BRANDEFENSE COUNTRY REPORT · BRAZIL 2026

# Brandefense Brasil: Relatório do Panorama de Ameaças Cibernéticas 2026

Identidades, autorização de pagamentos e continuidade de serviços em uma economia conectada

Odin by Brandefense
Período da pesquisa: 1 de janeiro a 22 de novembro de 2026
Versão 1.0 · Edição Pública de Pesquisa · TLP:CLEAR · 8 a 22 de novembro de 2026

**131 de 250**
domínios selecionados tinham uma credencial associada anunciada à venda na verificação

**10**
casos selecionados de alegações com trechos autênticos e anonimizados

**206**
listagens de ransomware associadas ao Brasil durante o período

**30 / 60 / 90**
dias para validação, controles exercitados e revisão da gestão

SUMÁRIO

# Sumário

**Translated with AI**

Esta edição foi traduzida com IA a partir do original em inglês. Em caso de divergência, prevalece a edição em inglês.


| | | |
|---|---|---|
| 01 | Resumo executivo | 05 |
| | Mapa do relatório | 10 |
| 02 | Contexto digital e operacional do Brasil | 11 |
| 03 | Exposição nacional: um conjunto selecionado de 250 domínios | 15 |
| 04 | Atividade na dark web: do anúncio à decisão com responsável | 22 |
| 05 | Incidentes e atividade por setor | 39 |
| 06 | Interrupções, desfiguração de sites e confiança nos serviços públicos | 58 |
| 07 | Ransomware, grupos com motivação financeira e espionagem | 64 |
| 08 | Fraude, dados pessoais e material de cartões de pagamento | 78 |
| 09 | Bancos e pagamentos: proteger a autorização para agir | 84 |
| 10 | Regulação e resposta nacional | 91 |
| 11 | Perspectivas e planejamento condicional | 96 |
| 12 | Plano de ação | 100 |
| A | Apêndice A. Escopo e limites das evidências | 107 |
| B | Apêndice B. Registro de evidências | 112 |
| C | Apêndice C. Fontes | 117 |
| D | Apêndice D. Glossário | 122 |

| | |
|---|---|
| Conselho e executivos | 01 05 11 12 |
| CISO e liderança de segurança | 03 04 05 07 12 |
| SOC, endpoints e identidade | 04 06 07 B |
| Pagamentos, fraude e proteção dos clientes | 05 08 09 |
| Jurídico e comunicação | 05 06 10 12 |

# Sobre esta edição

**Traduzido com IA.** Esta edição em português brasileiro foi traduzida do original em inglês. Em caso de divergência, prevalece a edição em inglês.

Preparado com auxílio de IA. Evidências, atribuições e limitações acompanham as conclusões.

As evidências brasileiras conectam cópia de dados cadastrais, ofertas de acesso, fraude em pagamentos e recuperação administrativa. A prioridade é validar a autorização afetada e proteger o serviço essencial e seus usuários.

## 206

listagens de ransomware associadas ao Brasil; alegações, não invasões confirmadas

## 80/100 (F)

indicador nacional do Atlas para o conjunto selecionado de 250 domínios

## 26

casos analisados; dez alegações e dezesseis casos de divulgação ou investigação

## 4

decisões para a liderança, todas ligadas a evidências de conclusão

# Sumário e caminhos de leitura


| Capítulo | Pergunta |
|---|---|
| 1 Resumo executivo | Quais decisões devem vir primeiro? |
| 2 Contexto brasileiro | Quais condições operacionais orientam a resposta? |
| 3 Exposição nacional | O que o conjunto selecionado permite afirmar? |
| 4 Atividade na dark web | O que os anúncios realmente dizem? |
| 5 Incidentes por setor | O que organizações e autoridades relataram? |
| 6 Interrupções e confiança | O serviço ficou indisponível, foi alterado ou apenas citado? |
| 7 Atores e campanhas | Quais rótulos e relações têm evidências de apoio? |
| 8 Fraude e dados pessoais | Como informações podem sustentar outra solicitação prejudicial? |
| 9 Bancos e pagamentos | Quem controla a autorização para agir? |
| 10 Regulação | Qual entidade, condição e canal de comunicação se aplicam? |
| 11 Perspectivas | Quais cenários condicionais justificam preparação? |
| 12 Plano de ação | Quem age e o que demonstra a conclusão? |
| Apêndices A–D | Escopo, registro de evidências, fontes e definições simples |

CAPÍTULO 01

# Resumo executivo

01

ESTE CAPÍTULO RESPONDE

Quais conclusões justificam decisões imediatas para organizações brasileiras?

**206**

listagens de ransomware, cada uma registrando uma alegação de extorsão


Seis conclusões 06

Quatro decisões para a liderança 07

O ano em números 07

O que permanece indisponível 08

CAPÍTULO 01

# Resumo executivo

EM RESUMO

As evidências sustentam quatro prioridades: validar identidades, proteger a autorização de pagamentos, envolver fornecedores e testar a continuidade. Comunicados descrevem cópia de cadastros, alteração de instruções de pagamento e recuperação administrativa. A Ransompedia registra 206 listagens associadas ao Brasil, sob 55 rótulos de grupos. Pesquisas técnicas descrevem separadamente malware bancário, roubo de identidades de pagamento e espionagem atribuída. São populações distintas, sem um total nacional de ataques. Designe responsáveis pelo acesso atual, pela proteção dos clientes, pelo serviço mínimo e pelas comunicações.

Este relatório combina observações do Brandefense Blackhole, listagens da Ransompedia, resultados de exposição do Atlas para domínios selecionados e informações públicas verificadas. Publicações, anúncios, listagens, casos públicos e associações de registros são unidades diferentes. Não são somados em um total nacional de ataques. [S1][S2][S3][S4]

A data de corte solicitada é 22 de novembro. As evidências refletem o que estava disponível durante a verificação naquele dia, ainda em andamento. A quinzena final aparece separadamente em §5.7. Publicação, incidente, descoberta e recuperação mantêm datas distintas.

## Seis conclusões

**1. A visibilidade da extorsão se distribui entre muitos rótulos.** A Ransompedia registra 206 listagens associadas ao Brasil no período, ante 160 em todo o ano de 2025. Thegentlemen, Lockbit5 e INC Ransom somam 72, ou 35,0%, das listagens atuais. As outras 134 pertencem a 52 rótulos. A comparação não representa crescimento anual entre períodos equivalentes nem confirma criptografia. [S2]

**2. A exposição cadastral exige uma resposta própria aos clientes.** A CVP confirma cópia de dados cadastrais em uma base que inclui seus 7,6 milhões de clientes ativos, além de antigos clientes. O Tesouro identifica aproximadamente 30.000 cadastros de serviços e outra base com cerca de 4.000 chaves Pix. Nenhum comunicado permite somar pessoas únicas nacionalmente ou presumir acesso a pagamentos. [S126][S127]

**3. A integridade do pagamento pode falhar em um fluxo legítimo.** Belo Horizonte informa que algumas guias emitidas entre 14 e 16 de novembro apresentavam dados de pagamento alterados. Cerca de 250 contribuintes pagaram guias afetadas. A prefeitura afirma que os valores foram bloqueados e as devoluções começaram em 17 de novembro. O comunicado não confirma todas as devoluções nem uma invasão da infraestrutura nacional do Pix. [S233][S234]

**4. Recuperação administrativa e operação física exigem testes separados.** Santos descreve um incidente em 6 de novembro e recuperação por etapas. A APS afirma que a capacidade de cargas e os acessos foram mantidos, enquanto a imprensa descreve lentidão administrativa. São medidas diferentes. Teste a tarefa essencial do usuário, a alternativa operacional e a conciliação posterior. [S128][S229][S228]

**5. Um anúncio de acesso precisa de validação antes da contenção.** As publicações selecionadas alegam possuir contatos financeiros, registros educacionais, dados municipais e acesso relacionado a pagamentos. Um anúncio de Pix publicado em novembro identifica o material como sendo de 2025. Uma narrativa de assistente virtual publicada em fevereiro contém datas inconsistentes. Esses detalhes justificam análise, sem confirmar uma nova invasão. [S1]

**6. As pesquisas sobre atores sustentam perguntas de controle distintas.** A pesquisa do Google sobre pagamentos, a análise da Elastic sobre malware bancário e a pesquisa da IBM sobre sessões sustentam controles separados. A Kaspersky inclui o Brasil em uma campanha de roubo de informações e espionagem, atribuída ao Armored Likho com confiança moderada. Nenhuma delas estabelece um operador comum entre os casos. [S18][S19][S20][S161]

## Quatro decisões para a liderança

1. **Valide as evidências de identidade e acesso.** Atribua cada alerta relevante a um serviço da organização, verifique situação e privilégios da conta e registre a contenção ou o encerramento. Registros históricos exigem resposta diferente de um acesso atual inseguro (§3–4, §12).
2. **Proteja a autorização de transações.** Mapeie identidades de assinatura, permissões de fornecedores e aprovação de mudanças de beneficiário. Demonstre revogação e verificação independente com transações simuladas (§5, §9, §12).
3. **Integre fornecedores e proteção dos clientes na resposta.** Identifique o controlador, o responsável pelo serviço, as categorias afetadas e o canal confiável de atendimento. Simule uma comunicação incompleta de incidente por um fornecedor (§5, §8, §10).
4. **Teste o serviço mínimo e as comunicações em conjunto.** Demonstre uma alternativa, concilie seus registros e preserve a cronologia de ciência para cada obrigação aplicável (§6, §10, §12).

## O ano em números

| 206 | 160 | 55 |
|---|---|---|
| Listagens da Ransompedia associadas ao Brasil no período de 2026 | Listagens associadas ao Brasil em todo o ano de 2025 | Rótulos de grupos nas listagens do período atual |
| O QUE NÃO MEDE | O QUE NÃO MEDE | O QUE NÃO MEDE |
| Invasões confirmadas, criptografia ou pagamento | Uma base de comparação de período equivalente | Operadores únicos ou organizações criminosas |

## 72 de 206

Listagens dos três principais rótulos, 35,0%

O QUE NÃO MEDE

Sua participação em todos os incidentes brasileiros

## 102 / 41 / 74 / 108

Listagens do período para Argentina / Chile / Colômbia / México

O QUE NÃO MEDE

Risco ajustado à população ou desempenho de segurança nacional

## 250

Domínios principais avaliados em dez grupos setoriais

O QUE NÃO MEDE

Entidades jurídicas independentes ou prevalência nacional de exposição

## 80/100 (F)

Indicador nacional do Atlas para o conjunto selecionado

O QUE NÃO MEDE

Percentual de violações, probabilidade de invasão ou classificação setorial

## 131 de 250

Domínios selecionados com uma credencial associada anunciada à venda na verificação

O QUE NÃO MEDE

Acesso testado, venda concluída ou invasão confirmada

## 26

Casos do relatório: dez alegações e dezesseis casos de divulgação ou investigação

O QUE NÃO MEDE

Vinte e seis invasões confirmadas

## 7,6 milhões

População de clientes ativos da CVP incluída na base afetada

O QUE NÃO MEDE

Total de pessoas únicas, incluindo antigos clientes

## Cerca de 30.000 / 4.000

Cadastros de serviços / chaves Pix do Tesouro em bases distintas

O QUE NÃO MEDE

Um total combinado de pessoas ou transferências autorizadas

## Cerca de 250

Contribuintes que, segundo a prefeitura, pagaram guias alteradas

O QUE NÃO MEDE

Todos os contribuintes ou pagamentos municipais

Os países de comparação foram selecionados como exemplos apenas para fornecer contexto; a sua escolha não implica uma classificação nem uma avaliação política.

Fontes: observações próprias [S1][S2][S3], comunicados oficiais [S126][S127][S233] e seus respectivos escopos. Os agregados de cartões são discutidos somente com seu escopo restrito em §8.2.

## O que permanece indisponível

O Atlas fornece indicador nacional de 80/100 (F) para o conjunto selecionado. Não há conjunto completo de higiene passiva nem índice de higiene disponível. Observações ausentes de controles não representam falhas. Não são publicadas notas setoriais nem estimativas nacionais de prevalência dos controles. [S3]

Alguns comunicados originais e segmentos de arquivos oficiais continuam sem verificação completa. O relatório não afirma cobrir todos os incidentes nacionais. Também não conclui sobre integridade eleitoral ou responsabilidade política a partir de alegações sobre sites, anúncios partidários ou retórica de fontes.

PRINCIPAIS CONCLUSÕES

**01**

Mantenha separadas listagens, publicações, casos oficiais e populações de registros.

**02**

Valide a autorização envolvida antes de decidir contenção ou ações para clientes.

**03**

Exercite integridade de pagamentos, comunicação de fornecedores e serviço mínimo com responsáveis definidos.

# Mapa do relatório

Doze capítulos, cinco caminhos de leitura. Siga a decisão que cabe à sua função; as limitações das evidências acompanham cada conclusão.

| | | |
|---|---|---|
| **Conselho e executivos** | Financiar a resposta e testar dependências críticas | Consulte 1 5 11 12 |
| **CISO e liderança de segurança** | Priorizar acessos, fornecedores e recuperação | Consulte 3 4 5 7 12 |
| **SOC, endpoints e identidade** | Validar comportamentos e autorização atual | Consulte 4 6 7 Apêndice B |
| **Pagamentos, fraude e proteção dos clientes** | Impedir que uma solicitação plausível resulte em dano | Consulte 5 8 9 |
| **Jurídico e comunicação** | Definir escopo, prazo e mensagem pública corretos | Consulte 5 6 10 12 |

| Grupo de capítulos | O que estabelece |
|---|---|
| 1–3 | Decisões, contexto e escopo medido ou indisponível do conjunto |
| 4–5 | Alegações de atores ao lado de divulgações oficiais e investigações |
| 6–7 | Evidências de serviço, pesquisas de campanhas e relações delimitadas |
| 8–10 | Fraude, autorização de pagamentos e obrigações por entidade |
| 11–12 | Planejamento condicional e evidências verificáveis de conclusão |
| Apêndices | Limites das populações, registro de casos, fontes e definições |

Os rótulos distinguem observação, alegação, confirmação oficial, pesquisa atribuída e inferência analítica. Uma oferta observada continua sendo uma alegação sobre seu conteúdo. Um incidente confirmado pode deixar sem resposta o ator, a entrada e o total de pessoas afetadas.

CAPÍTULO 02

# Contexto digital e operacional do Brasil

02

ESTE CAPÍTULO RESPONDE

Quais características da economia digital brasileira mudam as decisões deste relatório?

## 185 milhões

usuários de internet na estimativa contextual de outubro de 2026


2.1 Uma grande população digital, com unidades distintas 12

2.2 Identidades de pagamento conectam várias organizações 12

2.3 Serviços públicos têm vários limites de continuidade 13

2.4 A eleição de outubro é contexto, não atribuição 13

2.5 Coordenação nacional e deveres setoriais coexistem 13

CAPÍTULO 02

# Contexto digital e operacional do Brasil

EM RESUMO

Os serviços conectados do Brasil criam caminhos distintos entre dados de identidade e danos operacionais. Um cadastro copiado, uma sessão roubada e uma credencial autorizada de pagamento exigem respostas diferentes. Os casos públicos também mostram a necessidade de avaliar separadamente recuperação administrativa e operação física. Trate a eleição de outubro como contexto de comunicação, vinculando cada atribuição à fonte. Mapeie dependências de identidade, pagamentos e fornecedores antes de escolher a contenção.

## 2.1 Uma grande população digital, com unidades distintas

A estimativa da DataReportal para outubro de 2026 aponta 185 milhões de usuários de internet e penetração de 86,5%. Registra 218 milhões de conexões móveis e 154 milhões de identidades de usuários de redes sociais. Conexões e identidades em plataformas não contam pessoas únicas. [S16]

Esses números contextualizam serviços voltados aos clientes. Não explicam a origem de uma base roubada nem estabelecem a frequência de fraude entre brasileiros. Anúncios clandestinos podem citar o Brasil como mercado consumidor, suposta origem dos dados ou entrada em um catálogo multinacional.

A consequência operacional é proteger a transação e a recuperação da conta junto com o login. Nome conhecido, CPF ou telefone não devem, isoladamente, autorizar uma alteração sensível. O responsável pelo serviço deve definir a evidência mais forte exigida para essa mudança.

## 2.2 Identidades de pagamento conectam várias organizações

A pesquisa de setembro do Google Threat Intelligence Group descreve atividade financeira contra organizações capazes de emitir instruções de pagamento. Inclui bancos, processadores, varejistas e fornecedores de software financeiro. A atividade começou antes de 2026; a publicação não situa todas as invasões observadas neste ano. [S18]

Para os defensores, um mapa de dependências de pagamento deve identificar instituição, fornecedor técnico, identidade de assinatura, aprovação e responsável pela recuperação. Um fornecedor pode operar a tecnologia sem ser dono dos recursos. Um varejista pode deter uma credencial transacional sem ser banco.

Essa é uma interpretação para planejamento, sem afirmar que as organizações selecionadas compartilham determinada arquitetura. Valide as relações reais antes de atribuir um incidente a todo um grupo financeiro ou a cada cliente de um fornecedor.

## 2.3 Serviços públicos têm vários limites de continuidade

Os comunicados de Santos distinguem recuperação administrativa e continuidade portuária. O Tesouro distingue bases de dados pessoais afetadas, sistemas estruturais e impacto financeiro. Cada afirmação sustenta um limite operacional específico. Nenhuma permite concluir que todos os serviços públicos permaneceram intactos. [S127] [S128][S229]

O plano de incidentes deve definir o serviço mínimo em termos operacionais. Em um porto, isso inclui acesso autorizado e procedimentos de carga. Em um serviço público, inclui um canal funcional para o cidadão durante as restrições digitais.

Procedimentos manuais também geram registros que precisam ser conciliados depois. O responsável pela recuperação deve definir quem verifica os registros, resolve duplicidades e aprova a normalização. Um site responder é uma etapa, não o teste completo de recuperação.

## 2.4 A eleição de outubro é contexto, não atribuição

O calendário eleitoral estabelece o primeiro turno em 4 de outubro e eventual segundo turno em 25 de outubro de 2026. As datas estão no período observado. Não estabelecem que uma alegação cibernética próxima tenha relação com a eleição. [S17]

O relatório não conclui sobre integridade ou resultados eleitorais a partir de disponibilidade de sites, anúncios de registros ou linguagem política de atores. Cada alegação sobre tribunal, partido ou figura pública precisa de evidências próprias. Idioma e autodescrição não estabelecem nacionalidade nem direção estatal.

No planejamento de comunicação, aplique os mesmos padrões de verificação e proteção a todas as filiações políticas. Prepare um canal confiável de status e uma frequência de atualização. Separe serviços informativos de alegações sobre votação, apuração ou sistemas judiciais.

## 2.5 Coordenação nacional e deveres setoriais coexistem

A estratégia nacional de cibersegurança instituída pelo Decreto 12.573, em agosto de 2025, abrange proteção de cidadãos, serviços essenciais, cooperação e governança. É um marco estratégico. O relatório não a trata como prazo universal de comunicação de incidentes. [S21]

Proteção de dados, supervisão financeira, telecomunicações e coordenação governamental de incidentes têm finalidades distintas. O capítulo 10 apresenta decisões sustentadas pelos textos citados. Registro policial, notificação técnica e comunicação de dados pessoais não devem ser considerados equivalentes.

PRINCIPAIS CONCLUSÕES

**01**

Identidade, sessão e autorização de pagamento são limites de controle separados.

**02**

Datas eleitorais e retórica política não estabelecem atribuição nem impacto eleitoral.

**03**

Defina serviço mínimo e responsáveis pelas comunicações entre fornecedores e entidades jurídicas.

CAPÍTULO 03

# Exposição nacional: um conjunto selecionado de 250 domínios

ESTE CAPÍTULO RESPONDE

Quais sinais externos justificam validação no conjunto selecionado?

