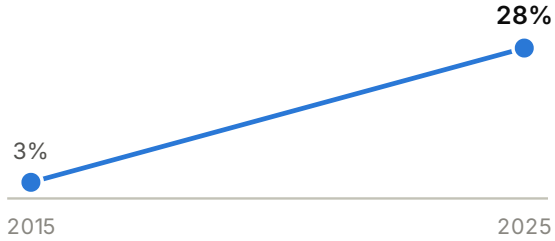
US$ milhões por organização, média global



Fonte: Ponemon, custo dos incidentes internos — edições 2016 e 2026

Ataques atribuídos a serviço de inteligência estrangeiro

% das empresas alemãs atacadas que apontaram essa origem



Fonte: Bitkom, Wirtschaftsschutz — edições 2015 e 2025

A série alemã é a única no mundo que pergunta diretamente, e da mesma forma há dez anos, se a empresa foi alvo de escuta no próprio local. Ela mede empresas alemãs, não brasileiras — e por isso serve como indicador de direção, não como medida do Brasil. O objetivo da pesquisa SCSDetect 2027 é produzir a medida nacional que hoje não existe.

2º

lugar do Brasil no ranking mundial de vítimas de stalkerware — software espião instalado em celulares — em todos os anos de 2020 a 2023

Kaspersky, State of Stalkerware — 2020 a 2023

R$ 7,19 mi

é o custo médio de uma violação de dados no Brasil em 2025; a cadeia de fornecedores é o vetor mais caro, com R$ 8,98 milhões

IBM, Cost of a Data Breach 2025 — recorte Brasil

362

comunicações de incidentes de segurança chegaram à ANPD em 2025 — quase uma por dia; eram 186 em 2021

ANPD, incidentes de segurança — 2021 a 2025

A exposição é alta e cresce onde a empresa menos olha: nas pessoas, nos telefones e nas salas de reunião.

Leitura SCSDetect

1 **A escuta no local voltou a ser um vetor relevante — e é o menos monitorado.**

É o dado mais surpreendente da década: um indicador que estava em 8% em 2015 chegou a 32% em 2025. Transmissores com conexão celular, gravadores em stand-by, que só transmitem em determinados horários e microfones do tamanho de uma moeda custam menos que um jantar de negócios e são vendidos sem controle. Não há estatística pública de taxa de achados em varreduras, aqui ou fora. O que existe são estimativas de prática profissional divulgadas por quem presta o serviço — a mais citada, da consultoria americana Murray Associates, fala em 2% a 5% das varreduras emergenciais, sem declarar amostra nem período. Tratamos isso como ordem de grandeza de mercado, não como medida.

2 **Mudou quem está por trás.**

Em 2015, os autores apontados eram principalmente funcionários e ex-funcionários, com 52%; serviços de inteligência estrangeiros apareciam em apenas 3% dos casos. Em 2025, o crime organizado é apontado por 68% das empresas atacadas e os serviços estrangeiros por 28%. A espionagem deixou de ser um desvio de conduta individual e virou atividade de organização — com orçamento, método e escala.

3 **O celular é o novo cofre, e o Brasil é campeão de vigilância nele.**

O segundo lugar do Brasil no ranking mundial de *stalkerware*, repetido em todos os anos da série, revela um mercado nacional maduro de software espião: o mesmo aplicativo usado contra um cônjuge é usado contra um executivo. A verificação técnica dos dispositivos de diretores, conselheiros e advogados passou a ser higiene básica de segurança, não serviço extraordinário.

4 **A pessoa de dentro continua sendo o canal de saída preferido da informação.**

O custo anual dos incidentes causados por pessoas de dentro multiplicou-se por quatro e meio em dez anos, e a média chegou a 25 incidentes por organização ao ano. A inteligência artificial acrescentou um vazamento novo e silencioso: uma em cada cinco organizações relatou violação envolvendo uso não autorizado de ferramentas de IA, e apenas 37% têm política para detectá-lo. No Brasil, esses incidentes comprometeram dados pessoais em 65% dos casos e propriedade intelectual em 40% — e é a propriedade intelectual que raramente aparece em notificação regulatória.

CASOS RECENTES

O que aconteceu no Brasil

Episódios documentados em decisões judiciais, comunicados oficiais ou imprensa de referência.

Quando	Caso	O que ensina
2017 a 2025	**Operação Spy.** Servidores da Receita Federal e do Ministério do Desenvolvimento extraíam do Siscomex dados sigilosos de comércio exterior — importações por CNPJ, fornecedores, clientes, volumes, preços, prazos — e os revendiam em relatórios ao setor privado. Até janeiro de 2025, a CGU havia condenado 36 empresas compradoras, com multas somando R$ 46 milhões.	Comprar inteligência de mercado de fonte ilícita é ato lesivo à administração pública. O comprador responde objetivamente, pela Lei Anticorrupção.
2018 a 2021	**Sistema FirstMile na Abin.** Contrato de R$ 5,7 milhões com fornecedor israelense deu à agência a capacidade de geolocalizar celulares explorando vulnerabilidades das redes 2G e 3G. A Polícia Federal concluiu o inquérito em junho de 2025 com mais de trinta indiciados e cerca de 60 mil acessos considerados irregulares.	Capacidade de vigilância fora de controle alcança executivos, advogados e jornalistas que orbitam a empresa.
jun. 2025	**Ataque à C&M Software.** Um funcionário de tecnologia vendeu login, senha e informações de estrutura por R$ 15 mil. Em cinco horas de madrugada, 166 transações desviaram R$ 541 milhões de uma única instituição cliente.	O maior ataque ao sistema financeiro brasileiro não explorou falha técnica: explorou uma pessoa dentro de um fornecedor.
nov. 2025	**Segredo industrial no TJSP.** Ex-empregado com cargo estratégico e acordo de confidencialidade passou a atuar em concorrente, que adotou métodos e características da antiga empregadora. O tribunal reconheceu concorrência desleal do empregado e da empresa e determinou cessação imediata do uso.	O desligamento é o momento de maior risco para o segredo de negócio — e a via judicial brasileira é cível, com prova difícil.
2020 a 2023	**Stalkerware.** O Brasil foi o segundo país do mundo em vítimas de software espião instalado em celulares em todos os anos da série: mais de 6.500 em 2020, 4.807 em 2021, 4.969 em 2022 e 4.186 em 2023, concentrando cerca de três quartos das vítimas latino-americanas.	O mesmo aplicativo vendido para vigiar um cônjuge serve para vigiar um diretor. O celular pessoal é o ponto cego do programa de segurança.