## 131 de 250

domínios selecionados tinham uma credencial associada anunciada à venda na verificação


3.1 Quadro do universo 16
3.2 O indicador nacional e seus limites de decisão 17
3.3 Associações de dispositivos e credenciais 17
3.4 Ofertas atuais, documentos e domínios semelhantes 19
3.5 Validação de contas antes da contenção 20
3.6 Controles passivos mantêm seu próprio denominador 20
3.7 Transforme evidência em trabalho com responsável 20

CAPÍTULO 03

# Exposição nacional: um conjunto selecionado de 250 domínios

EM RESUMO

No conjunto selecionado, 131 de 250 domínios tinham uma credencial associada anunciada à venda na verificação. O indicador nacional do Atlas é 80/100 (F). O retrato contém ao menos 2.022.570 associações de dispositivos e 12.126.465 associações de registros de credenciais. Esses registros sobrepostos descrevem os domínios selecionados, sem medir pessoas únicas, invasões confirmadas ou prevalência nacional. Designe responsáveis pela validação de contas atuais, investigação de dispositivos de funcionários e revisão de dados.

## 3.1 Quadro do universo

| Item | Definição |
|---|---|
| População selecionada | 250 domínios em dez grupos setoriais |
| Seleção | Cobertura intencional de serviços públicos, bancos, infraestrutura, grandes empresas e universidades |
| Unidade | Domínio principal candidato; titularidade jurídica e independência organizacional não validadas |
| Retrato da exposição | 22 de novembro de 2026 |
| Contexto de menções | 23 de novembro de 2025–22 de novembro de 2026 |
| Publicação | Indicador nacional do Atlas e contagens setoriais anônimas de sinais |
| Controles passivos | Sem conjunto completo de higiene disponível |
| Representatividade | Sem classificação por receita, amostra aleatória ou estimativa de prevalência nacional |
| Sobreposição | Serviços relacionados podem compartilhar operador; associações de registros podem se sobrepor entre domínios |

Os domínios selecionados são as unidades avaliadas. Alguns podem representar marcas, serviços ou entidades jurídicas relacionados. O conjunto sustenta validações delimitadas, sem contar empresas de titularidade independente. [S3]

## 3.2 O indicador nacional e seus limites de decisão

**O indicador nacional do Atlas é 80/100 (F).** Valores maiores indicam maior exposição observada neste conjunto. A nota não representa percentual de violações, probabilidade de invasão ou certificação de eficácia dos controles. [S3]

Somente o indicador nacional é publicado. As linhas setoriais contêm contagens medidas de sinais e seus denominadores. Não classificam setores por segurança, e nenhuma nota de organização ou setor é divulgada.

O retrato da exposição e o contexto de menções diferem do período de publicações do relatório. Registros históricos podem continuar visíveis após correção. O indicador não estabelece que todos os registros associados surgiram em 2026 ou continuam utilizáveis.

## 3.3 Associações de dispositivos e credenciais

O conjunto contém ao menos 2.022.570 associações de dispositivos, incluindo 108.555 associações de dispositivos de funcionários, e 12.126.465 associações de registros de credenciais. Dispositivos e credenciais aparecem, cada população, em 246 dos 250 domínios. Dispositivos de funcionários aparecem em 229 domínios. [S3]

| Setor | Domínios | Dispositivos, ao menos | Dispositivos de funcionários | Registros de credenciais |
|---|---|---|---|---|
| Bancos e finanças | 28 | 249.113 | 3.760 | 904.473 |
| Administração pública e justiça | 30 | 364.763 | 34.619 | 237.008 |
| Energia e serviços essenciais | 27 | 139.105 | 3.260 | 607.503 |
| Indústria e agronegócio | 27 | 20.413 | 3.905 | 620.288 |
| Telecomunicações e tecnologia | 22 | 188.057 | 26.693 | 5.490.480 |
| Varejo e serviços ao consumidor | 24 | 333.578 | 4.299 | 386.307 |
| Transportes e logística | 25 | 149.553 | 4.463 | 475.623 |
| Saúde e seguros | 24 | 171.725 | 2.389 | 330.327 |
| Educação e pesquisa | 25 | 213.867 | 24.187 | 2.995.842 |
| Pagamentos e serviços empresariais | 18 | 192.396 | 980 | 78.614 |
| Total | 250 | 2.022.570 | 108.555 | 12.126.465 |

As associações de dispositivos de funcionários integram a visão de dispositivos e não devem ser somadas a ela. Associações podem se sobrepor entre domínios. Os totais não representam dispositivos nacionais distintos nem pessoas únicas.

Telecomunicações e tecnologia reúnem 5.490.480 associações de registros de credenciais, e educação e pesquisa reúnem 2.995.842. Administração pública e justiça reúnem ao menos 364.763 associações de dispositivos. As concentrações sustentam validação por responsável, sem estabelecer taxas setoriais de invasão.

Um dispositivo associado a domínio de atendimento pode não pertencer ao prestador. Uma credencial pode envolver funcionário, cliente, estudante, prestador ou relação não resolvida. Estabeleça a relação antes de escolher a contenção.

## Populações setoriais de dispositivos e credenciais diferem em escala e significado




Fonte: observações de exposição para 250 domínios selecionados, 22 de novembro de 2026 [S3]. Associações podem se sobrepor e incluir material histórico; não representam pessoas únicas, invasões atuais ou prevalência nacional.

## 3.4 Ofertas atuais, documentos e domínios semelhantes

Neste retrato, 131 dos 250 domínios selecionados tinham uma credencial associada anunciada à venda na verificação. Associações de documentos aparecem em 201 domínios; observações de domínios semelhantes, em 206. As populações podem se sobrepor e não são somadas. [S3]

| Setor | Domínios | Domínios com ofertas de credenciais | Documentos | Domínios semelhantes |
|---|---|---|---|---|
| Bancos e finanças | 28 | 17 | 1.475 | 2.780 |
| Administração pública e justiça | 30 | 14 | 3.666 | 9.184 |
| Energia e serviços essenciais | 27 | 9 | 488 | 655 |
| Indústria e agronegócio | 27 | 6 | 461 | 2.774 |
| Telecomunicações e tecnologia | 22 | 15 | 668 | 2.442 |
| Varejo e serviços ao consumidor | 24 | 18 | 168 | 880 |
| Transportes e logística | 25 | 10 | 234 | 581 |
| Saúde e seguros | 24 | 13 | 150 | 1.235 |
| Educação e pesquisa | 25 | 18 | 339 | 574 |
| Pagamentos e serviços empresariais | 18 | 11 | 75 | 2.520 |
| Total | 250 | 131 | 7.724 | 23.625 |

Anúncios atuais estabelecem uma oferta, sem testar acesso, comprovar venda ou invasão da infraestrutura da organização. Valide conta anunciada, serviço e data da evidência com o responsável.

As 7.724 associações de documentos não estabelecem confidencialidade, obtenção ilícita ou download por adversário. Documentos públicos ou repetidos continuam sendo explicações plausíveis. O responsável pelos dados deve estabelecer titularidade e sensibilidade.

As 23.625 observações de domínios semelhantes são observações recentes. Semelhança isolada não estabelece impersonação ou phishing. Resultados ambíguos permanecem não resolvidos até validação do conteúdo e da relação pelas equipes de marca e abuso.

## 3.5 Validação de contas antes da contenção

Para conta da organização, estabeleça se está ativa e se a evidência é recente. Verifique privilégios, acessos, sessões, métodos de recuperação e correções anteriores. Registre se a relação envolve funcionário, prestador, cliente, estudante ou parte não resolvida.

Uma identidade privilegiada ativa pode justificar revogação urgente de sessões e revisão de acesso. Uma conta histórica desativada pode exigir registro do encerramento anterior. Trocar senha isoladamente não estabelece encerramento de delegações e sessões persistentes.

Observações de dispositivos de clientes podem exigir atuação de fraude ou proteção dos clientes. Não justificam automaticamente incidente na infraestrutura do prestador. A visão bancária anônima do capítulo 9 preserva esses limites.

## 3.6 Controles passivos mantêm seu próprio denominador

Não se publica prevalência de DMARC, SPF, DKIM, DNSSEC, TLS ou cabeçalhos web. Não há conjunto completo de higiene nem índice de higiene disponível. Observações indisponíveis não representam falhas dos controles nem são substituídas por zeros.

Os responsáveis devem validar remetentes legítimos e alinhamento da autenticação antes de ampliar a aplicação das políticas. Devem rever validade de certificados e dependências no próprio ambiente. O retrato da exposição não fornece a avaliação de configuração ausente.

## 3.7 Transforme evidência em trabalho com responsável

| Fila | Primeira decisão | Evidência de encerramento |
|---|---|---|
| Contas | A identidade pertence a serviço ativo da organização? | Validação datada e situação da conta |
| Dispositivos | A relação do dispositivo é pertinente e atual? | Registro de investigação e resposta |
| Proteção dos clientes | A evidência cria risco específico de fraude? | Avaliação de fraude e canal confiável |
| Configuração | O estado informado do controle está correto? | Configuração validada pelo responsável |
| Titularidade de dados | O material pertence à organização? | Categoria, idade e avaliação de acesso |

PRINCIPAIS CONCLUSÕES

**01**

O indicador nacional do Atlas descreve o conjunto selecionado, sem medir prevalência nacional.

**02**

Dispositivos, credenciais, anúncios e documentos exigem validações separadas.

**03**

Designe responsáveis separados para contas, dispositivos, dados e configurações, com evidência datada de encerramento.

CAPÍTULO 04

# Atividade na dark web: do anúncio à decisão com responsável

ESTE CAPÍTULO RESPONDE

O que está sendo oferecido e o que tornaria a informação acionável?

**10**

casos selecionados de alegações com trechos autênticos e anonimizados


4.1 Como ler a população de publicações 23
4.2 Caso A: arquivo de documentos de órgão público 24
4.3 Caso B: clientes, pedidos e entregas 25
4.4 Caso C: alegações sobre dados fiscais municipais 26
4.5 Caso D: responsáveis e histórico financeiro estudantil 28
4.6 Caso E: assistente virtual e cronologia inconsistente 29
4.7 Caso F: contatos recentes associados a banco 30
4.8 Caso G: oferta Pix em novembro identificada como 2025 32
4.9 Caso H: tabela de clientes de software empresarial 33
4.10 Caso I: certificados e rede interna 34
4.11 Caso J: acesso a infraestrutura financeira 35
4.12 Alegação e evidência 36
4.13 Outras narrativas e limites explícitos 36
4.14 Contexto das publicações e limites dos idiomas 37

CAPÍTULO 04

# Atividade na dark web: do anúncio à decisão com responsável

EM RESUMO

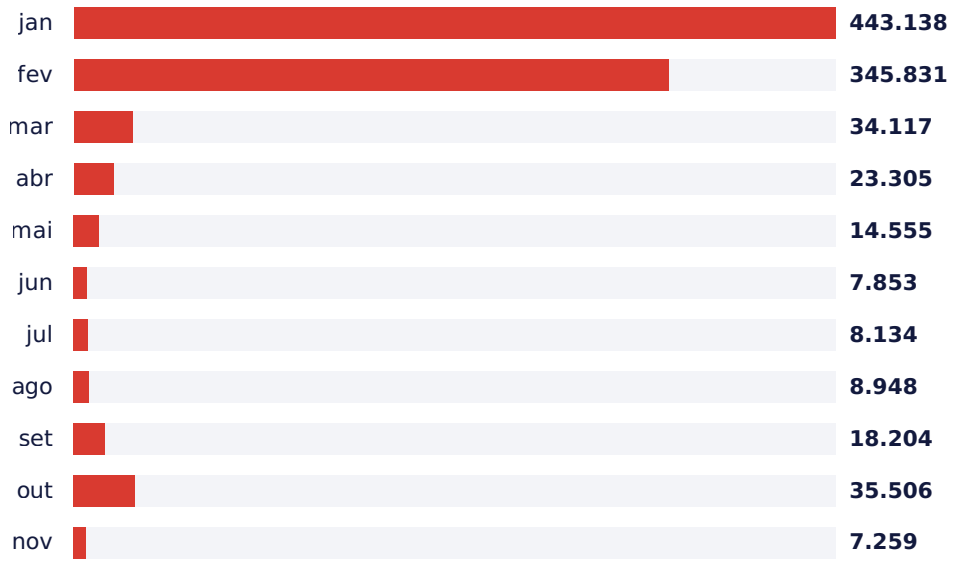
As publicações selecionadas anunciam registros públicos, processos de clientes, dados educacionais, contatos financeiros e acesso relacionado a pagamentos. A publicação evidencia a circulação da alegação. Não autentica dados, estabelece nova invasão ou confirma venda. Repetições e datas inconsistentes merecem análise sem virar incidentes adicionais. Leia cada oferta como um indício delimitado e peça ao responsável que valide os dados, a identidade ou a permissão envolvida.

## 4.1 Como ler a população de publicações

As observações do Brandefense Blackhole abrangem publicações associadas ao Brasil entre 1 de janeiro e 22 de novembro de 2026. A associação pode indicar suposto alvo, mercado consumidor, campo de dados ou discussão de eventos públicos. Não evidencia automaticamente direcionamento ao país. [S1]

O Blackhole registra 946.850 publicações associadas ao Brasil no período. Janeiro e fevereiro somam 788.969, ou 83,3% dessa população. Os meses seguintes têm visibilidade diferente. O padrão não estabelece mudança correspondente em atividade criminosa ou perdas. [S1]

### Observações mensais de publicações associadas ao Brasil; publicações não são incidentes




Fonte: observações de publicações associadas ao Brasil, 1 de janeiro–22 de novembro de 2026; dia de corte parcial. Publicações não são incidentes [S1].

A cobertura mais ampla do conteúdo é incompleta. As dez narrativas abaixo têm apoio nos trechos retidos, sem estimar que representem todos os eventos da população maior. Plataformas e idiomas descrevem contexto de publicação, sem estabelecer nacionalidade ou controle operacional.

Os casos selecionados não são os dez maiores incidentes brasileiros. Ilustram decisões distintas sustentadas por publicações retidas. Os trechos públicos retiram elementos de identificação, contatos, dados pessoais e caminhos de obtenção, preservando o significado da alegação.

**Um anúncio é evidência de um anúncio.** A base pode ser antiga, parcialmente pública, montada de várias origens ou apresentada de forma enganosa. O acesso oferecido pode estar obsoleto, limitado ou ser inventado. A confirmação exige evidências da organização relevante ou de outra fonte competente.

O capítulo separa o que foi observado do que não está estabelecido. Essa separação também orienta o registro de incidentes e o livro de evidências. A linguagem confiante de uma fonte não aumenta a confiança do relatório no acesso alegado.

## 4.2 Caso A: arquivo de documentos de órgão público

Uma publicação de 3 de janeiro alega possuir um arquivo incompleto ligado a um órgão público. O trecho menciona 2,9GB e chama os documentos de confidenciais. São descrições do autor, sem autenticação do conteúdo. [S1]

Cartão de evidência B01 — 3 jan 2026

**Autor do fórum** | Fórum de vazamentos | Forum | Inglês

ORIGINAL

SIZE : 2.9GB (not complete) THIS FOLDER CONTAINS DOCUMENTS ONLY [...] confidential documents related to the [public-sector body].

TRADUÇÃO

Tradução do trecho original: TAMANHO: 2,9GB (incompleto) ESTA PASTA CONTÉM APENAS DOCUMENTOS [...] documentos confidenciais relacionados ao [órgão público].

**Observado**
Um autor alega divulgar documentos ligados a um órgão público e anuncia um arquivo incompleto.

**Não estabelecido**
A alegação foi observada; não foram autenticados arquivos, confidencialidade, acesso atual, identidade do ator ou data de invasão.

A

CASO A

### Arquivo de documentos de órgão público

Administração pública

Alegação não verificada

| | |
|---|---|
| OBSERVADO | Circulação de uma alegação datada sobre arquivo e documentos. |
| NÃO ESTABELECIDO | Autenticidade, confidencialidade real, acesso atual, pessoas únicas ou data de invasão. |
| ALTERNATIVA | Exportação antiga, material público ou descrição enganosa poderiam produzir anúncio semelhante. |
| RESPONSÁVEL E AÇÃO | O responsável pelos dados deve validar categorias e idade dos documentos relevantes e revisar os registros autorizados de acesso correspondentes. |

**Conclusão**

Valide titularidade, idade e sensibilidade dos documentos.

O tamanho de um arquivo não estabelece impacto operacional. Se o responsável validar um documento sensível, a resposta deve seguir seu conteúdo e público autorizado. Não deve presumir entrada em todos os sistemas do órgão.

## 4.3 Caso B: clientes, pedidos e entregas

Uma oferta de varejo publicada em 4 de janeiro lista Contacts, Orders e Deliverylogs. A combinação descreve um processo de atendimento, sem estabelecer pessoas únicas. Uma resposta que cita o anúncio apenas o repete, sem confirmação independente. [S1]

Cartão de evidência B02 — 4 jan 2026

**Autor do fórum** | Fórum de vazamentos | Forum | Inglês

ORIGINAL

Offering a dataset originating from [a retail business]. [...] including Contacts, Orders, Deliverylogs.

TRADUÇÃO

Tradução do trecho original: Ofereço uma base de dados originária de [uma empresa varejista]. [...] incluindo Contatos, Pedidos e Registros de Entrega.

**Observado**
Um anúncio combina categorias de contatos de clientes, pedidos e entregas.

**Não estabelecido**
A lista alegada de campos foi observada; posse, atualidade, origem organizacional, quantidade de registros e venda concluída não foram verificadas. Uma resposta citada repete o anúncio.

B

CASO B

### Clientes, pedidos e entregas

Varejo

Alegação não verificada

| | |
|---|---|
| OBSERVADO | Categorias de campos alegadas e linguagem de venda. |
| NÃO ESTABELECIDO | Posse, organização de origem, idade, venda concluída ou total de clientes únicos. |
| ALTERNATIVA | O material poderia vir de prestador, exportação anterior ou anúncio copiado. |
| RESPONSÁVEL E AÇÃO | Responsáveis pelo serviço e pelos dados devem validar categorias e preparar verificação confiável para contatos sobre entregas e pagamentos. |

**Conclusão**

Valide origem e categorias do processo de clientes.

Varejista, transportador e fornecedor de software podem guardar registros relacionados. Defina quem controlava os dados antes de atribuir responsabilidade. Um detalhe plausível de entrega não deve autenticar uma cobrança inesperada.

## 4.4 Caso C: alegações sobre dados fiscais municipais

Uma narrativa de 14 de janeiro anuncia várias bases tributárias municipais, citando contribuintes, notas NFSe, declarações, registros de acesso e guias de pagamento. Outros anúncios municipais aparecem no material retido. Semelhança textual não demonstra mesmo operador ou evento. [S1]

Cartão de evidência B03 14 jan 2026

**Autor do fórum** Fórum de vazamentos Forum Inglês

ORIGINAL

multiple Brazilian municipal tax databases [...] The dataset includes taxpayer records, NFSe invoices, declarations, access logs, payment guides, and more.

TRADUÇÃO

Tradução do trecho original: várias bases tributárias municipais brasileiras [...] O conjunto inclui registros de contribuintes, notas NFSe, declarações, registros de acesso, guias de pagamento e mais.

**Observado**
O autor alega divulgar dados fiscais de várias bases associadas a serviços municipais.

**Não estabelecido**
As linhas alegadas abrangem várias bases; não estabelecem pessoas únicas, invasões municipais separadas, acesso atual ou notas autênticas. Publicação paralela usa texto semelhante.

C

CASO C

## Alegações sobre dados fiscais municipais

Serviços municipais

Alegação não verificada

| | |
|---|---|
| OBSERVADO | Alegação sobre várias bases fiscais e lista de categorias. |
| NÃO ESTABELECIDO | Invasões municipais separadas, contribuintes únicos, acesso atual ou notas autênticas. |
| ALTERNATIVA | Várias bases podem repetir registros de um serviço comum ou exportação histórica. |
| RESPONSÁVEL E AÇÃO | Mapeie limites do serviço e do fornecedor, valide registros e teste a autenticação de instruções de pagamento. |

**Conclusão**

Mapeie serviços fiscais e verifique instruções de pagamento.

Não some alegações de linhas em uma contagem de pessoas. Um contribuinte pode aparecer em nota, declaração, registro de acesso e guia. O mesmo material também pode ser anunciado mais de uma vez.

A resposta deve conectar proteção de dados e integridade de pagamento sem confundi-las. Uma guia copiada pode sustentar falsificação de identidade. Não estabelece capacidade de alterar guias atuais ou redirecionar uma transação.

## 4.5 Caso D: responsáveis e histórico financeiro estudantil

Uma publicação de 2 de fevereiro anuncia aproximadamente 763.000 registros pessoais e financeiros associados a um fornecedor educacional. O autor descreve perfis de responsáveis, CPF e históricos financeiros de estudantes. O número permanece uma alegação de linhas anunciadas. [S1]

Cartão de evidência B04 — 2 fev 2026

**Autor do fórum** | Fórum de vazamentos | Forum | Inglês

ORIGINAL

approximately 763,000 personal and financial records from [an education service provider] (Brazil). The dataset contains sensitive guardian profiles, national ID numbers (CPF), and detailed student financial histories.

TRADUÇÃO

Tradução do trecho original: aproximadamente 763.000 registros pessoais e financeiros de [um fornecedor educacional] (Brasil). O conjunto contém perfis sensíveis de responsáveis, CPF e históricos financeiros detalhados de estudantes.

**Observado**
Uma oferta liga identificadores de responsáveis a registros financeiros estudantis.

**Não estabelecido**
Linhas anunciadas não são estudantes ou responsáveis únicos. Posse, obtenção, precisão e acesso ao sistema de origem permanecem não verificados.

D

CASO D

### Responsáveis e histórico financeiro estudantil

Educação

Alegação não verificada

| | |
|---|---|
| OBSERVADO | Alegação ligada a fornecedor que conecta identificadores familiares e contexto financeiro educacional. |
| NÃO ESTABELECIDO | Total de estudantes ou responsáveis únicos, precisão, data de obtenção ou acesso aos sistemas do fornecedor. |
| ALTERNATIVA | As categorias podem combinar períodos distintos ou relações familiares repetidas. |
| RESPONSÁVEL E AÇÃO | Valide a relação com o fornecedor e reveja canais confiáveis para mensalidades, dívidas e recuperação de contas. |

**Conclusão**

Valide fornecedor e contatos confiáveis sobre mensalidades.

A instituição deve saber quem responde às famílias se houver divulgação de incidente no fornecedor. Nome correto de um responsável ou detalhe plausível de mensalidade não substitui verificação. A mensagem adequada depende de categorias validadas, sem adotar o número do anúncio.

## 4.6 Caso E: assistente virtual e cronologia inconsistente

Uma publicação de 6 de fevereiro alega divulgar parte de dados de um assistente virtual financeiro. Descreve exportação de setembro de 2022 a abril de 2026. O fim alegado é posterior à data armazenada da publicação, exigindo validação da cronologia. [S1]

Cartão de evidência B05 — 6 fev 2026

**Autor do fórum** | Fórum de vazamentos | Forum | Inglês

ORIGINAL

today we release [a financial services provider]'s [virtual assistant] partial dump. [...] exported all data from Sept 2022 to April 2026.

TRADUÇÃO

Tradução do trecho original: hoje divulgamos parte dos dados do [assistente virtual] de [um fornecedor de serviços financeiros]. [...] exportamos todos os dados de setembro de 2022 a abril de 2026.

**Observado**
Um anúncio parcial de assistente virtual mistura contagens de conversas e identidades e alega período encerrado depois da data armazenada da publicação.

**Não estabelecido**
A publicação é de 6 de fevereiro de 2026, mas diz que os dados chegam a abril de 2026. A inconsistência exige validação; não autentica a base nem estabelece fabricação. Categorias de identidade não podem ser somadas como pessoas únicas.

CASO E

E

### Assistente virtual e cronologia inconsistente

Serviços financeiros

Alegação não verificada

| | |
|---|---|
| OBSERVADO | Narrativa de divulgação parcial e datas inconsistentes. |
| NÃO ESTABELECIDO | Intervalo real, origem, acesso atual ou identidades únicas. |
| ALTERNATIVA | Erro de data, descrição reutilizada ou apresentação enganosa podem explicar a inconsistência; o registro não decide qual. |
| RESPONSÁVEL E AÇÃO | Valide titularidade do serviço, cronologia e categorias antes de adotar a quantidade ou declarar incidente na plataforma. |

**Conclusão**

Resolva a cronologia antes de adotar uma quantidade.

A inconsistência não autentica o material nem demonstra fabricação. Justifica preservar a incerteza. Conversas e identidades também são populações diferentes e não podem ser somadas como pessoas.

Textos relacionados aparecem depois. Isso estabelece continuidade da circulação de uma narrativa. Não demonstra acesso ativo durante todo o período ou posse dos dados por cada republicador.

## 4.7 Caso F: contatos recentes associados a banco

Em 11 de novembro, um vendedor alega possuir 22.705.600 contatos bancários, exportados uma semana antes, e oferece a venda integral ou segmentada. Data de obtenção e quantidade são afirmações do vendedor. A proporção anunciada de contas não é repetida como estatística bancária. [S1]

Cartão de evidência B06 — 11 nov 2026

**Autor do fórum** | Fórum de vazamentos | Forum | Inglês

ORIGINAL

I have 22,705,600 leads that I exported one week ago directly from [a bank]. [...] I am looking to sell this database, either in its entirety or in segments.

TRADUÇÃO

Tradução do trecho original: Tenho 22.705.600 contatos que exportei uma semana atrás diretamente de [um banco]. [...] Quero vender esta base inteira ou em segmentos.

**Observado**

Um vendedor em novembro alega possuir uma grande lista de contatos bancários e oferece venda integral ou segmentada.

**Não estabelecido**

Não se estabelece confirmação organizacional, população autenticada, obtenção, acesso atual, titularidade ou venda. A proporção alegada de contas do banco não é verificada e não deve ser repetida como estatística bancária.

F

CASO F

## Contatos recentes associados a banco

Bancos

Alegação não verificada

| | |
|---|---|
| OBSERVADO | Anúncio recente de contatos associados a banco e segmentação. |
| NÃO ESTABELECIDO | Confirmação organizacional, precisão, origem, atualidade, acesso presente ou venda concluída. |
| ALTERNATIVA | Uma lista pode reunir registros antigos, públicos, comercializados ou não relacionados, usando o banco como categoria de venda. |
| RESPONSÁVEL E AÇÃO | Valide origem e categorias; avalie risco de contatos fraudulentos separadamente do acesso aos sistemas bancários. |

**Conclusão**

Separe contatos anunciados de acesso aos sistemas bancários.

O anúncio é relevante para falsificação plausível de identidade. Não evidencia que cada contato anunciado seja cliente ativo, tenha conta com saldo ou tenha sofrido prejuízo. A proteção dos clientes deve usar o escopo validado.

## 4.8 Caso G: oferta Pix em novembro identificada como 2025

Um anúncio de 17 de novembro se apresenta como base Pix de 2025, alega mais de 4M de entradas e pede US$100. A própria descrição fornece um limite histórico. É preço pedido, sem venda concluída estabelecida. [S1]

Cartão de evidência B07 — 17 nov 2026

**Autor do fórum** | Fórum de vazamentos | Forum | Inglês

ORIGINAL

PIX DATABASE 2025 [...] Year: 2025 Records: 4M+ entries Country: Brazil [...] Price: $100 USD

TRADUÇÃO

Tradução do trecho original: BASE PIX 2025 [...] Ano: 2025 Registros: mais de 4M entradas País: Brasil [...] Preço: $100 USD

**Observado**
Um anúncio de novembro identifica explicitamente seus dados de Pix como material de 2025.

**Não estabelecido**
A data da publicação não estabelece invasão de 2026. Entradas não são pessoas ou transferências verificadas; sem ligação estabelecida com comunicado oficial específico, acesso utilizável a pagamentos ou venda.

CASO G

G

### Oferta Pix em novembro identificada como 2025

Pagamentos

Alegação não verificada

| | |
|---|---|
| OBSERVADO | Oferta de dados de pagamento associada ao Brasil com rótulo explícito de 2025. |
| NÃO ESTABELECIDO | Invasão de 2026, pessoas únicas, acesso utilizável a pagamentos ou conexão com comunicado oficial específico sobre Pix. |
| ALTERNATIVA | Agregação histórica e revenda podem explicar circulação atual sem acesso atual. |
| RESPONSÁVEL E AÇÃO | Verifique idade e origem e autentique independentemente pedidos que citem identificadores de pagamento. |

**Conclusão**

Dados históricos não estabelecem autorização atual.

Uma entrada ligada ao Pix não é necessariamente um segredo que autorize transferência. Ao mesmo tempo, um identificador histórico pode continuar útil em golpes. Separe avaliação de autorização de pagamento e avaliação de proteção de dados.

## 4.9 Caso H: tabela de clientes de software empresarial

Uma publicação de 19 de novembro alega material brasileiro datado de novembro de 2026 e identifica um arquivo de tabela de clientes. Associa os dados a software empresarial. Os rótulos continuam alegações e não estabelecem a data de obtenção. [S1]

Cartão de evidência B08 — 19 nov 2026

**Autor do fórum** | Fórum de vazamentos | Forum | Inglês

ORIGINAL

Country: Brazil Date: Nov 2026 [...] Table_Name:customers.csv

TRADUÇÃO

Tradução do trecho original: País: Brasil Data: novembro de 2026 [...] Nome_da_Tabela:customers.csv

**Observado**

Uma oferta de novembro descreve dados de clientes associados a um serviço de gestão empresarial.

**Não estabelecido**

Nome de tabela e função anunciada não estabelecem invasão atual do fornecedor, incidentes nos clientes, registros autênticos, pessoas afetadas ou venda.

H

CASO H

### Tabela de clientes de software empresarial

Software empresarial

Alegação não verificada

| | |
|---|---|
| OBSERVADO | Anúncio datado de dados de clientes associados a fornecedor. |
| NÃO ESTABELECIDO | Invasão do fornecedor, acesso atual, pessoas únicas ou incidentes separados em empresas clientes. |
| ALTERNATIVA | Exportação de cliente, base antiga ou coleção renomeada podem ter descrição semelhante. |
| RESPONSÁVEL E AÇÃO | Valide limites do fornecedor e dos clientes, categorias relevantes e o canal de comunicação de incidentes. |

**Conclusão**

Valide separadamente fornecedor e limites dos clientes.

Anúncios anteriores de software para restaurantes descrevem usuários, contatos comerciais e linhas de clientes. São alegações registradas separadamente. As categorias sobrepostas não são somadas à oferta de novembro como total nacional de vítimas do setor.

## 4.10 Caso I: certificados e rede interna

Uma publicação de 24 de março oferece certificados associados a um intermediário de serviços de pagamento e, separadamente, acesso à rede interna. Não autentica o material nem demonstra que os certificados poderiam autorizar pagamento. [S1]

Cartão de evidência B09 — 24 mar 2026

**Autor do fórum** | Fórum de vazamentos | Forum | Inglês

ORIGINAL

I am offering access to certificates belonging to [a payment services intermediary]. [...] Additionally, access to an internal network is available.

TRADUÇÃO

Tradução do trecho original: Ofereço acesso a certificados pertencentes a [um intermediário de serviços de pagamento]. [...] Além disso, há acesso a uma rede interna.

**Observado**
Um anúncio associa certificados de pagamento a suposto acesso à rede interna.

**Não estabelecido**
O anúncio não estabelece arquivo de certificado, estado de confiança, autorização transacional, usabilidade, acesso atual à rede, venda ou ligação com campanha nomeada.

CASO I

### Certificados e rede interna

Serviços de pagamento

Alegação não verificada

| | |
|---|---|
| OBSERVADO | Linguagem de venda de certificados e acesso interno em oferta datada. |
| NÃO ESTABELECIDO | Função, validade, privilégios, acesso atual, capacidade de transferência ou venda concluída. |
| ALTERNATIVA | Material obsoleto, de teste ou finalidade limitada pode ter descrição convincente sem autorização de pagamento em produção. |
| RESPONSÁVEL E AÇÃO | Peça aos responsáveis por pagamentos e pelo fornecedor que validem o escopo e demonstrem a revogação pertinente. |

**Conclusão**

Estabeleça escopo do certificado e revogação.

A pesquisa pública sobre identidades de pagamento torna essa uma pergunta de controle útil. Não liga o vendedor ao BREEZE COMET ou a um incidente financeiro confirmado. Semelhança de assunto não estabelece relação operacional. [S18]

## 4.11 Caso J: acesso a infraestrutura financeira

Uma oferta de 6 de julho descreve acesso ligado a fornecedor brasileiro de infraestrutura fintech e serviços bancários. Suas alegações mais amplas de permissão precisam de validação no ambiente real. O setor indicado não estabelece a identidade de cada cliente. [S1]

Cartão de evidência B10 — 6 jul 2026

**Autor do fórum** | Fórum de vazamentos | Forum | Inglês

ORIGINAL

Currently selling an access within a brazilian fintech company. SECTOR: Fintech/Infratech/BaaS REGION: Brazil

TRADUÇÃO

Tradução do trecho original: Vendo atualmente acesso em uma empresa fintech brasileira. SETOR: Fintech/Infratech/BaaS REGIÃO: Brasil

**Observado**
Um vendedor anuncia acesso que abrange administração de site e código, bases de dados, armazenamento de objetos, monitoramento e exportações de produção.

**Não estabelecido**
As funções anunciadas não estabelecem permissões efetivas, invasão da produção, autorização de transferência ou venda.

J

CASO J

### Acesso a infraestrutura financeira

Infraestrutura financeira

Alegação não verificada

| | |
|---|---|
| OBSERVADO | Anúncio de acesso com descrição de infraestrutura financeira. |
| NÃO ESTABELECIDO | Autorização administrativa atual, acesso de produção, movimentação de recursos, impacto em clientes ou transação concluída. |
| ALTERNATIVA | O acesso pode ser restrito, histórico, compartilhado indevidamente ou apresentado de modo enganoso. |
| RESPONSÁVEL E AÇÃO | Confirme a relação com o fornecedor, o ambiente e as permissões reais; coordene contenção delimitada com o responsável pelo serviço. |

**Conclusão**

Valide ambiente e permissões efetivas.

Um fornecedor de infraestrutura pode atender muitas organizações, mas uma oferta associada a ele não estabelece incidente em cada cliente. A primeira resposta deve localizar quem pode validar ou revogar o suposto acesso.

## 4.12 Alegação e evidência

| Alegação do ator | Evidência retida | Interpretação responsável |
|---|---|---|
| "Milhões de registros" | A publicação contém a quantidade | Linhas, pessoas e contas são unidades diferentes |
| "Exportação recente" | Data relativa no texto do vendedor | A obtenção precisa de validação |
| "Acesso de administrador" | Linguagem de permissões anunciadas | Privilégio e ambiente atuais não verificados |
| "Certificados" | Oferta menciona o material | Não estabelece autorização de assinatura de pagamentos |
| "Base Pix" | Rótulo de pagamento e ano alegado | Sem conexão automática com incidente divulgado |
| "Documentos confidenciais" | Descrição do autor | Classificação e titularidade precisam de validação |
| Anúncio repetido | A narrativa reaparece | Sem novo incidente ou confirmação independente |

O painel orienta a interpretação. Não nega a possibilidade de dano real. Identifica a proposição sustentada pela evidência, para que a próxima ação seja específica e verificável.

## 4.13 Outras narrativas e limites explícitos

O registro também inclui supostos acessos a câmeras residenciais, dados de moradores e funcionários, logins de serviços investigativos, plataforma de pagamentos e base financeira ligada ao varejo. Cada item preserva sua ação e incerteza. Nenhum vira invasão confirmada por aparecer ao lado de caso oficial. [S1]

Um anúncio relacionado a KYC afirma explicitamente que não é vazamento. É tratado como narrativa de serviço ou demanda, sem inferência automática de incidente. Material veicular identificado como sendo de 2024 permanece histórico, apesar da publicação em 2026.

Uma oferta de filiação partidária permanece alegação não verificada. Não sustenta conclusão de interferência eleitoral ou julgamento sobre partido. Da mesma forma, uma alegação logística de novembro não estabelece controle físico nem interrupção real.

Encaminhe os indícios aos responsáveis sem reproduzir dados pessoais ou facilitar contato com vendedores. Valide evidências da organização e preserve a decisão. Relevância para o relatório e confirmação de um evento prejudicial são decisões separadas.

Outras publicações anunciam webshells de serviços públicos e uma conta de correio em nuvem. Rótulos de venda, mensagem de pagamento de bot e quantidade sem unidade clara não verificam transação, validade da conta ou permissões atuais. Trate a alegação como pista para validar serviço próprio. [S1]

Uma publicação de 22 de novembro descreve uma suposta exportação de contatos profissionais associada a um fornecedor de informações empresariais. As categorias de diretórios, perfis e solicitações de suporte são alegações do autor. Não autenticam os registros nem estabelecem exposição de dados de pacientes, invasão, obtenção recente ou acesso atual. Valide a titularidade e o uso permitido antes de tratar a alegação como incidente de dados confidenciais. [S1]

Uma republicação de 18 de agosto descreve suposta divulgação de base do setor público, em vez de venda. Não autentica posse ou distribuição, nem estabelece correspondência com a oferta anterior de arquivos do Caso A. [S1]

Outra oferta de 22 de novembro descreve suposta exportação de um fornecedor de gestão de clientes e serviços de varejo. Menciona contatos, projetos de sites e solicitações de suporte. A descrição não verifica origem, registros, acesso atual, impacto nos clientes, data de obtenção ou venda concluída. Os limites do fornecedor e dos clientes exigem validação separada. [S1]

## 4.14 Contexto das publicações e limites dos idiomas

| Contexto | Rótulo | Publicações observadas |
|---|---|---|
| Plataforma | Telegram | 896.534 |
| Plataforma | Fórum de vazamentos | 1.840 |
| Idioma | Português | 116.772 |
| Idioma | Inglês | 60.682 |
| Idioma | Espanhol | 7.177 |
| Idioma | Russo | 26.878 |
| Idioma | Turco | 724.456 |

São observações de rótulos de publicação na posição de 22 de novembro, sem classificar incidentes. Os idiomas não contam pessoas ou atores distintos. Observações de plataforma e idioma não devem ser somadas. [S1]

Turco é o rótulo mais numeroso entre esses idiomas. Isso não estabelece nacionalidade turca, controle ou direcionamento dos operadores. Associação ao Brasil pode aparecer em circulação multilíngue, incluindo material repetido. As evidências dos casos sustentam perguntas de segurança mais delimitadas.

Para a defesa, a consequência é prática: avalie conteúdo e ativo próprio antes de escalar associação nacional ou linguística. Nem volume elevado de publicações nem nome bancário conhecido autentica base anunciada.

PRINCIPAIS CONCLUSÕES

**01**

A publicação estabelece circulação de uma alegação, com data e limites próprios.

**02**

Linhas, repetições e permissões anunciadas não estabelecem vítimas únicas ou acesso atual.

**03**

Atribua cada indício relevante a um responsável por dados, identidade, pagamento ou serviço e registre a decisão.

CAPÍTULO 05

# Incidentes e atividade por setor

ESTE CAPÍTULO RESPONDE

Quais divulgações mudam uma decisão de defesa e o que continua sendo alegação?

**10**

exemplos nomeados sustentados por confirmação oficial e ampla cobertura


5.1 Quadro de decisões setoriais 40
5.2 Incidentes confirmados com dados cadastrais 41
5.3 Integridade de pagamentos e disponibilidade financeira 42
5.4 Recuperação administrativa e continuidade operacional 44
5.5 Outros casos e campanhas oficiais 45
5.6 Outras divulgações em serviços 47
5.7 Atividade recente: 8 a 22 de novembro 51
5.8 Exclusões importantes e contexto histórico 54
5.9 Outras divulgações e notícias com limites definidos 55

CAPÍTULO 05

# Incidentes e atividade por setor

EM RESUMO

Divulgações públicas mostram cópia de cadastros, alteração de instruções de pagamento e recuperação administrativa prolongada. Não descrevem uma invasão comum. Os casos nomeados atendem aos critérios de confirmação e cobertura; os demais preservam descrições genéricas. Descoberta, divulgação, investigação e restauração têm datas separadas. Comece pela função afetada e pelo acesso estabelecido; escolha contenção, apoio aos clientes e continuidade conforme essa evidência.