O que diz a lei brasileira

O Brasil não tem um tipo penal de espionagem corporativa. A proteção está distribuída entre concorrência desleal, crimes informáticos, interceptação e proteção de dados — e, na maior parte dos casos, com penas brandas e prova difícil. O crime de espionagem criado em 2021 protege segredo de Estado, não segredo

de empresa. Isso desloca o peso para a prevenção e para a qualidade da evidência: sem prova técnica preservada, a maioria dos casos não passa da suspeita.

Norma	Conduta	Pena ou sanção
Lei 9.279/1996 (Propriedade Industrial), art. 195, incisos IX a XII	Concorrência desleal: dar ou receber vantagem para que empregado de concorrente traia o dever do emprego; divulgar, explorar ou utilizar sem autorização conhecimentos, informações ou dados confidenciais a que se teve acesso por relação contratual ou empregatícia, ainda que após o fim do contrato, ou obtidos por meios ilícitos.	Detenção de 3 meses a 1 ano, ou multa. Ação penal privada; a reparação corre na esfera cível.
Código Penal, art. 154-A Lei 12.737/2012, alterada pela Lei 14.155/2021	Invadir dispositivo informático para obter, adulterar ou destruir dados, ou instalar vulnerabilidades. A mesma pena alcança quem produz, vende ou distribui o programa usado na invasão.	Reclusão de 1 a 4 anos e multa; de 2 a 5 anos quando resulta em obtenção de segredos comerciais ou industriais ou em controle remoto do dispositivo.
Lei 9.296/1996, art. 10 redação da Lei 13.869/2019	Interceptar comunicações telefônicas, de informática ou telemática, ou promover escuta ambiental, sem autorização judicial.	Reclusão de 2 a 4 anos e multa.
Código Penal, arts. 153 e 154	Divulgação de segredo contido em documento ou correspondência confidencial e violação de segredo profissional.	Detenção de 1 a 6 meses ou multa; de 3 meses a 1 ano ou multa.
Lei 13.709/2018 (LGPD), arts. 48 e 52	Dever de comunicar incidentes de segurança à ANPD e aos titulares; sanções ao controlador que falha na proteção dos dados pessoais.	Multa de até 2% do faturamento, limitada a R$ 50 milhões por infração.
Lei 12.846/2013 (Anticorrupção)	Responsabilidade objetiva da pessoa jurídica por atos contra a administração pública — inclusive a compra de informação sigilosa de servidores, como na Operação Spy.	Multa de 0,1% a 20% do faturamento bruto, publicação da decisão e acordos de leniência.
Código Penal, art. 359-K Lei 14.197/2021	Obter ou divulgar indevidamente segredo de Estado ou informação sensível de defesa, segurança, inteligência ou relações exteriores.	Reclusão de 3 a 12 anos. **Protege segredo de Estado, não segredo empresarial** — não existe tipo penal autônomo de espionagem corporativa no Brasil.

Como medir a exposição na sua organização

Propomos que o conselho e a diretoria acompanhem, ao menos anualmente, um conjunto simples de indicadores de contrainteligência, ao lado dos indicadores de fraude já consolidados.

Indicador	Como medir	Referência de boa prática
Cobertura de varredura	% de salas críticas e veículos executivos verificados nos últimos 12 meses	100% ao ano; e antes de reuniões decisivas

Tempo desde a última varredura	Dias decorridos por ambiente crítico	Até 180 dias em ambientes de alta sensibilidade
Dispositivos móveis verificados	% de smartphones da alta administração verificados quanto a spyware no período	Semestral, e após viagens sensíveis ou suspeita
Achados e falsos positivos	Dispositivos, anomalias de radiofrequência e vulnerabilidades físicas por varredura, com classificação de criticidade	Registro histórico por ambiente
Incidentes internos e tempo de contenção	Número de incidentes envolvendo pessoas de dentro e dias até a contenção	Referência global de 2025: 25 incidentes por ano
Desligamentos de risco	% de saídas com acesso a informação sensível em que revogação de acessos, devolução de ativos e preservação forense se concluíram no mesmo dia	100%
Uso não autorizado de IA	Existência de política de detecção e número de eventos de exposição de dados em ferramentas de IA generativa	Em 2025, apenas 37% das organizações tinham política

Pesquisa SCSDetect 2027

Para que a próxima edição deste relatório traga uma medida brasileira de exposição à espionagem corporativa, a SCSDetect conduzirá em 2027 uma pesquisa confidencial com empresas de todos os portes, cobrindo incidência de escutas, vazamentos por pessoas de dentro, verificação de dispositivos e práticas de contrainteligência. A participação é anônima e os resultados agregados serão publicados. Interessados podem manifestar-se pelos contatos ao final deste documento.

CAPÍTULO 8 · NOVO NESTA EDIÇÃO

O que a prevenção evita — o outro lado da conta

Todo o resto deste relatório conta o que deu errado. Este capítulo conta o que foi barrado — e quanto custa barrar.

Um relatório de fraude tem um viés embutido: ele só enxerga o que aconteceu. A fraude impedida não vira caso, não entra em pesquisa e não aparece em nenhuma mediana. Reunimos aqui as poucas séries públicas que medem o outro lado — tentativas barradas, ataques sem sucesso e a diferença observada entre organizações que têm controles e organizações que não têm.

Uma advertência antes dos números. Nenhum dado desta seção prova que a prevenção *causou* a redução. Todos são de dois tipos: contagens feitas por quem vende a detecção, ou comparações entre grupos que se autosselecionaram — empresas com mais controles costumam ser maiores, mais reguladas e mais maduras, e essas características também reduzem perda. Onde a fonte usa linguagem de associação, nós usamos também.

O Pix é o raro caso em que o custo do falso positivo é público: R$ 26,5 bilhões travados para devolver R$ 1,38 bilhão.

O melhor dado brasileiro de prevenção é do Banco Central

18,2 mi

bloqueios cautelares de Pix suspeitos foram aplicados em 2025 — uma contagem administrativa do universo completo, não uma amostra

Banco Central, dados abertos do Pix — estatísticas de fraude e MED, jan. a dez. de 2025

R$ 1,38 bi

voltaram ao pagador a partir desses bloqueios: 3,19 milhões deles se confirmaram fraude, 17,5% do total

Banco Central, dados abertos do Pix — estatísticas de fraude e MED, jan. a dez. de 2025

R$ 26,5 bi

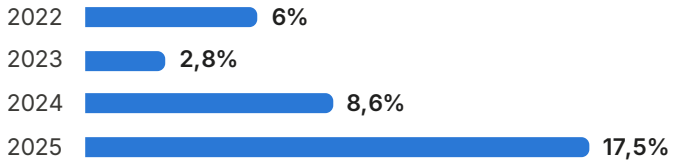
foram bloqueados e depois liberados — transações legítimas que passaram por atrito. É o preço do erro da prevenção

Banco Central, dados abertos do Pix — estatísticas de fraude e MED, jan. a dez. de 2025

O bloqueio cautelar do Pix é, entre tudo o que consultamos, o dado mais sólido: não é amostra nem estimativa, é a contagem administrativa do sistema inteiro. E é o único que publica os dois lados da balança — quanto a prevenção recupera e quanto ela trava indevidamente. Dos R$ 27,9 bilhões bloqueados preventivamente em 2025, R$ 26,5 bilhões eram de transações legítimas, liberadas depois.

Quanto do bloqueio preventivo se confirma fraude

Proporção dos bloqueios cautelares de Pix que terminaram em devolução ao pagador



O acerto do bloqueio subiu, mas a leitura exige cautela: o período coincide com mudanças de regra do Mecanismo Especial de Devolução e com uma quebra de série em outubro de 2025. É associação no tempo, não efeito medido de melhora dos modelos.

Fonte: Banco Central, dados abertos do Pix — estatísticas de fraude e MED, jan. a dez. de 2025

Leitura SCSDetect

Nenhum relatório comercial de segurança publica seu índice de falso positivo. O Banco Central publica. É por isso que este é o número que recomendamos ao conselho que peça de qualquer fornecedor de prevenção: não apenas quanto foi barrado, mas quanto foi barrado *à toa* — porque esse é o custo que a operação paga todo dia.

No e-commerce, a tentativa de fraude tem ticket médio duas vezes maior que a compra legítima.

O que foi barrado antes de virar prejuízo

2,3 mi

tentativas de fraude foram identificadas e barradas no e-commerce brasileiro em 2025

Serasa Experian, Mapa da Fraude no e-commerce — pedidos analisados de jan. a dez. de 2025

R$ 2,4 bi

em prejuízo deixaram de acontecer com essas tentativas barradas — cerca de um pedido suspeito a cada cem analisados

Serasa Experian, Mapa da Fraude no e-commerce — pedidos analisados de jan. a dez. de 2025

R$ 1.058

é o ticket médio da tentativa fraudulenta, contra R$ 539 da compra legítima: o fraudador tenta levar o dobro

Serasa Experian, Mapa da Fraude no e-commerce — pedidos analisados de jan. a dez. de 2025

O número do e-commerce tem uma virtude e uma limitação. A virtude: a fonte diz, sem rodeio, que as tentativas foram identificadas e barradas, e estima o prejuízo que não aconteceu. A limitação: o denominador nunca é divulgado — não se sabe quantos pedidos foram analisados no total —, e o valor evitado é o valor nominal dos pedidos recusados, sem descontar os legítimos recusados por engano.

3.501

ataques por semana, em média, sofreu cada organização monitorada na América Latina — 27% a mais que um ano antes

Check Point Research, volume médio de ataques por organização — junho de 2026

84%

das notificações de incidentes ao CERT.br em 2025 foram varreduras e tentativas malsucedidas contra serviços expostos

CERT.br, notificações de incidentes — ano de 2025

5.391

anúncios de aparelhos de espionagem foram retirados do ar pelo regulador alemão em 2024, em 2.640 investigações abertas

Bundesnetzagentur (Alemanha), fiscalização de aparelhos de espionagem — ano de 2024

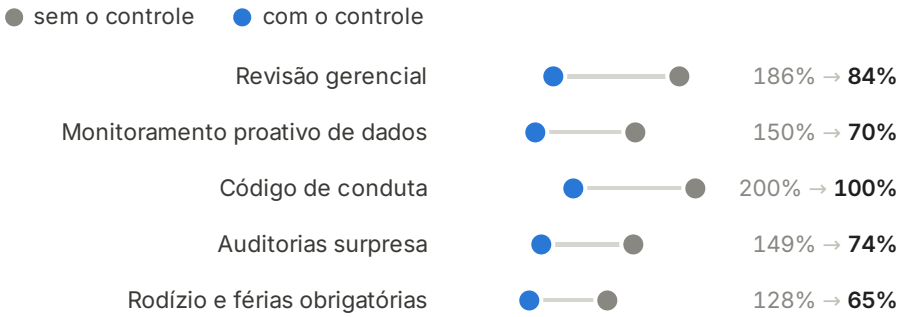
Sobre o dado do CERT.br: a instituição classifica como varredura as tentativas malsucedidas contra serviços expostos, e como invasão os ataques bem-sucedidos. Em 2025 foram 393.919 varreduras contra 3.729 invasões. A proporção **não** é uma taxa de sucesso dos atacantes: varreduras são notificadas automaticamente em massa, invasões são subnotificadas por razão reputacional. Serve para mostrar a composição do que se notifica, não a realidade do que se tenta.

Os três controles com maior diferença de perda são justamente os três menos adotados.