## 5.1 Quadro de decisões setoriais

As linhas combinam tipos de evidência diferentes sem transformá-los em taxas setoriais de incidentes.

| Setor | Evidências nesta edição | Tipo e limite | Primeira decisão |
|---|---|---|---|
| Bancos e pagamentos | Incidente em serviço Pix; alteração de guias; anúncios de acesso e contatos | Incidentes oficiais e ofertas separadas, não verificadas | Proteger autorização transacional e validar contas |
| Seguros | Cópia de cadastro da CVP | Categorias confirmadas; exclusões preliminares continuam datadas | Preparar proteção e comunicação com clientes |
| Administração pública | Divulgação do Tesouro; base histórica; alertas sobre sites | Comunicados confirmados e orientações de campanha | Definir responsáveis pelos dados e serviço mínimo |
| Transporte e logística | Sistemas administrativos e procedimentos manuais em Santos | Incidente confirmado; garantia de capacidade atribuída à autoridade | Exercitar alternativas e conciliação administrativa |
| Saúde | Investigação clínica, divulgação de portal e continuidade de atendimento | Comunicados oficiais e alegações; populações separadas | Rever acesso, alternativas clínicas e administração |
| Educação | Anúncio de dados financeiros de responsáveis e estudantes | Categorias e linhas alegadas, não verificadas | Validar escopo do fornecedor e mensagens de mensalidade |
| Varejo e serviços | Anúncios de dados de clientes, pedidos, câmeras e moradores | Alegações que incluem demandas e material histórico | Separar titularidade do serviço e origem dos dados |
| Indústria e energia | Divulgação de dados de clientes por concessionária, listagens e pesquisas atribuídas | Divulgação empresarial e alegações separadas; sem taxa representativa de invasão setorial | Validar acessos aplicáveis e dependências de recuperação |

Fontes: publicações retidas [S1], Ransompedia [S2] e fontes oficiais ou originais identificadas abaixo. Nenhum setor recebe uma nota do Atlas.

## 5.2 Incidentes confirmados com dados cadastrais

K

CASO K

### Cadastros da CVP e proteção dos clientes

Seguros

Incidente confirmado pela organização

| | |
|---|---|
| CONFIRMADO | O comunicado ao mercado da Caixa Seguridade diz que a CVP identificou acesso não autorizado e cópia de cadastros em 6 de novembro. A base afetada inclui os 7,6 milhões de clientes ativos, além de antigos clientes. [S126] [S226] |
| CATEGORIAS | O comunicado confirma nomes e CPF. Alguns registros também contêm contato e data de nascimento. A avaliação preliminar não encontrou evidências de impacto em dados financeiros ou de autenticação. [S126] |
| LIMITE | A população de clientes ativos não é o total de pessoas únicas. O comunicado não estabelece ator nem autentica uma oferta clandestina. A avaliação financeira permanece preliminar e atribuída à empresa. |
| RESPOSTA | Delimite as categorias, use contatos confiáveis e prepare-se para falsificação de identidade com informações cadastrais genuínas. |

**Conclusão**

Delimite categorias copiadas e proteção dos clientes.

A resposta deve distinguir a base afetada de cada sistema que compartilha a marca controladora. Uma declaração sobre a investida não estabelece invasão de um banco relacionado. A aprovação de nomes se aplica a este caso e ao escopo divulgado.

L

CASO L

### Cadastros do Tesouro e uma base analítica separada

Administração pública

Incidente confirmado pela organização

| | |
|---|---|
| CONFIRMADO | O Ministério da Fazenda informa que o Tesouro Nacional detectou acesso não autorizado a dados pessoais em 4 de novembro. O comunicado de 13 de novembro identifica cerca de 30.000 cadastros de serviços e outra base com aproximadamente 4.000 chaves Pix. [S127][S227] |

| | |
|---|---|
| LIMITE | As bases não constituem uma contagem sem sobreposição de pessoas. O ministério afirma que não houve impacto financeiro e nenhum sistema estrutural foi afetado. São conclusões do ministério, sem alcance para todos os serviços governamentais. |
| RESPOSTA | Reveja categorias e acessos relevantes. Autentique por um canal independente os contatos que utilizem informações reais de pagamento. |

**Conclusão**

Mantenha cadastros e chaves Pix como populações separadas.

A presença de uma chave Pix não estabelece, por si só, capacidade de iniciar transferência. O contexto de pagamentos gera uma questão de proteção dos clientes sem demonstrar invasão do sistema de pagamentos. Mantenha as duas proposições separadas no registro.

## 5.3 Integridade de pagamentos e disponibilidade financeira

M

CASO M

### Alteração de guias em Belo Horizonte

Pagamentos municipais

Incidente confirmado pela organização

| | |
|---|---|
| CONFIRMADO | A nota oficial atualizada informa alteração de dados em algumas guias emitidas entre 14 e 16 de novembro. Cerca de 250 contribuintes pagaram guias Pix alteradas, e os recursos não chegaram ao município. [S233][S234] |
| ATUALIZAÇÃO | A prefeitura afirma que os valores afetados foram bloqueados e as devoluções automáticas começaram em 17 de novembro. A nota não confirma que todas as devoluções já terminaram. [S233] |
| LIMITE | O problema confirmado é a integridade da instrução de pagamento. A nota não estabelece ator, entrada ou invasão do núcleo do Pix. |
| RESPOSTA | Verifique beneficiários, identifique o intervalo afetado e concilie devoluções e novos pagamentos pelo processo autorizado. |

**Conclusão**

Concilie beneficiários, bloqueios e devoluções iniciadas.

O caso muda a pergunta de controle. Um pagamento pode começar em um serviço genuíno e apresentar uma instrução incorreta ao pagador. Teste quem pode alterar essa instrução e como o pagador ou a equipe detecta um beneficiário não autorizado.

CASO N

N

## Suspensão temporária do Pix no Banco do Nordeste

Bancos

Incidente confirmado pela organização

| | |
|---|---|
| CONFIRMADO | O comunicado de 26 de janeiro identifica incidente de cibersegurança na infraestrutura de transações Pix e suspensão temporária. Naquele momento, não haviam sido identificados vazamento ou prejuízo às contas dos clientes. [S101][S201] |
| LIMITE | A afirmação inicial sobre contas de clientes não estabelece ausência de perda financeira institucional. Não identifica ator nem demonstra entrada no sistema nacional de pagamentos. |
| RESPOSTA | Separe saldos de clientes, recursos próprios, disponibilidade e acesso a dados. Defina um responsável pelas evidências de cada resultado. |

**Conclusão**

Separe resultados dos clientes e da instituição ao longo do tempo.

Segundo o trecho indexado do relatório de administração do banco, referente ao primeiro semestre, a fraude cibernética de janeiro causou perda de R$292 milhões, com recuperação de R$148 milhões até junho. O documento completo não pôde ser revisado. [S231]

São valores de perda e recuperação informados pelo banco naquele momento. Não estimam perdas do setor financeiro brasileiro. O relatório não infere perda líquida final nem conecta o incidente a uma oferta específica de acesso.

## 5.4 Recuperação administrativa e continuidade operacional

CASO O

### Sistemas administrativos e procedimentos manuais em Santos

Administração portuária

Incidente confirmado pela organização

| | |
|---|---|
| CONFIRMADO | A APS informa que seus sistemas foram afetados em 6 de novembro. Atualizações de 16 e 17 de novembro descrevem recuperação administrativa gradual e canais alternativos. O relato de 17 de novembro menciona exclusão de dados descoberta após o reinício dos sistemas. [S128][S229] |
| LIMITE OPERACIONAL | A APS afirma que manteve capacidade de movimentação e acesso de navios, caminhões e trens. A Folha relata preocupações de usuários com lentidão e procedimentos manuais. São medidas diferentes. [S229][S228] |
| LIMITE | A sequência não estabelece que uma falta de energia causou a invasão. Não se estabelece família de ransomware, entrada ou total verificado de dados pessoais. |
| RESPOSTA | Teste serviço mínimo, autorização manual e conciliação posterior. Acompanhe tarefas reais dos usuários durante a recuperação administrativa. |

**Conclusão**

Teste contingência administrativa e tarefas reais.

A atualização de 19 de novembro descreve procedimentos contingenciais de acesso e cadastro e afirma não haver registro de incidente relacionado de segurança pública. A garantia permanece vinculada àquela data. Não significa que a recuperação administrativa estava concluída. [S230]

## 5.5 Outros casos e campanhas oficiais

P

CASO P

### Dados cadastrais históricos em órgão federal

Administração pública

Incidente confirmado pela organização

| | |
|---|---|
| CONFIRMADO | Um comunicado de setembro descreve ataque em 12 de junho envolvendo base cadastral estática com informações históricas até 2019. Distingue essa base das informações atuais controladas separadamente e dos dados sob sigilo fiscal. [S119] |
| LIMITE | Dados antigos podem continuar sensíveis, mas a nota não estabelece invasão do cadastro atual, total verificado de pessoas ou ator identificado. |
| RESPOSTA | Identifique exportações históricas, responsáveis e permissões. Ajuste a comunicação às categorias reais, sem presumir que a idade elimina o risco. |

**Conclusão**

Reveja exportações históricas sem presumir acesso atual.

Q

CASO Q

### Um serviço de alertas e canais alternativos

Alertas públicos

Incidente relatado por autoridade

| | |
|---|---|
| RELATADO | Autoridades estaduais e municipais descreveram suspensão de uma plataforma após alertas falsos não autorizados em junho. Os comunicados indicam comunicação alternativa e continuidade do monitoramento local. [S113] |
| LIMITE | Não estabelecem operador, entrada ou motivo político. Um alerta falso não comprova uma emergência física real. |
| RESPOSTA | Exercite publicação autorizada, revogação e canal alternativo confiável. Preserve uma explicação clara de qual mensagem é genuína. |

**Conclusão**

Autentique alertas e exercite canais alternativos.

R

CASO R

## Investigação de extorsão contra uma instituição

Serviços institucionais

Investigação policial; alegações

| | |
|---|---|
| RELATADO | A nota da PF sobre a Operação Insidioso, de 7 de outubro, informa que uma instituição relatou ataque em julho, extração de dados sensíveis e posteriores cobranças. A ação visou um suposto facilitador. [S122] |
| LIMITE | A investigação não estabelece família de ransomware, criptografia bem-sucedida, instituição nomeada ou condenação. Exigência de pagamento e criptografia são proposições separadas. |
| RESPOSTA | Preserve a cobrança e as evidências de acesso. Exercite restauração e resposta à perda de dados sem esperar um rótulo de família. |

**Conclusão**

Prepare restauração e resposta à perda de dados separadamente.

S

CASO S

## Investigação sobre comercialização de dados de saúde

Dados de saúde

Investigação policial; alegações

| | |
|---|---|
| RELATADO | A Operação Glycon, anunciada pela PF em fevereiro, trata de suposto acesso, tratamento e uso comercial não autorizados de informações clínicas por serviço oferecido a profissionais de saúde. [S102] |
| LIMITE | Alegações policiais não são condenação. Não se estabelece total nacional de registros, entrada ou responsabilidade de cada profissional participante. |
| RESPOSTA | Valide fontes legítimas e permissões. Reveja exportações sensíveis e o canal de apoio a pessoas afetadas. |

**Conclusão**

Valide fontes legais e permissões de dados sensíveis.

Os dois casos policiais descrevem condutas alegadas diferentes. Não são ligados aos anúncios ou às famílias de malware sem evidências de apoio. As datas das operações também não estabelecem quando toda a conduta começou.

## 5.6 Outras divulgações em serviços

T

CASO T

### Unimed Natal separa atendimento e recuperação de sistemas

Saúde

Incidente confirmado pela organização

| | |
|---|---|
| CONFIRMADO | A nota de 14 de novembro informa investigação de incidente, protocolos de contenção e recuperação com especialistas. Afirma continuidade dos serviços assistenciais e hospitalares, com procedimentos alternativos quando necessários. [S166][S266] |
| LIMITE | A nota não confirma roubo, ator, família de ransomware, pessoas afetadas ou restauração concluída. O escopo é a Unimed Natal, sem estabelecer incidente em todas as organizações que compartilham a marca mais ampla. |
| RESPOSTA | Teste processos clínicos e administrativos separadamente. Mantenha canal confiável para autorizações e atendimento durante a recuperação dos aplicativos. |

**Conclusão**

Separe continuidade clínica e recuperação de aplicativos.

Notícias locais posteriores descrevem recuperação gradual e aplicativo indisponível. Os detalhes permanecem atribuídos à imprensa, sem substituir a declaração oficial datada sobre atendimento. Não se infere dano a pacientes nem fechamento hospitalar. [S266]

U

CASO U

### Incidente de outubro em portal divulgado em novembro

Benefícios de saúde

Nota oficial: texto completo não revisado

| | |
|---|---|
| RELATADO | Comunicado oficial indexado de 19 de novembro descreve acesso não autorizado ao portal de benefícios de saúde em 18 de outubro e phishing no dia seguinte. As categorias verificadas de prestadores pessoa jurídica incluem razão social, CNPJ, e-mail, dados bancários e hash de senha. [S165] |
| LIMITE | O documento completo não pôde ser revisado. Populações de prestadores pessoa física e beneficiários não são reconstruídas de outras notas. Não se estabelece total de prestadores, senha em texto aberto ou prontuário divulgado. |

| | |
|---|---|
| RESPOSTA | Valide contatos, dados de pagamento e acesso pertinente. Diferencie hash e senha em texto aberto e estabeleça a resposta adequada para as contas. |

**Conclusão**

Valide escopo dos prestadores e phishing posterior.

A avaliação preliminar aponta roubo de credencial privilegiada por phishing ou outro método externo à infraestrutura do portal. Permanece atribuída e provisória. O caso não estabelece acesso a sistemas de pagamento ou de supervisão. [S165]

CASO V

V

## SES-MT e continuidade do licenciamento sanitário compartilhado

Administração da saúde

Incidente compartilhado confirmado por autoridade

| | |
|---|---|
| CONFIRMADO | A declaração de 2 de novembro da SES-MT descreve ataque detectado em 1 de novembro e suspensão temporária de sistemas para verificações. Afirma continuidade hospitalar, de urgência e emergência com limitações de rede, enquanto a restauração seria gradual. [S268][S269] |
| EFEITO COMPARTILHADO | Cuiabá informa em 9 de novembro indisponibilidade da plataforma estadual de vigilância sanitária desde 3 de novembro. Protocolos, ordens de serviço, demandas de fiscais e licenças foram afetados, com prazos administrativos prorrogados automaticamente. [S167][S270] |
| LIMITE | São etapas e efeitos de um incidente estadual. Não estabelecem segunda invasão em Cuiabá, roubo de dados de pacientes, família de ransomware, vítimas ou restauração concluída. |
| RESPOSTA | Mapeie dependências de licenciamento e administração junto da continuidade clínica. Registre aprovações alternativas e mudanças de prazo que precisarão de conciliação. |

**Conclusão**

Mapeie licenciamento compartilhado sem criar outra invasão.

A garantia de atendimento estadual está vinculada à data da nota. O comunicado municipal estabelece efeito administrativo específico, sem demonstrar dano ao atendimento clínico. Não são importadas quantidades ou atribuições contestadas de outro evento anterior.

CASO W

## W ■ BTG Pactual separa disponibilidade do Pix e acesso a contas

Bancos

Carta da instituição em cópia; conclusões datadas

| | |
|---|---|
| CONFIRMADO | Carta da instituição datada de 24 de março descreve atividade atípica no Pix em 22 de março, suspensão preventiva e retomada no início de 23 de março. A cobertura independente confirma o episódio e a suspensão. [S300] [S301] |
| LIMITE DA FONTE | A carta assinada foi lida em site de terceiros. A rota oficial do documento foi identificada, mas seu conteúdo não pôde ser comparado a cópia legível no site oficial. |
| LIMITE | O banco afirma que contas de clientes não foram acessadas e dados de correntistas não foram expostos. São conclusões atribuídas, sem estabelecer ausência de perda para a instituição. |
| RESPOSTA | Designe responsáveis distintos pela disponibilidade, acesso às contas e recursos institucionais. Concilie transações afetadas antes de adotar estimativa de perda. |

**Conclusão**

Concilie disponibilidade, acesso de clientes e recursos institucionais.

A solicitação regulatória anexada à carta cita estimativa preliminar da imprensa. Não estabelece perda líquida final nem valor recuperado. Este relatório não adota estimativa monetária nem julga a relevância da divulgação. [S300]

CASO X

## X ■ Sírio-Libanês investiga possível acesso a relatórios de projetos

Projetos de saúde

Investigação confirmada; possível acesso

| | |
|---|---|
| INVESTIGAÇÃO CONFIRMADA | As perguntas e respostas oficiais do hospital identificam possível acesso não autorizado a sistema de relatórios de projetos sociais, descoberto em 21 de setembro. A cobertura de outubro confirma a investigação. [S302][S303] |
| CATEGORIAS | A nota lista informações de identidade, contato e saúde relacionadas aos programas potencialmente afetadas. Não confirma acesso a todas as categorias nem estabelece total de pessoas atingidas. [S302] |
| LIMITE | |

O hospital afirma que o atendimento continuou e que não havia identificado evidências de divulgação pública ou uso indevido. O possível acesso e sua extensão exata permaneciam sob investigação.

| | |
|---|---|
| RESPOSTA | Separe relatórios dos programas e sistemas clínicos. Identifique as categorias reais e comunique as pessoas por canal confiável adequado ao escopo estabelecido. |

**Conclusão**

Valide o programa sem inferir acesso à base geral de pacientes.

Confirmar a investigação não confirma toda alegação online. O relatório não infere família de ransomware, acesso à base geral de pacientes, recuperação concluída ou conclusão jurídica pelo intervalo entre descoberta e notícia pública.

Y

CASO Y

### Plataforma de ativos digitais e nota de evento subsequente do investidor

Serviços de ativos digitais

Cópia de documento do investidor: efeito financeiro incerto

| | |
|---|---|
| RELATADO POR INVESTIDOR | Demonstração financeira elaborada por investidor identifica ataque cibernético a plataforma de ativos digitais em 2 de novembro. O documento foi autorizado em 12 de novembro e lido em cópia independente. [S169] |
| LIMITE | O investidor afirma que possíveis perdas e efeitos na avaliação ainda não podiam ser estimados com confiabilidade. A cópia não foi comparada a documento legível em site oficial. Perda final, recuperação e ressarcimentos não estão estabelecidos. |
| RESPOSTA | Separe disponibilidade, conciliação de ativos e obrigações com clientes. Use atualização validada do operador responsável antes de presumir conclusão de saques ou devoluções. |

**Conclusão**

Concilie ativos e obrigações com atualizações validadas.

A plataforma mantém descrição genérica. Uma distribuição de 30 de outubro discutida no mesmo documento não é a data do ataque. Estimativas da imprensa não são adotadas como resultado financeiro final. [S169]

CASO Z

Z

## Portal de projetos com acesso confirmado a dados cadastrais

Serviços financeiros de projetos

Nota oficial: nome omitido

| | |
|---|---|
| CONFIRMADO | A nota oficial de uma instituição financeira afirma que o incidente foi identificado e contido em 4 de outubro. Identifica acesso não autorizado a dados de identidade, contato, credenciais e contas de financiamento de projetos. [S172] |
| LIMITE | A página não estabelece data de publicação, total de pessoas, exposição de senha em texto simples, ator ou resultado financeiro final. A previsão de indisponibilidade do portal não estabelece restauração até este corte. |
| RESPOSTA | Contate usuários por rota confiável, valide credenciais pertinentes e proteja dados de pagamento dos projetos. Defina a função mínima do portal e concilie trabalho adiado após a recuperação. |

**Conclusão**

Valide credenciais e dados de pagamento de projetos.

O nome permanece omitido porque não se estabeleceu cobertura independente suficientemente ampla. Um incidente separado de dezembro de 2025 discutido em demonstrações posteriores não é ligado ao episódio de outubro. [S172]

## 5.7 Atividade recente: 8 a 22 de novembro

A quinzena final inclui comunicados, atualizações, anúncios e operações sobre condutas anteriores. Não deve ser lida como contagem de novas invasões em novembro.

| Publicação ou atualização | Item | Evidência e limite temporal | Primeira resposta |
|---|---|---|---|
| 9 de novembro | Atualização de serviço compartilhado em Cuiabá | Incidente estadual em 1 de novembro; licenças afetadas, sem segunda invasão municipal [S167][S268] | Conciliar licenças e prazos prorrogados |
| 11 de novembro | Anúncio de contatos associados a banco | Não verificado; a atualidade alegada pertence ao vendedor [S1] | Validar origem e contas da organização |
| 12 de novembro | Comunicado da CVP | Descoberta em 6 de novembro; clientes atuais e antigos [S126][S226] | Delimitar categorias e proteção dos clientes |

| Publicação ou atualização | Item | Evidência e limite temporal | Primeira resposta |
|---|---|---|---|
| 12 de novembro | Demonstração de investidor | Descreve evento de 2 de novembro em plataforma de ativos digitais; efeito financeiro final incerto [S169] | Concilie ativos e obrigações |
| 13 de novembro | Comunicado do Tesouro | Descoberta em 4 de novembro; duas populações distintas [S127] | Validar acesso e contatos confiáveis |
| 13 de novembro | Notícia de aviso em comércio digital | Conhecimento empresarial relatado em 12 de outubro; sem nova data de invasão nem conclusão jurídica [S173] | Estabeleça categorias e escopo da comunicação |
| 13 de novembro | Notícia de investigação em plataforma de segurança pública | Relatos policiais e municipais citados pela imprensa; alegação sobre usuário legítimo separada de notícias sobre câmeras de fornecedor [S323] | Valide permissões, dados e limites dos serviços |
| 14 de novembro | Nota da Unimed Natal | Atendimento continuou com alternativas; sem roubo ou restauração concluída estabelecidos [S166][S266] | Testar funções clínicas e administrativas separadamente |
| 15 de novembro | Notícia de tentativas contra site educacional | Relato ministerial atribuído; sem acesso bem-sucedido ou origem estabelecida [S309] | Valide evidências do serviço |
| 16–19 de novembro | Recuperação e contingência em Santos | Um incidente iniciado em 6 de novembro [S128][S229] [S230] | Testar administração e operação separadamente |
| 16–19 de novembro | Guias e devoluções em Belo Horizonte | Guias alteradas em 14–16 de novembro; devoluções iniciadas depois [S233] | Conciliar beneficiários, devoluções e novos pagamentos |
| 16 de novembro | Notícia de exposição de arquivos judiciais | Confirmação atribuída ao tribunal em 14 de novembro; nota direta indisponível, sem ator estabelecido [S179] | Valide arquivos e preserve o limite do serviço |
| 16–19 de novembro | Atualizações de orientações do CTIR | Orientações de correio e servidor web atualizadas; gestão de conteúdo atualizada em 10 de novembro; sem contagem de incidentes [S320][S321][S322] | Relacione serviços implantados às orientações oficiais atuais |
| 17 de novembro | Anúncio de base associada ao Pix | Material explicitamente de 2025; sem nova invasão de 2026 estabelecida [S1] | Verificar idade e origem antes da contenção |

| Publicação ou atualização | Item | Evidência e limite temporal | Primeira resposta |
|---|---|---|---|
| 17 de novembro | Anúncio internacional Radar pela PF | Ações de maio a setembro; oito domínios desativados no Brasil [S129] | Usar avisos relevantes sem importar totais internacionais |
| 17 de novembro | Investigação sobre contas de benefícios | Alegação de acesso e transferências não autorizados; sem condenação [S130] | Validar contas e transações afetadas |
| Nota de 17 de novembro | Investigação de lista acadêmica | Nota direta confirma investigação; indisponibilidade separada por falha de equipamentos não foi maliciosa, segundo a universidade [S196] | Separe avaliação da exposição e restauração do hardware |
| 18 de novembro | Reportagem sobre dados bancários | Imprensa cita uso indevido de credencial válida; declaração direta indisponível [S131] | Distinguir da invasão dos sistemas do banco |
| Notícias de 18–19 de novembro | Acesso a cadastros bancários | Nota bancária citada pela imprensa descreve detecção em 12 de novembro e revogação da credencial; nota integral direta indisponível [S194] | Separe acesso cadastral das conclusões bancárias sobre ausência de invasão e transações relacionadas |
| 19 de novembro | Reportagem sobre plataforma de entregas | Imprensa cita resposta da empresa; categorias e populações diferentes [S132] | Obter escopo oficial específico por população |
| 19 de novembro | Comunicado sobre portal de benefícios de saúde | Acesso e phishing em outubro; escopo de prestadores pessoa jurídica [S165] | Validar contatos, pagamentos e acesso |
| 19 de novembro | Anúncio de tabela de clientes de software | Alegação de dados associados a fornecedor, não verificada [S1] | Validar escopo do fornecedor e dos clientes |
| 19 de novembro | Investigação sobre instalação telefônica | Operação em 18 de novembro; equipamentos e atividade sob investigação [S133] | Rever abuso de mensagens e verificação independente |
| Notícias de 19 de novembro | Comunicado de plataforma de entregas | Relato atribuído à empresa identifica contenção em 14 de novembro, com categorias diferentes conforme o público [S195] | Oriente cada população; não infira acesso a contas de pagamento |
| Nota à imprensa de 20 de novembro | Portal de informação pública | Declaração institucional reproduzida pela imprensa descreve possível ataque e site indisponível [S197] | Preserve a incerteza e valide a situação atual do serviço |

| Publicação ou atualização | Item | Evidência e limite temporal | Primeira resposta |
|---|---|---|---|
| Publicação de 22 de novembro | Alegação de exportação de informações empresariais [S1] | Publicação de fórum descreve supostos dados de diretórios, perfis profissionais e solicitações de suporte | Alegação do autor; sem registros autenticados nem conclusão sobre pacientes, invasão ou acesso atual |
| Publicação de 22 de novembro | Alegação de exportação de gestão de clientes [S1] | Oferta separada descreve supostos registros de contatos, projetos de sites e solicitações de suporte | Sem origem autenticada, acesso atual, data de obtenção, impacto nos clientes ou venda estabelecidos |
| Pesquisa de novembro | Campanha multinacional de terminais de pagamento | Descoberta em agosto, sem demonstrar novas infecções em novembro [S232] | Validar software e investigar endpoints relevantes |

Os relatos bancário e de plataforma permanecem atribuídos à imprensa, com nomes omitidos por falta de registro da fonte oficial direta. Suas exclusões devem acompanhar o evento: não se acrescenta impacto em senhas, tokens ou dados de pagamento sem suporte.

## 5.8 Exclusões importantes e contexto histórico

| Item | Tratamento | Motivo |
|---|---|---|
| Operação de março sobre lavagem em fornecedor de pagamentos | Contexto de investigação [S104] | Suposta invasão original em agosto de 2025 |
| Processo regulatório de julho sobre operadora de saúde | Contexto regulatório [S114] | Ransomware de 2025; processo não é sanção final |
| Ação municipal sobre dados de saúde em outubro | Resultado regulatório [S125] | Divulgação em diário oficial ocorreu em setembro de 2025 |
| Investigação transnacional de lavagem | Contexto de investigação [S117] | Instituição estrangeira e invasão histórica |
| Mensagem de encerramento de conta bancária | Excluída dos exemplos maliciosos [S112] | Fonte atribui o fato a erro de comunicação operacional |
| Desligamento preventivo em órgão | Resposta preventiva [S124] | Autoridade afirma que não houve invasão nem vazamento de documentos |
| Entradas recentes de agregadores sem confirmação | Não tratadas como incidentes confirmados | Divulgação original e identidade do evento não estabelecidas |
| Notícia financeira identificada como ficção | Excluída integralmente [S189] | O artigo descreve expressamente cenário fictício, sem incidente verificado |

| Item | Tratamento | Motivo |
|---|---|---|
| Notícias históricas de universidade, energia, saúde e logística | Fora dos novos eventos [S184][S190] [S191][S192][S193] | Eventos anteriores ou mudanças sem data; visibilidade atual na busca não estabelece nova invasão |
| Manchete de alerta falso citando regulador | Mesmo episódio da plataforma de avisos [S187][S113] | Sem incidente separado nos sistemas do regulador ou caso adicional |

Essas exclusões preservam o significado do ano. Uma página atual pode descrever uma invasão anterior, uma investigação ou uma precaução. Nenhuma deve virar silenciosamente outra invasão confirmada de 2026.

## 5.9 Outras divulgações e notícias com limites definidos

| Publicação ou evento | Papel e fonte | Informação sustentada | Limite preservado |
|---|---|---|---|
| Notícia de 21 de abril | Instituição financeira [S310] | A imprensa reproduz nota bancária sobre incidente e normalização gradual | Sem perda ou total de contas autorizado; nome omitido |
| Identificação em 1 de junho | Cooperativa financeira [S174] | Nota oficial identifica dados pessoais, contatos e relações de contas e contratos | A cooperativa exclui senhas e dados para transações; data da publicação incerta |
| Evento de 21 de julho; notícia de 27 de julho | Rede de serviços financeiros de varejo [S311] | Restrições temporárias após atividade atípica relatada | Relatos individuais não são perda nacional; nota direta indisponível |
| Incidente de 17 de setembro; notas posteriores | Plataforma de depósitos judiciais [S175] | Notas judiciais descrevem restauração gradual informada pelo banco | Sistemas judiciais separados da plataforma bancária; estimativas de perda não adotadas |
| Suspeita em 4 de agosto; nota de 8 de outubro | Hospital [S181] | Declaração do hospital confirma acesso e obtenção de dados; atendimento continuou segundo a instituição | Fonte reproduzida pelo destinatário original; total desconhecido, sem uso público indevido identificado então |
| Notícias de maio | Serviço de consulta de benefícios [S170] | Cobertura independente cita relato do operador sobre acesso a dados | Terminologia das populações e evidência original incertas; fora dos casos nomeados confirmados |
| Atualização de 5 de novembro | Instituição do setor financeiro [S177] | HTML oficial confirma acesso não autorizado ligado a processos de pagamento após suspeita de 26 de outubro | Investigação e avisos individuais continuavam; sem total ou resultado final de dano |
| Nota de 21 de setembro | Serviços judiciais compartilhados [S178] | Nota oficial descreve acessos detectados em 18 de agosto e 3 de setembro, com ambos os sistemas restaurados | Datas distintas não estabelecem ator comum nem invasão em cada tribunal regional |

| Publicação ou evento | Papel e fonte | Informação sustentada | Limite preservado |
|---|---|---|---|
| Notícia de 27 de outubro | Portal de informações públicas [S180] | Declaração do operador descreve imagens alteradas e suspensão preventiva | Operador não identificava impacto mais amplo ou em dados sensíveis naquele momento; investigação continuava |
| Nota de 23 de fevereiro | Prestador de serviços de exames [S182] | Nota oficial confirma instabilidade em 20 de fevereiro e prorrogação de prazo | Sem confirmação oficial de ransomware, extração ou ator |
| Notícia de 30 de abril | Prestador de serviços financeiros [S183] | Nota atribuída ao banco descreve suspensão preventiva após movimento atípico | Banco não confirmara ataque; afirmações de ausência de perdas ou vazamento permanecem atribuídas |
| Interrupção em outubro; atualização de 6 de novembro | Plataforma judicial eletrônica [S185] | Relato próprio de entidade profissional descreve interrupção externa e medidas de continuidade | Relato de participante; fonte direta do operador indisponível, sem invasão ou roubo de dados estabelecido |
| Detecção em 12 de novembro; notícias de 18–19 de novembro | Banco [S194][S325] | Imprensa cita nota bancária confirmando acesso cadastral não autorizado por uso indevido de credencial válida, depois revogada | Nota integral direta indisponível; segundo o banco, sem invasão, exposição de senhas/tokens ou transações relacionadas identificadas; sem total de pessoas |
| Identificação em 14 de novembro; notícias de 19 de novembro | Plataforma de entregas [S195][S326] | Nota atribuída à empresa distingue telefones de clientes, telefone/CPF de parceiros e dados variáveis de entregadores, inclusive contas para repasses em alguns casos | Nota direta indisponível; não atribua todos os campos a todos nem infira acesso à conta; empresa exclui impacto em senhas/cartões e informa continuidade |
| Nota de 17 de novembro; cobertura de 21 de novembro | Universidade pública [S196] [S327] | Nota oficial investiga lista exposta de nomes, cursos e coeficientes de rendimento acadêmico | Sem invasão, origem ou total de pessoas estabelecidos; indisponibilidade separada por falha de hardware não foi maliciosa, segundo a instituição |
| Nota à imprensa de 20 de novembro | Portal de informação pública [S197][S328] | Declaração institucional integral reproduzida por dois veículos descreve possível ataque e portal indisponível | Fonte direta indisponível; sem furto, ator, impacto em sistemas mais amplos ou recuperação concluída confirmados |

## Dados de clientes de energia: exposição sem invasão operacional estabelecida

O fato relevante da Cemig de 14 de maio identifica exposição de dados de aproximadamente 135.000 clientes identificados naquele estágio. As categorias incluem cadastros, contatos, CPF e valores de faturas. A cobertura independente confirma a divulgação. [S314][S315]

A empresa afirma que o acesso não autorizado foi bloqueado após a detecção e as operações não foram afetadas. São conclusões empresariais datadas. Não estabelecem acesso a sistemas de controle elétrico, interrupção, ator ou total final de pessoas afetadas. [S314]

Na proteção de clientes, dados genuínos de faturas e identidade podem tornar convincente uma cobrança não autorizada. Valide beneficiários e contatos de suporte de forma independente. Separe essa resposta de proteção de dados de investigação operacional, salvo evidência que estabeleça ligação.

As linhas preservam acontecimentos sustentados sem transformar cada notícia em dossiê plenamente verificado. Não autenticam anúncio clandestino nem estabelecem ator comum. Intervalos de comunicação não são usados para decidir conformidade jurídica.

PRINCIPAIS CONCLUSÕES

**01**

Cadastros copiados, instruções alteradas e administração indisponível exigem responsáveis diferentes.

**02**

Publicações recentes frequentemente atualizam incidentes ou investigações anteriores.

**03**

Preserve conclusões iniciais e posteriores sem ampliar indevidamente suas garantias.

CAPÍTULO 06

# Interrupções, desfiguração de sites e confiança nos serviços públicos

ESTE CAPÍTULO RESPONDE

O serviço ficou indisponível, foi alterado ou apenas citado?

**2025**

ano do evento indicado em uma alegação de interrupção que circulou em 2026


6.1 Uma alegação histórica circulando no período atual 59
6.2 Três tipos de dano aos serviços públicos 60
6.3 Uma sequência de evidências para alegações de indisponibilidade 61
6.4 O calendário de outubro fornece contexto, não atribuição 61
6.5 Cronologia: datas com seu tipo de evidência 62
6.6 Decisões de continuidade que resistem à atribuição incerta 62
6.7 O que fortaleceria ou mudaria a avaliação 63

CAPÍTULO 06

# Interrupções, desfiguração de sites e confiança nos serviços públicos

EM RESUMO

A linguagem de interrupção é fácil de repetir e difícil de validar. Uma narrativa publicada em janeiro alega negação de serviço, mas situa a suposta indisponibilidade em janeiro de 2025. Fontes oficiais descrevem separadamente alertas públicos falsos, desfiguração por uploads e recuperação administrativa. Nenhuma sustenta aqui uma interrupção nacional ligada à eleição. Avalie a tarefa do usuário, preserve a data e diferencie disponibilidade do site e controle do serviço. Teste um canal público alternativo antes do próximo incidente.

## 6.1 Uma alegação histórica circulando no período atual

Uma publicação de janeiro e sua repetição em outubro alegam negação de serviço e extração de dados em um órgão ambiental estadual. A narrativa situa explicitamente a indisponibilidade em 9 de janeiro de 2025. A circulação pertence a 2026; a suposta interrupção, não. [S1]

O material não estabelece de forma independente duração, alcance geográfico, causa ou efeito operacional. Suas acusações políticas não acrescentam evidência técnica e foram omitidas. O nome do órgão permanece reservado por não atender aos requisitos de identificação de incidentes.

**Publicação atual não significa incidente atual.** A distinção muda a cronologia e a resposta. Uma nova alegação sobre evento antigo pode justificar revisão de registros ou atenção a golpes. Não justifica anunciar nova interrupção nem atribuir problemas atuais ao autor.

| Proposição | O que está retido | O que não está estabelecido |
|---|---|---|
| Uma alegação de negação de serviço circulou em 2026 | Narrativa datada e repetições | Medições independentes de tráfego ou serviço |
| A narrativa indica data anterior | O autor menciona janeiro de 2025 | Cronologia autenticada do evento |
| Há uma quantidade alegada de dados | A afirmação do anúncio | Dados autênticos, pessoas únicas ou transferência verificada |
| A narrativa contém linguagem política | A fonte contém defesa de posições | Atribuição técnica, mandato público ou motivo validado |

A próxima etapa útil é a verificação interna pelo responsável real pelo serviço. Compare horário, relatos de usuários, avisos de fornecedores e registros operacionais. Uma afirmação anônima não resolve se a falha foi hostil, acidental ou não relacionada.

## 6.2 Três tipos de dano aos serviços públicos

Disponibilidade significa que o usuário consegue concluir a tarefa. Integridade significa apresentar e registrar a informação correta. Confidencialidade significa impedir acesso não autorizado à informação. Um incidente pode afetar várias dimensões, mas evidência de uma não estabelece as demais.

O caso de alertas do capítulo 5 envolve mensagens falsas e suspensão de plataforma, com alternativas descritas pelas autoridades. Levanta questões de autenticidade e continuidade. Não estabelece emergência real, identidade do atacante ou falha de todo o monitoramento local. [S113]

O alerta de uploads do CTIR descreve desfiguração de plataformas públicas. Quando validada, uma página alterada evidencia problema de integridade de publicação. Não estabelece, por si só, acesso a toda a organização, a sistemas eleitorais ou ao controle operacional. [S152]

As atualizações de Santos tratam de recuperação administrativa e acesso contingencial. A afirmação de capacidade de cargas mantida deve acompanhar os relatos de lentidão. Capacidade, demora transacional e restauração são medidas diferentes. [S229][S228]

Declaração de operador de 5 de novembro, reproduzida pela imprensa especializada, descreve volume excepcional de DDoS nos seis meses anteriores. O operador afirma que o ambiente de serviços digitais governamentais não sofreu interrupção ou invasão. Não há quantidade pública de tráfego nem atribuição estabelecida. [S171]

Separadamente, notícia de 15 de novembro cita ministro da Educação relatando tentativas contra site de avaliação e afirmando que foram controladas. Não fornece conclusão de acesso bem-sucedido, total de tentativas ou origem estabelecida. Nenhum relato estabelece impacto em sistemas eleitorais. [S309]

Nota universitária de 22 de outubro descreve restrições preventivas de serviços após alerta de segurança. Afirma expressamente que não havia identificado invasão ou acesso indevido aos sistemas naquele momento. Indisponibilidade preventiva deve permanecer separada de resultado hostil confirmado. [S308]

Nota sindical de setembro descreve ataque ao serviço de votação online e remarcação de assembleia. Embora os participantes fossem bancários, a nota não estabelece incidente na infraestrutura do banco ou nas contas de clientes. Separe o dono do serviço e o empregador dos participantes. [S188]

## 6.3 Uma sequência de evidências para alegações de indisponibilidade

| Evidência | Conclusão adequada | Uso operacional |
|---|---|---|
| Um autor cita um site | O autor afirmou direcionamento | Avisar o responsável pelo canal acordado e verificar relevância |
| Uma imagem mostra erro | A página falhou naquele contexto exibido | Reproduzir a tarefa no monitoramento autorizado |
| O responsável confirma degradação | Um problema delimitado foi confirmado | Aplicar prioridades de continuidade e publicar atualização datada |
| Registros mostram tráfego hostil anormal | Há evidência técnica para investigação | Coordenar mitigação e preservar registros |
| Investigação competente atribui a atividade | Existe atribuição com confiança declarada | Atribuir a conclusão à fonte e preservar seus limites |

São etapas analíticas de resposta, sem constituir nota ou afirmar que a etapa final ocorreu no caso histórico. Uma imagem pode mostrar falha real e deixar a causa sem resposta. Evite apresentá-la como medição de disponibilidade nacional.