A diferença entre ter e não ter o controle

Perda mediana nas organizações sem o controle e com o controle

Em milhares de dólares; ordenado pela diferença entre as duas situações

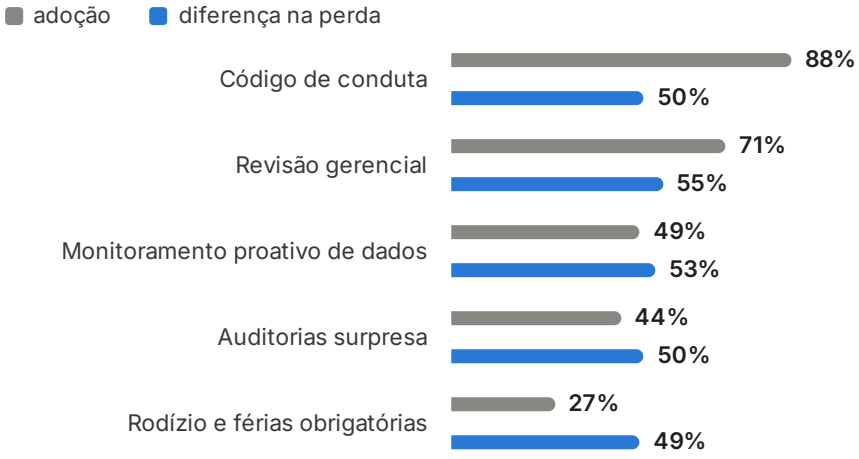


Revisão gerencial — presente em 71% dos casos · **Monitoramento proativo de dados** — presente em 49% · **Código de conduta** — presente em 88% · **Auditorias surpresa** — presente em 44% · **Rodízio e férias obrigatórias** — presente em 27%

Fonte: ACFE, Occupational Fraud 2026 — figuras 27 a 29

O descompasso entre o que se adota e o que funciona

Cinza: proporção das organizações que têm o controle · Azul: diferença percentual na perda mediana



Os três controles ligados às maiores diferenças de perda — monitoramento proativo, auditorias surpresa e rodízio de funções — são justamente os menos adotados. O código de conduta, quase universal, é o que menos separa os dois grupos.

Fonte: ACFE, Occupational Fraud 2026 — figuras 27 a 29

O efeito do treinamento antifraude

SEM TREINAMENTO

US$ 150 mil

foi a perda mediana nas organizações que não treinavam nem funcionários nem gestores

ACFE, Occupational Fraud 2026 — seção de treinamento antifraude

COM TREINAMENTO

US$ 84 mil

foi a perda mediana onde os dois grupos eram treinados — e o funcionário treinado tem o dobro da chance de fazer a denúncia que descobre a fraude

ACFE, Occupational Fraud 2026 — seção de treinamento antifraude

O achado mais útil desta página não está em nenhuma linha isolada, e sim no cruzamento das duas primeiras. Monitoramento proativo de dados, auditorias surpresa e rodízio de funções com férias obrigatórias aparecem associados às maiores diferenças de perda mediana — e estão entre os controles menos implantados, presentes em 49%, 44% e 27% das organizações. A lacuna se concentra nas empresas com menos de cem funcionários, que é o perfil da maior parte do parque empresarial brasileiro: entre elas, o canal de denúncia existe em 24% dos casos, contra 85% nas maiores.

> **Leitura SCSDetect**
>
> Há uma assimetria que vale nomear: mede-se o que é regulado. Do lado do consumo — Pix, e-commerce, identidade digital — o Brasil tem dados de prevenção oficiais e granulares. Do lado corporativo, não existe nenhum. Por isso a varredura eletrônica não aparece em tabela alguma desta página: não há estatística pública de taxa de achados, aqui ou fora. É essa lacuna que a pesquisa SCSDetect 2027 pretende começar a preencher.

CAPÍTULO 9 · NOVO NESTA EDIÇÃO

A década que mudou o risco 2015 – 2025

Os números do relatório se moveram porque estas coisas aconteceram. Trinta marcos, em quatro eixos.

Nenhum dos indicadores deste relatório se moveu sozinho. A queda do tempo de detecção, o crescimento da denúncia, a explosão do custo dos incidentes internos e o salto da escuta no local são consequência de decisões legislativas, operações policiais, incidentes e mudanças tecnológicas que podem ser datadas. Esta é a cronologia — em quatro eixos, com fonte para cada marco na lista de referências.

Integridade: de atenuante a condição de contrato

A Lei Anticorrupção entrou em vigor em janeiro de 2014, mas foi a regulamentação de 2015 que transformou "programa de integridade" de conceito em lista auditável. Dez anos depois, sem programa comprovado não há contrato público de grande vulto nem reabilitação após sanção.

Quando	O que aconteceu	Por que importa para a empresa
mar. 2015	**Decreto 8.420 regulamenta a Lei Anticorrupção.** Fixou dezesseis parâmetros de avaliação do programa de integridade: comprometimento da alta direção, código de conduta, treinamentos, análise de risco, controles contábeis, canais de denúncia, monitoramento e transparência em doações políticas.	Foi o momento em que o compliance virou checklist auditável pelo poder público.
jun. 2016	**Lei das Estatais.** A Lei 13.303 passou a exigir das estatais código de conduta, área de conformidade, auditoria interna ligada ao conselho, comitê de auditoria estatutário e treinamento anual.	Estendeu a exigência às maiores compradoras do país.
jul. 2017	**Primeiro acordo de leniência federal.** CGU e AGU assinaram com uma construtora o primeiro acordo com base na Lei 12.846: R$ 500 milhões, pagos ao longo de 22 anos.	Abriu a via negocial que se tornou a principal forma de encerrar risco corporativo.
2017 a 2019	**Os estados criam suas próprias exigências.** Rio de Janeiro, Distrito Federal, Espírito Santo, Amazonas, Rio Grande do Sul, Mato Grosso e Pernambuco passaram a exigir programa de integridade de quem contrata com o estado acima de determinados valores.	Criou um mosaico de obrigações estaduais quatro anos antes da exigência federal.
fev. 2021	**Encerra-se o ciclo das forças-tarefa.** A força-tarefa da Lava Jato no Paraná foi absorvida pelo Gaeco do Ministério Público Federal, com balanço de 79 fases, 533 denunciados, 17 acordos de leniência nos quais foi negociada a devolução de cerca de R$ 15 bilhões — dos quais cerca de R$ 4,3 bilhões efetivamente recuperados até então.	O risco migrou do processo penal concentrado para o administrativo difuso.
abr. 2021	**Nova Lei de Licitações.** A Lei 14.133 passou a obrigar o vencedor de contratações de grande vulto a implantar programa de integridade em seis meses.	Compliance deixou de ser atenuante e virou condição contratual.
jul. 2022	**Decreto 11.129 sobe a régua.** Substituiu o decreto de 2015 e passou a exigir, de forma explícita, diligência sobre terceiros, verificação em fusões e aquisições e independência da instância de integridade.	A diligência de fornecedor deixou de ser cláusula e virou processo.