## 6.4 O calendário de outubro fornece contexto, não atribuição

O calendário oficial marcou o primeiro turno em 4 de outubro e eventual segundo turno em 25 de outubro. Isso cria um período previsível de planejamento da comunicação e continuidade. Não estabelece relação entre o calendário e um incidente. [S17]

Esta edição não identifica, nas evidências apresentadas, evento nacional de DDoS eleitoral verificado na fonte. Esse limite de cobertura não afirma ausência de tentativas. Sites públicos, campanhas, tribunais e serviços eleitorais são objetos distintos, com responsáveis diferentes.

O relatório não toma posição sobre candidatos, partidos, decisões judiciais, políticas públicas ou relações exteriores. Quando relevante, uma descrição política permanece atribuída ao autor. Não substitui evidência do serviço, e acusações carregadas não são reproduzidas.

Verifique a função afetada antes de usar um cenário eleitoral. Trata-se de página informativa, e-mail de pessoal, serviço de campanha ou sistema de administração eleitoral? A resposta define o responsável pela continuidade e a declaração pública adequada.

Uma republicação de 26 de outubro afirma que um ator divulgou dados de uma organização política após alegação anterior de invasão. A atribuição e a divulgação permanecem não verificadas. A publicação não autentica conteúdo, origem, total de pessoas únicas ou impacto eleitoral. Não estabelece ligação comprovada com a oferta anterior de filiação. Valide a organização e o serviço afetado sem adotar o enquadramento político do autor. [S1]

## 6.5 Cronologia: datas com seu tipo de evidência

| | |
|---|---|
| 24 jan 2026 | **Autor do fórum**<br>Circula uma alegação de interrupção explicitamente situada em janeiro de 2025 [S1] |
| 21 mai 2026 | **Fonte oficial**<br>CTIR publica orientação sobre desfiguração por uploads; datas individuais não estabelecidas [S152] |
| 20 jun 2026 | **Fonte oficial**<br>Comunicados descrevem alertas falsos e canais alternativos [S113] |
| 8 set 2026 | **Fonte oficial**<br>CTIR alerta sobre manipulação de resultados de busca em serviços públicos [S120] |
| 4 out 2026 | **Fonte oficial**<br>Data oficial do primeiro turno eleitoral [S17] |
| 7 out 2026 | **Fonte oficial**<br>PF anuncia investigação de roubo de dados e extorsão ocorrido em julho [S122] |
| 16 nov 2026 | **Fonte oficial**<br>Santos publica atualização administrativa sobre o incidente de 6 de novembro [S128] |
| 19 nov 2026 | **Fonte oficial**<br>Belo Horizonte atualiza sua nota sobre guias e devoluções [S233] |

As entradas distinguem alegações, orientações oficiais, contexto do calendário e relatos de incidentes. Não é um gráfico de contagem de incidentes. Várias publicações tratam de atividades anteriores e não devem ser somadas como interrupções simultâneas.

## 6.6 Decisões de continuidade que resistem à atribuição incerta

Primeiro, defina a tarefa pública mínima. Um porto pode precisar de cadastro e acesso seguros antes de recuperar toda a administração. Um município pode precisar de pagamento verificado antes de restaurar o desenho normal da página. A prioridade cabe ao responsável operacional.

Segundo, estabeleça um canal alternativo confiável antes de o principal falhar. Explique sua finalidade e autenticação em condições normais. Durante o incidente, date as atualizações e indique funções operantes, atrasadas e ações a evitar.

Terceiro, preserve a integridade na contingência. Um processo manual pode manter o serviço e introduzir riscos de conciliação, aprovação ou fraude. Defina quem valida beneficiários, registra exceções e concilia o sistema definitivo.

Quarto, teste a recuperação pelas tarefas dos usuários. Um servidor acessível não demonstra que agendamento, pagamento ou embarque funcionem corretamente. Peça à operação que demonstre a tarefa necessária e registre o resultado.

Por fim, mantenha as declarações proporcionais aos fatos. Informe o que o responsável confirmou, quando concluiu e quando haverá atualização. Separe alegações em investigação de condições observadas do serviço.

## 6.7 O que fortaleceria ou mudaria a avaliação

Interrupção atual confirmada independentemente, nota oficial, registros corroborados ou atribuição técnica competente fortaleceriam uma conclusão específica. A evidência precisa identificar função e data do evento, sem apenas repetir a alegação.

Negativa posterior ou causa não maliciosa documentada também mudaria a avaliação. Preserve a correção no mesmo registro. Retirar uma incerteza sem registrar a nova fonte reduz a utilidade para os defensores.

PRINCIPAIS CONCLUSÕES

**01**

Separe a data de publicação da data da suposta indisponibilidade.

**02**

Disponibilidade, integridade de mensagens e acesso a dados exigem evidências diferentes.

**03**

Exercite canais alternativos confiáveis e concilie todos os registros de contingência.

CAPÍTULO 07

# Ransomware, grupos com motivação financeira e espionagem

ESTE CAPÍTULO RESPONDE

Quais rótulos de atores ajudam uma decisão?

**206**

listagens de ransomware associadas ao Brasil durante o período


7.1 A população de listagens de ransomware 65
7.2 Quatro comparadores regionais 68
7.3 Identidades de pagamento: BREEZE COMET 69
7.4 Malware bancário: TCLBANKER 70
7.5 Identidade no navegador: UnregStealer 71
7.6 Espionagem e roubo de informações: Armored Likho 72
7.7 Outras pesquisas financeiras relevantes para o Brasil 73
7.8 Alertas oficiais e o responsável pelo controle 75
7.9 Mapa de relações e visão de técnicas 76

CAPÍTULO 07

# Ransomware, grupos com motivação financeira e espionagem

EM RESUMO

A Ransompedia registra 206 listagens associadas ao Brasil, distribuídas entre 55 rótulos de grupos. Três rótulos somam 72 listagens, ou 35,0% do total. Listagens continuam sendo alegações. Pesquisas separadas descrevem roubo de identidades de pagamento, malware bancário, sessões de navegador e uma campanha atribuída de espionagem. As fontes não estabelecem operadores comuns ou total nacional de vítimas. Priorize controles de acesso e recuperação sustentados por cada fonte, em vez de usar o nome do ator como plano de controle.

## 7.1 A população de listagens de ransomware

**A contagem descreve visibilidade pública de extorsão.** A Ransompedia registra 206 listagens associadas ao Brasil entre 1 de janeiro e 22 de novembro de 2026. Registra 160 em todo o ano de 2025. São períodos distintos, sem representar crescimento anual entre intervalos equivalentes. [S2]

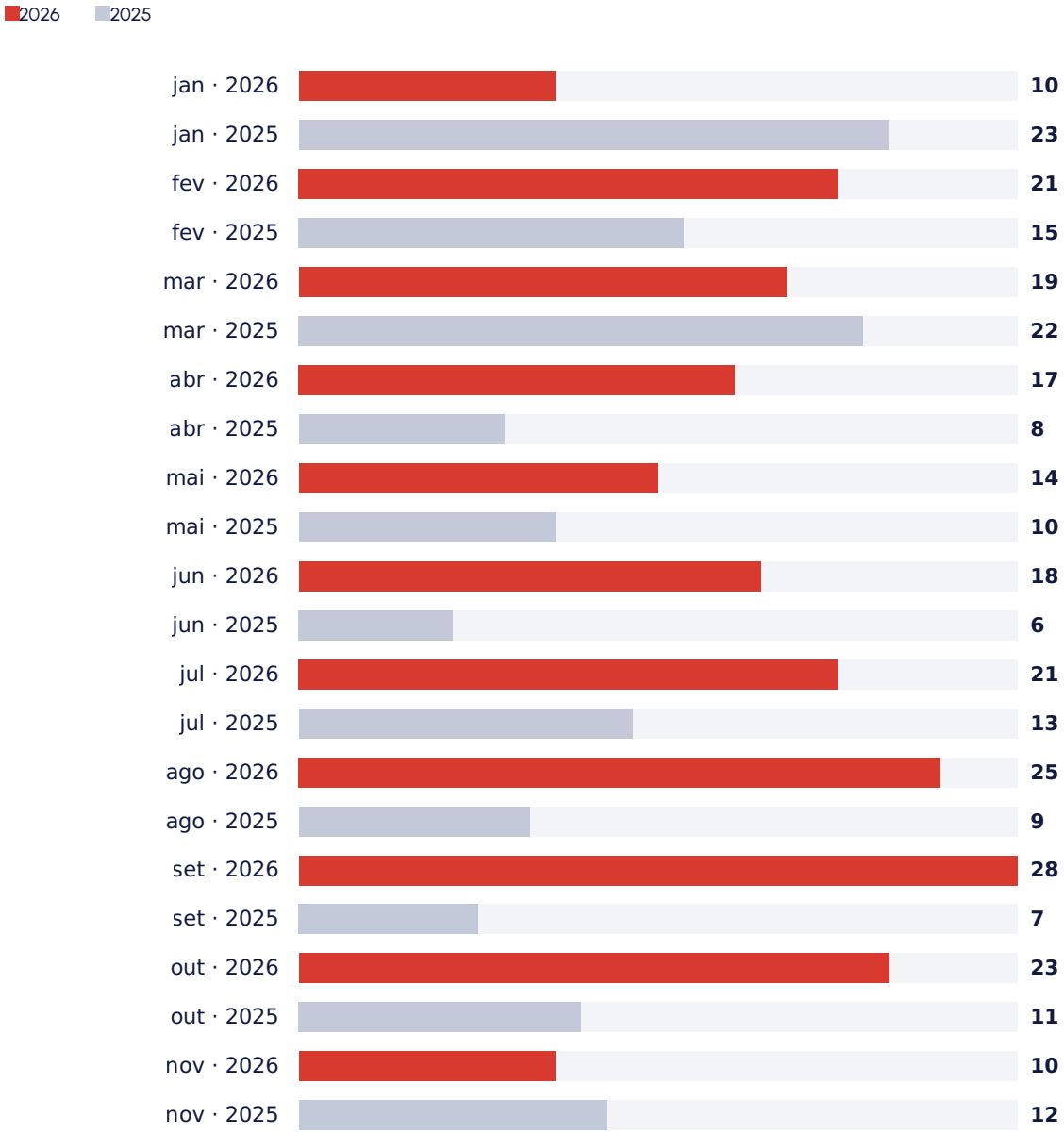
Uma listagem não estabelece independentemente criptografia, quantidade copiada, pagamento ou início da invasão. Pode tratar de fornecedor, subsidiária ou material histórico. A tabela mantém listagens como unidade.

| Rótulo na Ransompedia | Listagens no período | Parcela de 206 | Interpretação |
|---|---|---|---|
| Thegentlemen | 34 | 16,5% | Maior rótulo nesta observação; sem conclusão sobre todas as alegações |
| Lockbit5 | 27 | 13,1% | Preserva o rótulo registrado; sem continuidade automática com outros nomes |
| INC Ransom | 11 | 5,3% | Rótulo de listagem, sem contagem de incidentes confirmados |
| Outros rótulos | 134 | 65,0% | Distribuídos entre os outros 52 rótulos |
| Total | 206 | 100% | Listagens associadas ao Brasil no período definido |

Os três principais rótulos somam 72. A parcela conjunta é 35,0%, calculada sobre 206. Percentuais individuais arredondados podem não reproduzir o percentual conjunto arredondado. Rótulos não estabelecem membros, infraestrutura ou comando comuns.

A série mensal é 10, 21, 19, 17, 14, 18, 21, 25, 28, 23 e 10 listagens, de janeiro a novembro. Novembro termina na data de corte. Setembro tem a maior contagem mensal observada, mas publicação não estabelece pico de invasões. [S2]

### Listagens de ransomware associadas ao Brasil por mês; novembro é parcial




Fonte: listagens da Ransompedia associadas ao Brasil, cada uma uma alegação [S2]. Janeiro-novembro de cada ano; novembro de 2026 cobre 1-22 de novembro, dia de corte parcial; novembro de 2025 é o mês completo. Períodos distintos; não é taxa de crescimento entre períodos equivalentes.

As barras anteriores mostram o mês correspondente completo de 2025. Novembro de 2026 é parcial; suas barras não comparam períodos equivalentes. Publicação de listagem não estabelece a data da invasão. [S2]

A resposta prática vai além dos principais nomes. Um exercício deve testar acesso a identidade, backups, dados empresariais e comunicação externa. A resposta à extorsão também precisa de responsável pelos dados mesmo quando a restauração funciona.

## Thegentlemen

Rótulo de listagens de ransomware/extorsão | Sem atribuição de nacionalidade ou Estado

### NO BRASIL, 2026

2026-01-01–2026-11-22

34 listagens associadas ao Brasil

### ESCOPO RELATADO

Organizações associadas ao Brasil em listagens; resultados não verificados

### EM FONTES PÚBLICAS

[S2] 34 alegações em listagens, sem confirmar invasão ou criptografia.

### NOSSA AVALIAÇÃO

34 alegações em listagens, sem confirmar invasão ou criptografia.

CONFIANÇA

Alta para a contagem; alegações subjacentes não verificadas

## Lockbit5

Rótulo de listagens de ransomware/extorsão | Sem atribuição de nacionalidade ou Estado

### NO BRASIL, 2026

2026-01-01–2026-11-22

27 listagens associadas ao Brasil

### ESCOPO RELATADO

Organizações associadas ao Brasil em listagens; resultados não verificados

### EM FONTES PÚBLICAS

[S2] 27 alegações em listagens, sem confirmar invasão ou criptografia.

### NOSSA AVALIAÇÃO

27 alegações em listagens, sem confirmar invasão ou criptografia.

CONFIANÇA

Alta para a contagem; alegações subjacentes não verificadas

## INC Ransom

Rótulo de listagens de ransomware/extorsão | Sem atribuição de nacionalidade ou Estado

NO BRASIL, 2026

2026-01-01–2026-11-22

11 listagens associadas ao Brasil

ESCOPO RELATADO

Organizações associadas ao Brasil em listagens; resultados não verificados

EM FONTES PÚBLICAS

[S2] 11 alegações em listagens, sem confirmar invasão ou criptografia.

NOSSA AVALIAÇÃO

11 alegações em listagens, sem confirmar invasão ou criptografia.

CONFIANÇA

Alta para a contagem; alegações subjacentes não verificadas

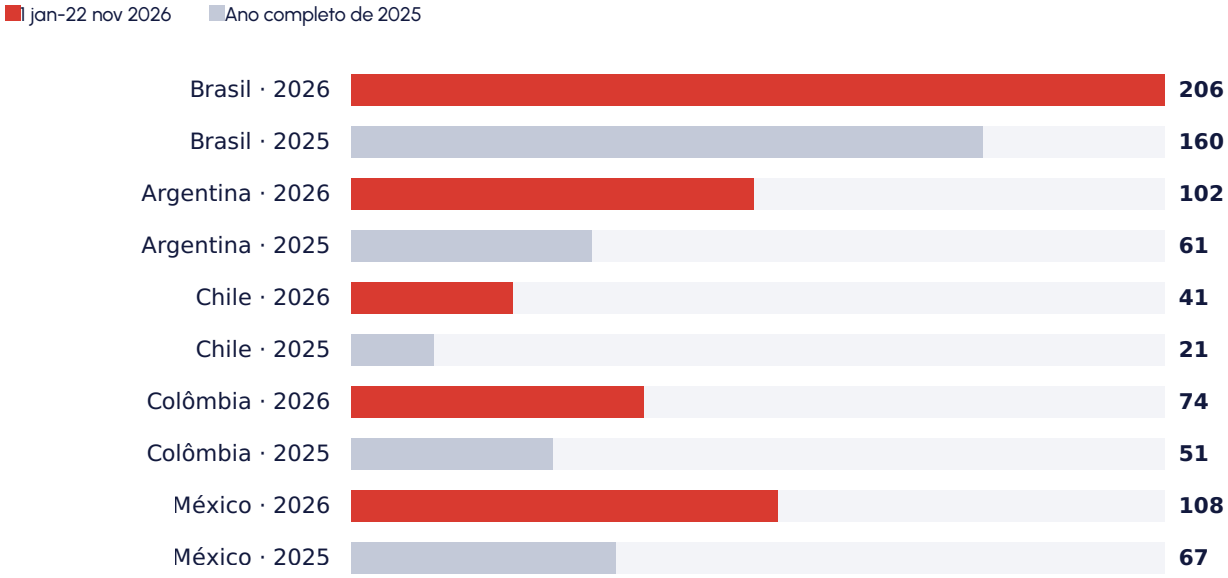
## 7.2 Quatro comparadores regionais

| País | 2026 até o corte | Todo o ano de 2025 | Por que fornece contexto |
|---|---|---|---|
| Brasil | 206 | 160 | País do relatório; escala e condições de divulgação diferem |
| Argentina | 102 | 61 | Grande economia vizinha de serviços e indústria |
| Chile | 41 | 21 | Contexto regional de finanças, mineração e infraestrutura |
| Colômbia | 74 | 51 | Grande mercado regional de serviços e finanças |
| México | 108 | 67 | Grande mercado latino-americano industrial e financeiro |

Os países de comparação foram selecionados como exemplos apenas para fornecer contexto; a sua escolha não implica uma classificação nem uma avaliação política.

Fonte: mesma observação da Ransompedia e mesmas datas de análise. [S2]

### Listagens datadas de ransomware no Brasil e em quatro pares regionais




Fonte: listagens da Ransompedia associadas a países; cada uma registra uma alegação de extorsão [S2]. 2026: 1 de janeiro-22 de novembro, dia de corte parcial; 2025: ano completo. Períodos distintos; não é classificação de segurança nacional.

O Brasil tem o maior número de listagens entre esses pares selecionados nesta observação. A afirmação diz respeito à população registrada. Não classifica segurança nacional, competência institucional ou risco por organização.

A tabela não tem denominador comum de tamanho econômico, organizações conectadas, propensão à divulgação ou cobertura de atacantes. Não transforme contagens absolutas em probabilidade de incidente para uma organização brasileira. Empresas com fornecedores nesses mercados devem usá-las para decidir onde testar continuidade.

## 7.3 Identidades de pagamento: BREEZE COMET

A pesquisa de setembro do Google descreve BREEZE COMET como financeiramente motivado e informa investigações iniciadas em 2024. Os casos brasileiros incluem instituições financeiras, varejo, comércio eletrônico e serviços de pagamento. O relato abrange atividade até 2026. [S18]

**Uma identidade transacional pode importar mais que um login.** O Google descreve roubo e abuso de material válido de TLS mútuo e segredos de pagamento. Também descreve engenharia social, ferramentas de administração remota e fornecedores. É o relato do pesquisador sobre casos investigados, sem generalização para todos os provedores.

A decisão de defesa é inventariar quem pode obter, copiar, substituir e revogar certificados transacionais e material de assinatura. Separe acesso ao aplicativo e autorização para movimentar recursos. Verifique evidências de mudanças de beneficiário e substituições emergenciais de credenciais.

Um relato sobre fornecedor não estabelece todos os clientes como vítimas. Uma oferta que menciona certificados também não comprova relação com essa campanha. A oferta privada e a pesquisa pública permanecem fluxos separados de evidência.

### BREEZE COMET

Anteriormente rastreado pelo Google como UNC5669

Atividade financeira | Motivação financeira segundo o Google

NO BRASIL, 2026

2026-09-01

A pesquisa abrange investigações desde 2024 e atividade até 2026

ESCOPO RELATADO

Serviços financeiros e de pagamento

EM FONTES PÚBLICAS

[S18] Reveja identidades transacionais e autorização de fornecedores; sem ligação estabelecida com os vendedores selecionados.

NOSSA AVALIAÇÃO

Reveja identidades transacionais e autorização de fornecedores; sem ligação estabelecida com os vendedores selecionados.