dez. 2024	**Decreto 12.304 fecha o ciclo.** Regulamentou a comprovação do programa de integridade em contratos de grande vulto, como critério de desempate em licitação e em pedidos de reabilitação após sanção.	Sem programa comprovado, não há contrato nem reabilitação.
mai. 2025	**R$ 10 bilhões devolvidos.** A CGU anunciou 32 acordos de leniência assinados desde 2017 e mais de R$ 10 bilhões efetivamente devolvidos aos cofres públicos.	Consolida a leniência como principal canal de resolução de risco.
dez. 2025	**Novas regras de leniência.** Portaria conjunta da CGU e da AGU criou o mecanismo de reserva de benefício durante investigação interna, critérios objetivos de cálculo e redução de até dois terços por autodenúncia.	Abriu janela formal para autodenúncia após fusões e aquisições.

Dados: de ativo sem dono a passivo regulado

Em 2015 não havia lei geral de proteção de dados no Brasil, nem autoridade, nem dever de comunicar incidentes. Dez anos depois há tudo isso — e uma agência reguladora com poder de sanção.

Quando	O que aconteceu	Por que importa para a empresa
mai. 2016	**Decreto regulamenta o Marco Civil da Internet.** Impôs padrões técnicos de segurança: controle estrito de acesso, autenticação dupla, registros detalhados de quem acessou o quê e quando, e criptografia.	Primeira norma brasileira a exigir controles técnicos de segurança de empresas privadas.
ago. 2018	**A LGPD é sancionada.** A Lei 13.709 entrou em vigor em setembro de 2020 e suas sanções administrativas passaram a valer em agosto de 2021.	Tratamento irregular de dados deixou de ser risco reputacional e virou risco financeiro.
nov. 2020	**Lançamento do Pix.** Em cinco anos o sistema alcançou 170 milhões de adultos e mais de 20 milhões de empresas.	Criou, em um lustro, a maior superfície de fraude do país.
jan. 2021	**Megavazamento de 223 milhões de CPFs.** Veio a público uma base com dados de praticamente toda a população brasileira: nome, nascimento, gênero e, em versões pagas, documento, renda, score de crédito, endereço e parentes.	A base de identidade do país inteiro está comprometida — dado cadastral deixou de servir como fator de autenticação.
mai. 2021	**Lei 14.155 cria a fraude eletrônica.** Elevou a pena da invasão de dispositivo informático e criou o furto e o estelionato mediante fraude eletrônica, ambos com reclusão de 4 a 8 anos.	Deu à fraude digital pena comparável à do roubo.
out. 2022	**A ANPD vira autarquia.** A autoridade ganhou autonomia funcional para fiscalizar, e não apenas orientar.	Deu dentes à lei sancionada quatro anos antes.
jul. 2023	**Primeira sanção da ANPD.** Advertência e duas multas contra uma microempresa que ofertava listas de contatos, por tratamento sem base legal e por não atender à requisição da autoridade.	Estabeleceu que não cooperar com a requisição é infração autônoma.
dez. 2023	**Política Nacional de Cibersegurança.** Instituiu a política e um comitê nacional com assento para o setor empresarial.	Primeira moldura de governança com participação formal das empresas.
jun. 2025	**O maior ataque ao sistema financeiro brasileiro.** Credenciais legítimas, vendidas por um funcionário de tecnologia de um fornecedor por R$ 15 mil, permitiram desviar R$ 541 milhões de uma instituição em cinco horas de madrugada.	O elo mais fraco não foi o sistema: foi uma pessoa dentro de um fornecedor.

set. 2025	**O fornecedor de tecnologia vira entidade regulada.** Resolução do Banco Central criou o credenciamento dos prestadores de serviços de tecnologia do sistema financeiro, com capital mínimo, certificação de segurança, auditoria externa anual e planos de continuidade testados.	Resposta direta ao ataque de junho: terceirizar tecnologia deixou de terceirizar o risco.

Crime organizado: da hipótese à operação

Até meados da década, a infiltração de facções em empresas formais era tratada como hipótese acadêmica. Entre 2024 e 2025 ela virou operação policial, com valores, setores e nomes.

Quando	O que aconteceu	Por que importa para a empresa
abr. 2024	**Operação Fim da Linha.** O Ministério Público de São Paulo mirou duas viações acusadas de lavar dinheiro de facção; foram bloqueados mais de R$ 600 milhões. As empresas transportavam cerca de 700 mil passageiros por dia.	Primeira demonstração em escala de crime organizado operando como concessionário de serviço público.
fev. 2025	**O crime na economia lícita é dimensionado.** Estudo do Fórum Brasileiro de Segurança Pública estimou em R$ 146,8 bilhões por ano o faturamento do crime organizado com quatro produtos lícitos: combustíveis, bebidas, ouro e tabaco.	Colocou o tema na agenda corporativa ao mostrar que o dinheiro do crime circula em setores formais.
ago. 2025	**Operações Carbono Oculto, Quasar e Tank.** Força-tarefa de mais de mil servidores cumpriu mais de 400 mandados em oito estados, bloqueou R$ 3,2 bilhões em bens e apurou cerca de R$ 140 bilhões movimentados, envolvendo mil postos, quatro refinarias, 21 carteiras de fundos e uma fintech operando como banco paralelo.	Fornecedor, cliente, distribuidor e fundo de investimento passaram a ser pontos possíveis de contágio.
ago. 2025	**As fintechs entram no mesmo regime das instituições financeiras.** No mesmo dia da operação, a Receita Federal passou a exigir das fintechs as obrigações de informação das instituições financeiras tradicionais.	Fechou a brecha regulatória usada para mover dinheiro dentro do sistema formal.
nov. 2025	**A indústria mede o que o crime lhe custa.** Sondagem com 1.398 empresas de 32 setores apurou R$ 107 bilhões por ano: R$ 68,8 bilhões em prevenção e segurança e R$ 39,1 bilhões em perdas diretas.	Quantifica o custo que a empresa já paga hoje, e não o risco hipotético.

Tecnologia: o vetor mudou três vezes em dez anos

Ransomware, trabalho remoto e inteligência artificial generativa redesenharam o caminho do ataque — cada um em menos de cinco anos.

Quando	O que aconteceu	Por que importa para a empresa
nov. 2020	**Ransomware paralisa um tribunal superior.** O acervo inteiro de processos foi criptografado e a instituição ficou cerca de sete dias sem operar. O que salvou foram os backups, que não haviam sido atingidos.	Primeiro caso brasileiro de alto perfil em que ransomware parou uma instituição inteira.
mai. 2021	**Resgate milionário no agronegócio.** Uma companhia de controle brasileiro confirmou o pagamento de US$ 11 milhões em bitcoin após ataque que atingiu plantas nos Estados Unidos e na Austrália — mesmo já tendo restaurado os sistemas.	Pagar deixou de ser questão de recuperar dados e virou questão de evitar vazamento.

mar. 2022	**A pandemia entra nos números da fraude.** A pesquisa global de fraude ocupacional registrou que cerca de metade dos casos analisados foi afetada pela pandemia: o trabalho remoto abriu oportunidades novas e, ao mesmo tempo, forçou o reforço de controles.	A dispersão física dos controles alterou a estrutura da fraude, não apenas o seu volume.
nov. 2023	**O deepfake chega ao Brasil.** Levantamento com mais de dois milhões de tentativas de fraude registrou alta de 830% em deepfakes no Brasil entre 2022 e 2023, com o país concentrando quase metade dos casos da América Latina.	Primeiro ano em que a IA generativa aparece nos números brasileiros de fraude.
2024 e 2025	**A escalada da fraude sintética.** O Brasil passou a registrar incidência de deepfake cinco vezes maior que a dos Estados Unidos e dez vezes maior que a da Alemanha, com alta de 126% em 2025 e cerca de 39% de todos os deepfakes identificados na América Latina.	O vetor migrou de documento falsificado para rosto e voz sintéticos.
jul. 2025	**A IA não autorizada entra na conta.** Uma em cada cinco organizações relatou violação envolvendo uso não autorizado de ferramentas de IA, e apenas 37% tinham política para detectá-lo. No Brasil, esses incidentes comprometeram dados pessoais em 65% dos casos e propriedade intelectual em 40%.	O dado pessoal vazado gera notificação à ANPD; a propriedade intelectual vazada não gera registro nenhum.

O que isso significa para 2026

Os quatro eixos convergem para o mesmo ponto. A integridade virou condição contratual; os dados viraram passivo regulado; o crime organizado entrou na cadeia de fornecimento; e a tecnologia colocou rosto e voz sintéticos ao alcance de qualquer fraudador. Nos quatro casos, a informação da empresa — quem são os fornecedores, qual é o preço-limite, o que foi decidido na última reunião de conselho — passou a valer mais para terceiros do que o dinheiro em caixa. É essa mudança de alvo que o capítulo anterior mede.

QUEM PRODUZIU ESTE RELATÓRIO

A SCSDetect

Detectar. Localizar. Neutralizar.

Suas conversas mais sensíveis não podem vazar.

A SCSDetect é uma empresa brasileira de contrainteligência corporativa. Desde 2008, realiza varreduras eletrônicas e físicas para detectar dispositivos de escuta, câmeras ocultas, rastreadores e software espião em ambientes, veículos, linhas e celulares de organizações que não podem permitir que suas conversas vazem.

Atuamos para conselhos e diretorias, escritórios de advocacia, instituições financeiras, órgãos públicos e residências de executivos — em São Paulo, Rio de Janeiro, Brasília e, sob demanda, em todo o território nacional.

Serviços

Varredura de ambientes (TSCM)

Espectro de radiofrequência, junção não linear (NLJD), câmera térmica e inspeção física.

Varredura de dispositivos móveis

Detecção de *spyware* e *stalkerware*, permissões e indicadores de comprometimento.

Varredura veicular

Carros executivos e blindados: rastreadores GPS, transmissores e gravadores em stand-by.

Varredura de telefonia fixa

Linhas analógicas, digitais e VoIP, cabeamento, quadros e centrais.

Apoio forense a investigações

Extração e preservação de conversas e dados com cadeia de custódia.

Programas contínuos

Calendário de varreduras, verificação prévia de reuniões críticas e atendimento emergencial em até 4 horas.

A varredura atesta a condição do ambiente no momento da inspeção. Por isso a periodicidade importa mais do que o equipamento.

O que detectamos

Câmeras ocultas, escutas e grampos, rastreadores GPS, dispositivos em stand-by (que só transmitem em determinados horários), transmissores ocultos e por corrente portadora, IMSI catchers, microfones a laser e *spyware* em celulares.

Como trabalhamos

Independência

Não comercializamos equipamentos de segurança eletrônica: o laudo não é um orçamento disfarçado.

Dois laudos

Um executivo e um técnico, detalhados no anexo desta publicação.

Confidencialidade

Comunicação e servidores criptografados, equipe nominal no laudo, processos alinhados à LGPD e à ISO/IEC 27001.

Quando uma empresa nos procura

Situação	O que costuma estar em jogo
Negociação em curso	Fusões e aquisições, concorrências, acordos societários e disputas em que a proposta, o preço-limite ou a estratégia jurídica não podem chegar ao outro lado antes da hora.
Vazamento já ocorrido	Informação confidencial que reaparece fora da empresa, concorrente que antecipa propostas, decisão interna conhecida antes da comunicação oficial. Aqui a varredura é também coleta de evidência.
Investigação interna	Apuração de denúncia, conflito de interesses ou desvio, em que as reuniões do comitê e os dispositivos das pessoas envolvidas precisam estar limpos e as provas, preservadas.
Rotina de governança	Programa periódico de verificação das áreas críticas, com registro histórico por ambiente — o formato que permite ao conselho acompanhar o indicador de exposição descrito no capítulo 7.