CONFIANÇA

Pesquisa atribuída; sem prevalência nacional

## 7.4 Malware bancário: TCLBANKER

A pesquisa de maio da Elastic descreve TCLBANKER, na atividade REF3076, como malware bancário com recursos de comunicação e credenciais. Descreve instalação maliciosa, carregamento de DLL e propagação em contextos autenticados de mensagens e e-mail. [S19]

A lista de domínios bancários monitorados no artigo descreve o que o malware reconhece. Não estabelece invasão de cada banco listado. Infecção do dispositivo de um cliente e incidente na infraestrutura bancária exigem responsáveis diferentes.

Uma mensagem de conta conhecida pode ser hostil. Bancos, comerciantes e empregadores devem testar o relato de anexos inesperados de contatos confiáveis. O isolamento do dispositivo precisa ser coordenado com invalidação de sessões e revisão da atividade posterior.

A Elastic discute semelhanças com malware anterior. Essas relações permanecem avaliação técnica do pesquisador. O relatório não infere operador único por trás de ferramentas semelhantes nem as liga a vendedores anônimos.

## TCLBANKER / REF3076

Campanha de malware bancário | Atividade financeira descrita pela Elastic

NO BRASIL, 2026

2026-05-07

Publicação de pesquisa da campanha

ESCOPO RELATADO

Usuários bancários e comunicações autenticadas

EM FONTES PÚBLICAS

[S19] Valide instalação e sessões pertinentes; domínios monitorados não são bancos vítimas.

NOSSA AVALIAÇÃO

Valide instalação e sessões pertinentes; domínios monitorados não são bancos vítimas.

CONFIANÇA

Pesquisa atribuída; sem inferência de impacto na infraestrutura bancária

## 7.5 Identidade no navegador: UnregStealer

A publicação de junho da IBM descreve UnregStealer como campanha operada por pessoas para roubo de credenciais de navegador de usuários bancários brasileiros. Descreve extensão maliciosa, material de sessão e interação do operador, após descoberta em maio. [S20]

A resposta não termina na troca de senha. Uma extensão maliciosa pode manter acesso à navegação, e uma sessão válida pode sobreviver à mudança. Reveja política do navegador, origem da extensão, revogação de sessões e transações em conjunto.

É uma descrição de campanha, sem evidência de entrada nos sistemas dos bancos citados. Também não fornece total nacional de clientes afetados. A detecção deve ser validada pelo dispositivo e pelos registros da conta daquele cliente.

### UnregStealer

Roubo de credenciais de navegador | Direcionamento financeiro descrito pela IBM

NO BRASIL, 2026

2026-06-16

Publicação após descoberta em maio

ESCOPO RELATADO

Usuários bancários brasileiros

EM FONTES PÚBLICAS

[S20] Reveja extensões e invalide sessões afetadas junto da contenção da conta.

NOSSA AVALIAÇÃO

Reveja extensões e invalide sessões afetadas junto da contenção da conta.

CONFIANÇA

Pesquisa atribuída; sem total nacional de usuários

## 7.6 Espionagem e roubo de informações: Armored Likho

A pesquisa da Kaspersky de 3 de julho identifica vítimas no Brasil, na Rússia e no Cazaquistão, principalmente em governo e infraestrutura elétrica. Atribui BusySnake Stealer ao Armored Likho com confiança moderada, com base em ferramentas e atividade de rede. [S161]

**A atribuição pertence ao pesquisador, com a confiança declarada.** O artigo descreve arquivos de phishing, roubo modular de credenciais e sessões e acesso remoto. Caracteriza mistura de atividade financeira contra indivíduos e espionagem contra organizações.

Não identifica organização brasileira, número de vítimas no país, patrocinador estatal ou nacionalidade. Não estabelece interrupção elétrica. A associação circunstancial com outro ator não basta para criar relação operacional confirmada neste relatório.

Defensores de governo e energia devem revisar sessões privilegiadas, acesso remoto e separação entre administração e ambientes operacionais. A presença do país entre vítimas justifica avaliar o comportamento descrito, sem evidenciar dano a uma instalação específica.

### Armored Likho

campanha BusySnake Stealer

Roubo de informações e espionagem | Atividade financeira e espionagem segundo a Kaspersky; sem atribuição estatal

NO BRASIL, 2026

2026-07-03

Pesquisa original inclui Brasil entre os países das vítimas

ESCOPO RELATADO

Governo e infraestrutura elétrica; sem sujeito brasileiro nomeado

EM FONTES PÚBLICAS

[S161] Reveja sessões privilegiadas e acesso remoto; sem interrupção elétrica estabelecida.

NOSSA AVALIAÇÃO

Reveja sessões privilegiadas e acesso remoto; sem interrupção elétrica estabelecida.

CONFIANÇA

Atribuição de confiança moderada da Kaspersky

## 7.7 Outras pesquisas financeiras relevantes para o Brasil

A pesquisa de março da Kaspersky sobre GoPix descreve fraude relacionada à área de transferência contra usuários brasileiros. O controle relevante é verificar beneficiário e dados finais por exibição ou processo confiável. Reconhecer a marca não valida o destino. [S105]

O artigo de abril sobre JanelaRAT descreve ameaça financeira na América Latina. O número brasileiro de detecções discutido pertence a 2025 e não aparece como contagem de 2026. A pesquisa continua útil para revisar dispositivos e contas. [S106]

Motivação financeira inferida de roubo observado não deve virar atribuição de nacionalidade. As campanhas estão incluídas porque a pesquisa original sustenta relevância brasileira e ações úteis. Idioma ou mercado semelhantes não estabelecem cooperação.

A pesquisa de março sobre BeatBanker descreve malware Android em usuários brasileiros, com funções bancárias e mineração e variantes posteriores com acesso remoto BTMOB. A entrega imita aplicativos conhecidos. Isso sustenta verificar origem e permissões, sem estabelecer invasão de infraestrutura bancária. [S23]

A pesquisa de junho descreve anexos maliciosos no WhatsApp que instalam administração remota legítima em vários países, incluindo o Brasil. A observação original é de junho, apesar da circulação posterior em fóruns. A atribuição tem baixa confiança, sem grupo conhecido estabelecido. Reveja instalações e permissões de suporte não solicitadas. [S24]

A pesquisa de setembro da Check Point sobre Gambling Goblin descreve servidores brasileiros de governo e educação usados em fraude de buscas, acompanhada desde meados de 2025. Descreve módulos Apache maliciosos. A ligação com Earth Berberoka é avaliação da fonte, com confiança moderada a alta; não se infere patrocínio estatal. Reveja módulos e publicação delegada. [S25]

## Gambling Goblin

Abuso de servidores e fraude em buscas | Atividade criminosa segundo a Check Point; sem atribuição estatal

NO BRASIL, 2026

2026-09-02
Campanha acompanhada desde meados de 2025

ESCOPO RELATADO

Servidores web de governo e educação

EM FONTES PÚBLICAS

[S25] Reveja módulos e autorização de publicação; a ligação com Earth Berberoka é avaliação do pesquisador.

NOSSA AVALIAÇÃO

Reveja módulos e autorização de publicação; a ligação com Earth Berberoka é avaliação do pesquisador.

CONFIANÇA
Ligação de confiança moderada a alta segundo a Check Point

### KREMLIN: sessões bancárias e nomes que podem induzir erro

A pesquisa de 14 de setembro da Elastic descreve REF9334 e seu conjunto KREMLIN, acompanhado desde maio de 2025. A operação usa documentos como iscas e extensões maliciosas para roubar credenciais e sessões. O nome não sustenta atribuição ao Estado russo. [S304]

O responsável pertinente é a equipe de endpoints e identidades de navegador. Valide extensões inesperadas, preserve evidências de instalação e invalide sessões afetadas. Uma isca bancária não estabelece acesso à infraestrutura do banco. Não há operador comum estabelecido com UnregStealer ou TCLBANKER.

### PhantomEnigma: infraestrutura confiável pode entregar documento inseguro

A investigação de 16 de julho da ANY.RUN descreve infraestrutura governamental brasileira usada na entrega e iscas com tema policial. Distingue servidores abusados na distribuição e alvos confirmados. A ligação do componente específico de backdoor a PhantomEnigma recebe confiança moderada a alta. [S305]

Isso sustenta revisar autorização de publicação, anexos suspeitos e execução posterior mesmo quando a mensagem passa pela autenticação do remetente. Não transforma cada órgão citado em sujeito nomeado. O relatório não adota total nacional de vítimas nem operador comum com outras campanhas.

### Pacotes de integração bancária e autorização por certificados

A pesquisa de 28 de maio da Socket identifica pacote malicioso que se passa por biblioteca de integração bancária. Descreve roubo de identificadores de cliente, arquivos de certificados PFX e suas senhas. O material pode permitir personificação da integração, dependendo das permissões e dos controles financeiros. [S313]

Valide o publicador e o pacote entregue; estabeleça se material real de autenticação foi usado. Revogue e substitua certificados e credenciais expostos. A pesquisa não estabelece invasão da instituição imitada nem ligação com o anúncio de certificados do Caso I.

## 7.8 Alertas oficiais e o responsável pelo controle

| Alerta oficial | O que a fonte sustenta | Decisão do responsável |
|---|---|---|
| Páginas falsas de serviços públicos | CTIR descreve phishing com temas de serviços [S147] | Verificar mensagens pelo canal autorizado |
| Abuso de subdomínios legítimos | CTIR descreve material malicioso em endereços governamentais [S148] | Rever publicação delegada e subdomínios sem uso |
| Instruções ClickFix | CTIR descreve verificações e erros falsos [S149] | Ensinar a interromper pedidos inesperados de comandos locais |
| Roubo de códigos de dispositivo e tokens | CTIR descreve abuso de autenticação em nuvem e sessões [S150] | Rever contexto, duração e revogação |
| Possível atividade interativa de operador | CTIR descreve explicitamente uma possível campanha [S151] | Investigar sem declarar criptografia |
| Desfiguração por uploads | CTIR descreve conteúdo executável em áreas de envio [S152] | Aplicar política de uploads e separar conteúdo de serviços executáveis |
| Campanha de credenciais de gateway | CTIR alerta sobre material de autenticação exposto [S153] | Avaliar acesso e substituir credenciais pertinentes |
| Manipulação de buscas | CTIR descreve abuso da visibilidade de sites públicos [S120] | Verificar resultados, responsáveis e alterações publicadas |

Os alertas descrevem mecanismos ou investigações. Publicação não estabelece a data de cada evento, e números de recomendações não são totais de vítimas. Não se infere motivo político pelo contexto de serviço público.

### Informações de fornecedores, autorização em nuvem e integridade web

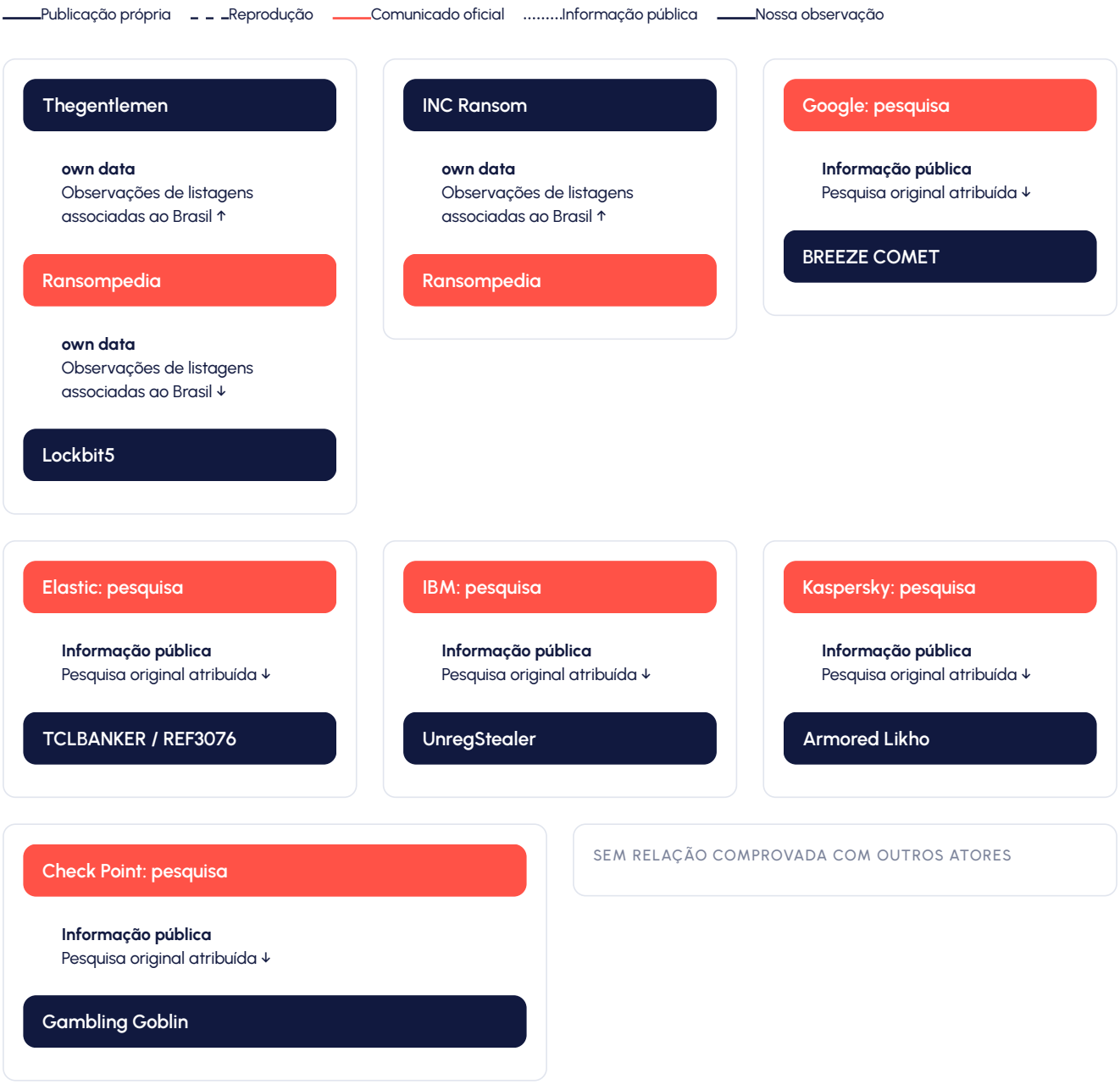
O alerta do CTIR de 21 de maio descreve exposição de dados de fornecedor, documentos internos e código-fonte. A recomendação de 22 de maio acrescenta verificação de integridade das atualizações e restrições administrativas. São conclusões e recomendações da autoridade, sem confirmar invasão em cada cliente. [S316] [S317]

O fornecedor mantém descrição ampla. Não se infere total de órgãos afetados, nova atribuição ou ligação direta com anúncio de acesso. Valide produto pertinente, segredos expostos e administração permitida antes de aplicar a resposta ao ambiente cliente.

A orientação de 24 de junho do CTIR descreve riscos de identidades privilegiadas e abuso de recursos, incluindo mineração não autorizada. O responsável pela nuvem deve rever permissões de aplicativos e criação inesperada de recursos junto da recuperação da conta. Não há total nacional de vítimas ou perdas. [S318]

O alerta de 14 de agosto descreve alterações não autorizadas em páginas e recomenda investigar evidências no contexto do serviço. Arquivo suspeito isolado é insuficiente para estabelecer exploração. Este relatório não adota limite técnico de versões nem conta cada site público como incidente. [S319]

## 7.9 Mapa de relações e visão de técnicas



O mapa separa observações próprias de listagens da Ransompedia e pesquisas públicas atribuídas. Uma fonte ligada a uma campanha significa que a descreveu. Não indica participação do pesquisador na atividade.

Não há ligação inferida de coordenação entre vendedores de acesso, malware bancário e rótulos de ransomware. Interesse comum no Brasil ou em credenciais é insuficiente. Uma relação futura exigiria evidência técnica ou operacional concreta e confiança explícita.

TÉCNICAS DESCRITAS NAS PESQUISAS CITADAS, POR TÁTICA

| Acesso inicial | Execução | Descoberta | Coleta |
|---|---|---|---|
| T1566.001<br>Anexo de phishing direcionado | T1059.001<br>PowerShell | T1082<br>Descoberta de informações do sistema | T1113<br>Captura de tela |

Comportamentos citados na pesquisa TCLBANKER da Elastic [S19]; rótulos verificados na MITRE [S26][S27][S28][S29]. Sem medir prevalência. [S19]

| Tática | Técnica | Pergunta de controle | Fonte da definição |
|---|---|---|---|
| Acesso inicial | T1566.001, anexo de phishing direcionado | A equipe relata anexo inesperado de conta conhecida? | MITRE [S26] |
| Execução | T1059.001, PowerShell | O responsável distingue scripts aprovados de atividade suspeita? | MITRE [S27] |
| Descoberta | T1082, informações do sistema | O contexto explica inspeção incomum do sistema? | MITRE [S28] |
| Coleta | T1113, captura de tela | A equipe investiga capturas inesperadas? | MITRE [S29] |

São comportamentos descritos na fonte, com definições verificadas na MITRE. As perguntas de controle são recomendações analíticas. [S19]

A visão de técnicas segue comportamentos descritos pela Elastic para TCLBANKER. É apoio à revisão de uma campanha, sem gráfico de prevalência ou afirmação de que cada comportamento ocorreu em todos os casos brasileiros. [S19]

Pergunte se o controle gera evidência útil ao respondente. A equipe consegue identificar instalação inesperada, validar o componente carregado e revogar a sessão de comunicação associada? Nomear uma técnica sem responsável pela evidência não encerra o risco.

PRINCIPAIS CONCLUSÕES

**01**

Trate as 206 listagens como alegações, com o período observado.

**02**

Separe autorização de pagamento, malware em clientes e evidências de espionagem.

**03**

Use rótulos para localizar pesquisas e atribua controles aos comportamentos sustentados.

CAPÍTULO 08

# Fraude, dados pessoais e material de cartões de pagamento

ESTE CAPÍTULO RESPONDE

O que uma observação pode estabelecer sobre fraude?

**3**

perguntas distintas: dados publicados, acesso a contas e prejuízo financeiro real


8.1 Dados sustentam uma história; não autenticam quem liga 79
8.2 Escopo das observações de cartões 79
8.3 Uma campanha de terminais com denominador global 80
8.4 Investigações mostram vários caminhos de fraude 80
8.5 Investigações recentes sobre fraude em contas 81
8.6 Controle a próxima solicitação plausível 82
8.7 Acesso com finalidade legítima e instruções em documentos 82

CAPÍTULO 08

# Fraude, dados pessoais e material de cartões de pagamento

EM RESUMO

Identificadores publicados, ofertas de acesso e material de cartões geram perguntas diferentes. Um registro observado não estabelece conta utilizável atualmente ou transação concluída. Comunicados policiais mostram investigações sobre falsificação de identidade, abuso de contas e acesso legítimo; pesquisas técnicas descrevem roubo em dispositivos de clientes. Preserve cada população e situação separadamente. Valide contas relevantes nos registros internos autorizados e ofereça um canal confiável para verificar solicitações inesperadas.

## 8.1 Dados sustentam uma história; não autenticam quem liga

Os anúncios selecionados combinam identificadores e contexto prático: responsável e mensalidade, cliente e entrega, contribuinte e nota ou relação bancária. As combinações permanecem alegações até a validação. Sua relevância defensiva está na plausibilidade de uma mensagem de falsificação de identidade. [S1]

Quem sabe um CPF ou transação recente não está necessariamente autorizado. O atendimento deve autenticar pelo processo estabelecido, sem usar fatos familiares como prova de identidade. Não peça a clientes transferência para suposta conta segura ou divulgação de código de autenticação.

As notas da CVP e do Tesouro tornam a distinção concreta. Identificam dados cadastrais e exclusões ou limites datados. Não estabelecem que um vendedor detenha aqueles registros nem que cada pessoa afetada tenha sofrido fraude. [S126][S127]

**Exposição e prejuízo exigem evidências separadas.** Registre origem do contato, categorias afetadas e atividade resultante na conta. Diferencie suspeita, tentativa e transferência não autorizada confirmada no cadastro do cliente e no relato executivo.