ANEXO TÉCNICO

Metodologia de varredura eletrônica

Uma varredura que só procura o que transmite encontra menos da metade do que existe.

A varredura de contramedidas eletrônicas (TSCM, na sigla em inglês) combina camadas independentes. Cada uma cobre uma classe de dispositivo que as outras não enxergam — razão pela qual uma inspeção baseada apenas em “detectores de escuta” portáteis oferece falsa segurança.

Camada	O que faz	O que só ela encontra
Análise de espectro de RF Analisadores em tempo real e radiogoniometria	Mapeia o espectro do ambiente, compara com a linha de base da região e localiza a origem de emissões anômalas, inclusive em faixas celulares e Wi-Fi.	Transmissores ativos, inclusive GSM/4G, Wi-Fi e Bluetooth disfarçados de equipamento comum.
Detecção por junção não linear (NLJD)	Emite um sinal e identifica a resposta característica de semicondutores, mesmo em dispositivos desligados ou sem bateria.	Dispositivos em stand-by, gravadores desligados e eletrônicos embutidos em paredes, móveis e forros.
Imagem térmica	Identifica assinaturas de calor de componentes eletrônicos em operação atrás de superfícies.	Equipamentos ocultos em estruturas, alimentados pela rede elétrica.
Análise de telefonia	Testa linhas analógicas, digitais e VoIP, cabeamento e quadros quanto a derivações, impedâncias anômalas e dispositivos em série.	Grampos na infraestrutura de telefonia e em cabos estruturados.
Inspeção física	Desmontagem controlada de tomadas, luminárias, detectores, mobiliário, quadros e itens de decoração; conferência de inventário de equipamentos.	Gravadores autônomos sem emissão, câmeras a pilha e itens de origem desconhecida no ambiente.
Verificação de dispositivos móveis	Análise de aplicativos, perfis de configuração, permissões, consumo de dados e indicadores de comprometimento.	*Spyware* e *stalkerware* instalados no aparelho da própria vítima.

Quando varrer

- **Periodicamente**, em salas de conselho, diretoria, jurídico, M&A e P&D — recomendamos intervalo máximo de seis meses em ambientes de alta sensibilidade.
- **Antes de eventos críticos:** reuniões de conselho, negociações de fusão ou aquisição, definição de propostas em concorrências, audiências e apurações internas.
- **Após mudanças de ocupação:** novas instalações, reformas, manutenção de ar-condicionado, cabeamento ou elétrica executadas por terceiros.
- **Sob suspeita concreta:** informações confidenciais que reaparecem fora da empresa, concorrente que antecipa propostas, vazamento de decisões ainda não comunicadas.
- **Em desligamentos sensíveis:** saída de executivos, disputas societárias e litígios de alta exposição.

O que fazer ao suspeitar

- **Não fale sobre a suspeita no ambiente suspeito.** Se houver um dispositivo, a conversa sobre a varredura será a primeira coisa que ele vai capturar.
- **Não procure sozinho.** Manipular um dispositivo destrói vestígios e inviabiliza a perícia — e a maioria dos "detectores" de consumo não encontra o que importa.
- **Combine a varredura por canal externo** (telefone pessoal, fora das instalações) e com o menor número possível de pessoas informadas.
- **Preserve o ambiente** como está até a chegada da equipe técnica e **trate o achado como evidência:** documentação fotográfica, laudo técnico e cadeia de custódia são o que transforma a descoberta em ação legal possível.

O que o laudo entrega

Relatório executivo

Escopo e ambientes verificados, resumo dos achados com classificação de criticidade, conclusão objetiva sobre a integridade de cada ambiente e recomendações priorizadas — no formato em que um conselho ou uma diretoria decide.

Relatório técnico

Instrumentação utilizada e respectiva calibração, registros de espectro e capturas de tela, fotografias datadas, metodologia por camada, linha de base de radiofrequência do local e cadeia de custódia dos itens recolhidos — o documento que sustenta uma ação judicial.

Limites do método

Nenhuma varredura oferece garantia permanente: ela atesta a condição do ambiente no momento da inspeção. Um dispositivo pode ser instalado no dia seguinte, e por isso a periodicidade e o controle de acesso importam mais do que qualquer equipamento isolado. Da mesma forma, a varredura de ambientes não substitui os controles de segurança da informação em redes e sistemas — ela cobre exatamente a lacuna que esses controles não alcançam: o espaço físico, o espectro de radiofrequência e os aparelhos pessoais.

REFERÊNCIAS

Fontes e referências

Todo dado deste relatório tem origem identificada. Nenhum número foi estimado pela SCSDetect.

Os endereços eletrônicos foram verificados em setembro de 2026. As observações de comparabilidade estão indicadas junto a cada gráfico ao longo do documento. Onde as duas pontas da comparação vêm da mesma pesquisa aplicada com a mesma metodologia, isso está dito no texto.

A série comparável 2015 × 2025

- ACFE — Association of Certified Fraud Examiners. *Report to the Nations on Occupational Fraud and Abuse — 2016 Global Fraud Study*. 2.410 casos em 114 países, investigados entre janeiro de 2014 e outubro de 2015. acfe.com/fraud-resources/report-to-the-nations
- ACFE. *Occupational Fraud 2024: A Report to the Nations*. 1.921 casos em 138 países, incluindo 93 na América Latina e Caribe.
- ACFE. *Occupational Fraud 2026: A Report to the Nations*. 2.402 casos em 143 países, investigados entre janeiro de 2024 e setembro de 2025.
- Transparência Internacional. *Índice de Percepção da Corrupção*, edições 2015 e 2025 (esta publicada em fevereiro de 2026). transparency.org/en/cpi e transparenciainternacional.org.br
- Bitkom. *Spionage, Sabotage und Datendiebstahl — Wirtschaftsschutz im digitalen Zeitalter*, 2015 (1.074 empresas alemãs) e, com o Bundesamt für Verfassungsschutz, *Wirtschaftsschutz* 2023, 2024 e 2025 (1.002 empresas na última edição). bitkom.org
- Ponemon Institute. *Cost of Insider Threats*, 2016; e Ponemon Institute com DTEX Systems, *2026 Cost of Insider Risks — Global Report*, campo encerrado em setembro de 2025, 354 organizações.
- IBM Security e Ponemon Institute. *Cost of a Data Breach Report*, edições 2016 (média global) e 2025 (com recorte Brasil). ibm.com/reports/data-breach

Brasil: fraude, integridade, corrupção e crime organizado

- PwC. *Pesquisa Global sobre Crimes Econômicos 2016* — edição global (6.337 respondentes em 115 países) e recorte Brasil; e *Global Economic Crime Survey 2024*, recorte Brasil. pwc.com.br
- Kroll. *Global Fraud & Risk Report 2016/2017* — recorte Brasil, mais de cinquenta executivos.
- Grant Thornton Brasil. *Diagnóstico das Fraudes no Brasil*, divulgado em 2025, referente aos últimos doze meses. grantthornton.com.br
- Aliant. *Pesquisa Nacional de Canais de Denúncias* — 1ª edição (2015) e 11ª edição (2026, com 245.518 relatos de 2025).
- LEC — Legal Ethics Compliance. *Anuário Compliance on Top 2024*.
- Instituto Ethos e Controladoria-Geral da União. *Programa Pró-Ética* — ciclos de 2015 a 2025-2026. gov.br/cgu
- Controladoria-Geral da União. Balanço dos acordos de leniência (maio de 2025), *Operação Spy* (janeiro de 2025) e processos administrativos de responsabilização (2025).
- Transparência Internacional Brasil. Pesquisa com profissionais de compliance sobre crime organizado e integridade, dezembro de 2025.

- Fórum Brasileiro de Segurança Pública. *Follow the Products*, 2025 (ano-base 2022).
- Confederação Nacional da Indústria. Sondagem com 1.398 empresas de 32 setores, campo em novembro de 2025.
- Receita Federal, Polícia Federal e Ministério Público de São Paulo. Operações *Carbono Oculto*, *Quasar* e *Tank*, agosto de 2025.
- Autoridade Nacional de Proteção de Dados. Comunicações de incidentes de segurança, série de 2021 a 2025.
- Serasa Experian. Tentativas de fraude de janeiro a setembro de 2025. Febraban, prejuízo com golpes, balanço de 2024.

Espionagem, vazamento de dados e ameaça interna

- Verizon. *Data Breach Investigations Report*, edições 2015, 2016 e 2026. verizon.com/business/resources/reports/dbir
- Kaspersky. *State of Stalkerware*, edições de 2020 a 2023 — a mais recente cobre dados de 2023. securelist.com
- Sumsub. *Identity Fraud Report*, edições 2023 e 2025. Check Point Software, *Global Ransomware Report 2024*.
- The IP Commission. *Update to the IP Commission Report*. National Bureau of Asian Research, 2017.
- Murray Associates. Estimativa de prática profissional sobre achados em varreduras de contramedidas emergenciais, publicada pela própria consultoria, sem amostra, período ou metodologia declarados. counterespionage.com

Legislação e regulação

- Brasil. *Lei nº 9.279/1996* (Propriedade Industrial), art. 195; *Lei nº 9.296/1996*, art. 10; *Código Penal*, arts. 153, 154, 154-A e 359-K.
- Brasil. *Lei nº 12.846/2013* (Anticorrupção); *Decreto nº 8.420/2015* e *Decreto nº 11.129/2022*; *Lei nº 13.303/2016*; *Lei nº 14.133/2021* e *Decreto nº 12.304/2024*; *Lei nº 14.230/2021*.
- Brasil. *Lei nº 12.965/2014* (Marco Civil da Internet) e *Decreto nº 8.771/2016*; *Lei nº 13.709/2018* (LGPD); *Lei nº 14.155/2021*; *Lei nº 14.197/2021*; *Lei nº 14.460/2022*.
- Banco Central do Brasil. Resolução BCB nº 498, de setembro de 2025, sobre prestadores de serviços de tecnologia da informação do sistema financeiro.

FALE COM A SCSDETECT

Contatos

Atendimento emergencial sob suspeita de escuta: resposta em até 4 horas.

Para avaliação de exposição, agendamento de varredura, apoio a investigações internas ou participação na pesquisa SCSDetect 2027.

Comercial e agendamento
(11) 2539-0001
(11) 95328-4126 (WhatsApp)
contato@scsdetect.com

Responsável pelo relatório
Rodrigo Alves — COO
Varredura eletrônica e contrainteligência
contato@scsdetect.com

São Paulo — matriz
Alameda Santos, 1827
Cerqueira César · 01419-002
São Paulo/SP

Rio de Janeiro e Brasília
Atendimento regional
e operações em todo o território nacional
sob demanda

SCSDetect
scsdetect.com
Contrainteligência corporativa desde 2008

GrupoSCS
gruposcs.com.br
A SCSDetect é uma empresa do GrupoSCS

Relatório Anual 2026 · Fraude e espionagem corporativa no Brasil · Publicado em setembro de 2026.

Aviso

As informações aqui apresentadas são de natureza geral e não tratam das circunstâncias de nenhum indivíduo ou entidade específica. A SCSDetect emprega os melhores esforços na exatidão do que reproduz, sem garantir que permaneça correto no futuro. Os dados citados são de autoria das instituições identificadas em cada gráfico e no capítulo de fontes; a SCSDetect não tem relação com elas. Este documento não constitui aconselhamento jurídico: nenhuma ação deve ser tomada com base nele sem orientação profissional qualificada.

Reprodução

SCSDetect

Se a informação vale, alguém já pensou em ouvi-la.

A varredura só encontra o que está lá. A decisão de procurar é sua — e costuma ser tomada depois do primeiro vazamento, quando o prejuízo já aconteceu.

Agende uma avaliação de exposição das suas áreas críticas: salas de conselho e diretoria, jurídico, M&A, P&D, veículos executivos e dispositivos da alta administração.

SCSDetect

Alameda Santos, 1827 — São Paulo/SP · Rio de Janeiro · Brasília

(11) 2539-0001 · (11) 95328-4126 (WhatsApp)

contato@scsdetect.com · scsdetect.com

Uma empresa do GrupoSCS · gruposcs.com.br