## 8.2 Escopo das observações de cartões

ESCOPO DOS NÚMEROS DOS CARTÕES

Estes números descrevem um conjunto limitado de observações de cartões de pagamento da Brandefense. Não estabelecem validade atual, titulares únicos, roubo nacional de cartões ou perdas por fraude.

O agregado descreve observações de cartões de pagamento, com suas unidades. Repetir a observação de um cartão não gera outro titular. O status anunciado não é registro de autorização do emissor, e preço anunciado não evidencia venda concluída. [S4]

O conjunto contém 1.229 observações distintas de cartões associados ao Brasil, com 1.411 ocorrências. Observações distintas de cartões e ocorrências são unidades diferentes. Os valores não estabelecem validade atual ou perdas dos emissores. [S4]

O total não pode ser associado a bases de clientes para inferir taxa de fraude. Não há denominador de cartões ativos emitidos no Brasil. Comparar emissores também exigiria validar identidade, tempo e escopo; esta edição não publica classificação nominal de emissores.

Nenhuma observação de cartão estabelece como a informação saiu originalmente de um sistema. Infecção de endpoint, interceptação de pagamento, arquivo antigo, revenda e anúncio repetido podem produzir material semelhante. Atribuir um incidente exige evidências adicionais.

## 8.3 Uma campanha de terminais com denominador global

A investigação original da Cybernews descreve descoberta de campanha de roubo de informações em terminais em agosto de 2026. Relata 782 sistemas afetados globalmente e pelo menos um milhão de registros únicos de cartões, com a maioria dos sistemas descrita como brasileira. [S232]

São quantidades globais dos pesquisadores. O total exato apenas do Brasil não é consistente entre os relatos e foi omitido. Nenhum banco ou varejista nomeado atende aos requisitos de confirmação independente para essa campanha.

A pesquisa descreve uso da CVE-2024-49138, vulnerabilidade de elevação de privilégios do Windows. A NVD registra limites de versões afetadas e liga a correção do fornecedor. Trata-se de vulnerabilidade previamente corrigida em relato de campanha de 2026, sem nova divulgação da falha. [S5]

A resposta começa pelo parque real: versão do sistema, atualização, componentes, suporte remoto e tratamento de dados de pagamento. Valide sinais relevantes em sistemas autorizados. A descrição ampla não estabelece que uma loja específica foi afetada.

Os pesquisadores observaram o servidor exposto fechado em 31 de agosto e comunicaram os resultados ao CTIR em 8 de setembro. Isso não estabelece que a campanha terminou ou que os terminais afetados foram remediados. A publicação em novembro não transforma a atividade de agosto em nova onda de infecções de novembro. [S232]

## 8.4 Investigações mostram vários caminhos de fraude

| Relato oficial | Alegação ou conclusão sustentada | Limite neste relatório | Responsável pela resposta |
|---|---|---|---|
| Operação de falso advogado em fevereiro | Polícia descreve falsificação e indução a acesso remoto [S103] | Mandados e suspeitas não são condenações | Proteção dos clientes e suporte de endpoints |

| Relato oficial | Alegação ou conclusão sustentada | Limite neste relatório | Responsável pela resposta |
|---|---|---|---|
| Pix Seguro em maio | Autoridades descrevem mensagens e páginas falsas e suposta fraude [S107] | Bens bloqueados não são total estabelecido de perdas | Fraude e comunicação verificada |
| Falso gerente em maio | Polícia estadual descreve o esquema [S108] | Prisões não estabelecem culpa | Atendimento e resposta a fraude |
| Investigação de acesso interno em maio | Polícia descreve suposto abuso e bloqueio de bens [S110] | Bens bloqueados não equivalem a valores roubados | Responsável pelo acesso, RH e investigação |
| Investigação de arquivos bancários em julho | PF descreve suposta captura de informações internas [S115] | Sem conclusão geral sobre plataforma ou clientes | Dados e resposta a acesso privilegiado |
| Fraude em contas sociais em julho | PF descreve suposto uso indevido de credenciais [S116] | Sem atribuição a todas as contas de pessoal | Contas e proteção dos clientes |
| Investigação de infostealer em agosto | PF descreve suspeita de hospedagem e distribuição de software de roubo [S154] | Uma investigação não mede prevalência nacional | Endpoints e identidade |
| Instalação telefônica em novembro | Polícia estadual informa equipamentos sob investigação [S133] | Dispositivos e chips não contam vítimas | Abuso de mensagens e proteção dos clientes |

Vários casos envolvem falsificação de identidade ou acesso legítimo, sem falha de aplicativo visível remotamente. A pergunta comum é quem pode agir e como verificar essa autorização de forma independente. A tabela não estabelece uma rede criminosa única.

## 8.5 Investigações recentes sobre fraude em contas

A investigação da PF de 9 de novembro trata de conta que supostamente recebeu recursos de fraude eletrônica. A operação de 11 de novembro envolve suspeita de fraude bancária, contas beneficiárias e lavagem. Nenhuma fornece total nacional de vítimas ou perdas. [S155][S156]

A investigação de benefícios de 17 de novembro também descreve suposto acesso a contas e transferências. Quando pertinente, as alegações justificam revisão delimitada da conta. Não podem ser somadas a listagens de ransomware ou invasões de organizações. [S130]

O anúncio Radar reúne ações internacionais de maio a setembro. O resultado específico do Brasil é a desativação de oito domínios fraudulentos. Os totais internacionais de casos e prisões não são totais brasileiros. [S129]

Desativar um domínio ou bloquear uma conta é resultado de intervenção. Não demonstra identificação de todas as vítimas, recuperação de todos os pagamentos ou fim do ecossistema. A proteção precisa manter canal para relatos e correções.

## 8.6 Controle a próxima solicitação plausível

Em serviços ao consumidor, prepare uma mensagem curta de verificação antes do incidente. Informe onde verificar o contato e quais ações nunca serão solicitadas em conversa não iniciada pelo cliente. Confirme que todos os canais dão a mesma orientação.

Em pagamentos internos, separe a mensagem da autorização. Uma caixa postal ou conta genuína de fornecedor pode enviar alteração indevida de beneficiário. Confirme a mudança por canal confiável estabelecido antes da solicitação.

Na recuperação de identidade, considere o que o impostor já pode saber. CPF, nascimento ou contrato correto não devem substituir a autenticação prevista. Ofereça uma alternativa que não dependa dos mesmos dados expostos.

Ao relatar incidentes, preserve a incerteza. Informe se há oferta publicada, exposição validada, login suspeito ou transferência não autorizada. A distinção ajuda jurídico, fraude e serviços a escolherem a resposta.

## 8.7 Acesso com finalidade legítima e instruções em documentos

Nota do STF de 17 de fevereiro descreve investigação de acessos a dados fiscais. Atribui a conclusão inicial a relatório da Receita Federal que identificou acessos sem justificativa funcional estabelecida, seguidos de divulgação de informações sigilosas. A investigação policial continuava. [S306]

É relato investigativo atribuído, sem julgamento de pessoas, decisão judicial ou motivação política. Não estabelece invasão da infraestrutura do tribunal. A pergunta de controle é se o acesso a dados sensíveis tem finalidade válida e registro verificável de forma independente.

Nota de outro tribunal, de 20 de maio, identifica instruções ocultas em documentos apresentados para influenciar processamento por IA. O tribunal afirma que suas proteções neutralizaram as tentativas e anunciou medidas investigativas. A nota não estabelece influência bem-sucedida sobre decisão. [S307]

O conteúdo documental deve permanecer evidência para análise. Responsáveis por aplicativos devem definir instruções confiáveis, limitar permissões de ferramentas e testar se pedidos incorporados alteram a tarefa permitida. A equipe jurídica deve validar o resultado. São recomendações analíticas, sem posição sobre processos.

Notícias sobre plataforma de segurança pública também descrevem investigação de suposta divulgação por usuário legítimo. Relatos policiais e municipais permanecem atribuídos. Notícia separada sobre câmeras de fornecedor não é unida ao caso. Não há julgamento da política de vigilância nem de culpa individual. [S323]

O relato oficial indexado de operação de 7 de maio descreve investigação de suspeita de extração, retenção e venda de dados públicos. Cobertura independente confirma a operação. O documento completo não pôde ser revisado. Não se estabelece população final, data de invasão ou condenação. [S186]

PRINCIPAIS CONCLUSÕES

**01**

Dados pessoais conhecidos não autenticam um pedido de pagamento.

**02**

Observações de cartões e totais de pesquisadores têm populações restritas e diferentes.

**03**

Valide atividade de contas e prejuízo com o responsável pelo serviço.

CAPÍTULO 09

# Bancos e pagamentos: proteger a autorização para agir

ESTE CAPÍTULO RESPONDE

Qual acesso pode alterar um pagamento?

**4**

camadas separadas: cliente, instituição, fornecedor e infraestrutura de pagamentos


9.1 Separe as camadas do pagamento 85
9.2 O que as ofertas selecionadas realmente dizem 86
9.3 Identidades transacionais precisam de inventário próprio 86
9.4 Concilie declarações iniciais e conclusões posteriores 87
9.5 Cadastros e a distinção das chaves Pix 87
9.6 A lição das guias municipais 87
9.7 Perguntas ao fornecedor pelo responsável de pagamentos 88
9.8 Endpoints, fraude e infraestrutura precisam de registro comum 88
9.9 A população distinta de incidentes da supervisão 89
9.10 Uma visão anônima da exposição bancária 89

CAPÍTULO 09

# Bancos e pagamentos: proteger a autorização para agir

EM RESUMO

As evidências abrangem suspensão temporária do Pix em banco, alteração de guias municipais, divulgação de cadastros, malware em dispositivos e anúncios de acesso a fornecedores. Esses eventos não estabelecem fraqueza comum ou invasão nacional do sistema de pagamentos. A pergunta central é qual autorização uma identidade possui. Mapeie cliente, instituição, fornecedor e infraestrutura de pagamentos separadamente; teste revogação de certificados, validação de beneficiário e continuidade com quem pode interromper uma transação insegura.

## 9.1 Separe as camadas do pagamento

Um cliente pode perder uma sessão enquanto a infraestrutura bancária permanece íntegra. Uma instituição pode sofrer incidente financeiro sem perda confirmada nos saldos dos clientes. Um fornecedor pode expor acesso pertinente a vários clientes sem evidência de que todos foram afetados.

A quarta camada é a própria infraestrutura de pagamentos. Exposição de identificadores Pix, anúncio com a palavra Pix ou interrupção em participante não estabelece invasão nacional. Cada afirmação precisa de evidência para o limite real do sistema.

| Camada | Evidência relevante nesta edição | O que estabelecer internamente |
|---|---|---|
| Dispositivo e sessão do cliente | Pesquisas de malware bancário e extensão [S19][S20] | Estado do dispositivo, sessões válidas e atividade posterior |
| Instituição | Incidente datado do Banco do Nordeste e relatório posterior [S101][S231] | Recursos próprios, saldos de clientes, dados e disponibilidade separadamente |
| Fornecedor ou operador delegado | Certificados e infraestrutura anunciados; pesquisa do Google [S1][S18] | Permissões, limites de clientes e autoridade de revogação |
| Infraestrutura de pagamentos | É necessária evidência específica da infraestrutura | Limite real do sistema, acesso e impacto operacional |

Instruções de pagamento e informações cadastrais são categorias de evidência que podem atravessar essas quatro camadas. Separe suas perguntas de validação da camada afetada.

| Categoria de evidência | Evidência relevante nesta edição | O que estabelecer internamente |
|---|---|---|
| Instruções de pagamento | Guias alteradas de Belo Horizonte [S233] | Beneficiário pretendido, alteração autorizada e conciliação |
| Informações cadastrais | Populações distintas divulgadas pelo Tesouro [S127] | Categorias e intervalo reais; sem presumir autorização de pagamento |

As camadas podem interagir, mas a interação é possibilidade analítica até ser verificada. Um exercício deve colocar o problema no fornecedor e perguntar se a instituição consegue contê-lo rapidamente. Deve testar também a evidência exigida do fornecedor.

## 9.2 O que as ofertas selecionadas realmente dizem

O caso I anuncia certificados ligados a intermediário de pagamentos e menciona rede interna separadamente. O caso J anuncia acesso associado a fornecedor de infraestrutura financeira e serviços bancários. São ofertas observadas, sem capacidade verificada de transferência. [S1]

Uma oferta separada de abril alega acesso a comunicações e documentos enviados que envolvem certificados de pagamento. Também alega persistência e venda anterior. O relatório não autentica as afirmações, conecta as ofertas ou infere transação financeira concluída.

**Mencionar certificado não demonstra autorização de pagamento.** Sua função pode variar por ambiente, permissão e validade. É preciso estabelecer o que autentica, se continua válido, quem pode revogá-lo e quais ações permite.

Não valide a alegação contatando o vendedor ou usando o acesso anunciado. O caminho operacional é a evidência autorizada da instituição e do fornecedor. Ela deve estabelecer se alguma identidade, permissão ou segredo relevante exige contenção.

## 9.3 Identidades transacionais precisam de inventário próprio

A pesquisa BREEZE COMET do Google descreve material válido de TLS mútuo e segredos de pagamento em atividades investigadas. Justifica examinar identidades transacionais separadamente das senhas comuns de usuários. [S18]

O inventário deve identificar função empresarial, sistema, titular autorizado e revogação emergencial. Deve distinguir produção e teste. Sem isso, uma substituição urgente pode ignorar a autorização real ou interromper um serviço intacto.

Reveja aprovação para emitir, exportar e substituir certificados. Confirme que a emergência não elimina silenciosamente a separação de funções. Registre como a contraparte sabe que a identidade antiga perdeu validade.

Um segredo pode não estar na estação e permanecer em implantação, registro de suporte ou repositório antigo. Peça ao responsável que demonstre a revisão de acesso e o resultado da substituição. Uma política isolada não evidencia encerramento de acesso.

Esse é um modelo de controle recomendado, sem concluir que cada local citado continha segredos brasileiros de pagamento. A pesquisa justifica a pergunta; as evidências da organização determinam a exposição.

## 9.4 Concilie declarações iniciais e conclusões posteriores

A nota inicial do Banco do Nordeste trata de suspensão temporária do Pix e informa ausência de prejuízo identificado em contas de clientes ou vazamento naquele momento. O relatório posterior descreve perda institucional e recuperação. As declarações podem tratar de resultados e datas distintos. [S101][S231]

O registro deve preservar a declaração original, o horário e a atualização posterior. Não substitua uma garantia inicial por outra mais ampla. Também não reescreva a declaração como se a instituição já conhecesse todas as conclusões posteriores.

A mesma distinção se aplica à exclusão preliminar da CVP sobre dados financeiros e de autenticação. É uma conclusão datada e limitada à investigação da empresa. Não autentica anúncios nem garante a situação de marcas relacionadas. [S126]

No relato executivo, separe dados, recursos de clientes, recursos próprios, disponibilidade e recuperação. Cada linha precisa de fonte e data. Um status geral positivo pode esconder resultado ainda não resolvido em outra dimensão.

## 9.5 Cadastros e a distinção das chaves Pix

O Tesouro distingue aproximadamente 30.000 cadastros de serviços de outra base analítica com cerca de 4.000 chaves Pix. As populações não podem ser somadas como pessoas únicas. A presença da chave não estabelece autorização de transferência. [S127]

O registro do Banco Central também distingue exposição pessoal e acesso a dinheiro ou autenticação em comunicados individuais. Vários itens têm intervalos claros, mas datas originais de divulgação não resolvidas. Não viram uma série completa de incidentes de 2026. [S134][S135][S136][S137][S138][S139]

A mensagem segura identifica campos reais e o canal de proteção. Evite dizer que todos os titulares tiveram saldo acessado sem apoio no comunicado. Evite também considerar os identificadores inofensivos apenas porque não iniciam uma transferência sozinhos.

Um fraudador pode combinar identificador genuíno e pedido falso. A resposta é verificação independente e evidência da conta, sem afirmar que o identificador funciona como senha de pagamento.

## 9.6 A lição das guias municipais

Belo Horizonte informa que guias alteradas enviaram recursos a destino diferente do município. A autoridade bloqueou valores afetados e iniciou devoluções. O problema confirmado é a integridade da instrução apresentada ao contribuinte. [S233]

Quem recebe pagamentos digitais deve testar o caminho entre emissão autorizada e beneficiário exibido. Verifique se a mudança é perceptível ao pagador e se a equipe concilia o recebedor esperado com a liquidação real.

Reemissão manual pode ampliar a confusão. Forneça uma orientação oficial sobre novos pagamentos e devoluções. Preserve quais guias foram afetadas, sem tratar todo pagamento municipal pendente como suspeito.

O caso não identifica invasão do núcleo de pagamentos, grupo criminoso ou entrada inicial. Seu valor é a pergunta concreta: quem pode alterar a instrução e como detectar essa alteração?

## 9.7 Perguntas ao fornecedor pelo responsável de pagamentos

| Pergunta | Evidência verificável | Decisão se faltar evidência |
|---|---|---|
| Qual cliente e ambiente essa identidade atende? | Responsável definido e registro do ambiente | Restringir uso até a validação delimitada |
| Quem pode emitir, exportar ou substituir? | Revisão atual de permissões e aprovação | Remover autorização desnecessária e confirmar |
| Conseguimos revogar rapidamente? | Teste de revogação e confirmação da contraparte | Exercitar antes de aceitar a garantia |
| Quais transações a utilizaram? | Registros autorizados pertinentes | Escalar a lacuna ao responsável pelo pagamento |
| O que ocorre ao isolar o fornecedor? | Procedimento demonstrado de serviço mínimo | Definir decisão e responsável pela continuidade |
| Como verificar mudanças de beneficiário? | Verificação independente e conciliação | Exigir canal confiável de confirmação |
| Que comunicação o fornecedor oferece? | Contato contratado, escopo e atualizações | Corrigir a dependência de comunicação |

A tabela é um modelo de revisão defensiva. Não avalia os controles de fornecedor específico. Transforma um alerta vago em decisão que o responsável pode revisar.

## 9.8 Endpoints, fraude e infraestrutura precisam de registro comum

Um alerta bancário pode chegar aos endpoints antes de fraude identificar transferência incomum. Uma identidade de fornecedor pode chegar à instituição antes de um cliente relatar problema. As equipes precisam de identificador comum de incidente e escalonamento claro.

Registre observação, validação, autorização revogada e atividade ainda sob análise. Vincule o atendimento aos fatos delimitados. Não distribua dados sensíveis brutos apenas para demonstrar que o caso existe.

Feche o ciclo depois da contenção. Confirme que a identidade nova funciona, a anterior não funciona e pagamentos atrasados foram conciliados. Reveja se alguma exceção emergencial permanece após a normalização.

As observações sustentam essa prioridade de coordenação. Não medem taxa de fraude bancária, classificam bancos ou estabelecem responsabilidade de autoridade de pagamentos por uma alegação anônima.

## 9.9 A população distinta de incidentes da supervisão

O relatório de estabilidade do BCB de outubro registra 99 incidentes comunicados por instituições supervisionadas até setembro de 2026, contra 76 em todo o ano de 2025 e 59 em 2024. Adverte que melhorias na detecção e comunicação aumentam a visibilidade. São comunicações de supervisão, uma população distinta dos casos, publicações e listagens deste relatório. [S324]

## 9.10 Uma visão anônima da exposição bancária

O grupo selecionado de bancos e finanças contém 28 domínios. O subconjunto de emissores contém 13 domínios de emissores de cartões. São populações selecionadas, sem constituir cadastro completo dos bancos brasileiros. [S3][S4]

| Observação | Grupo completo | Subconjunto de emissores |
|---|---|---|
| Domínios selecionados | 28 | 13 |
| Domínios com anúncios atuais de credenciais | 17 | 12 |
| Associações de dispositivos de funcionários | 3.760 | 3.113 |
| Associações de registros de credenciais | 904.473 | 822.157 |

O subconjunto de emissores contém ao menos 180.783 associações de dispositivos fora da categoria de funcionários. A titularidade permanece não resolvida. As observações não estabelecem infecção da infraestrutura operada pelos bancos nem acesso autorizado a pagamentos. [S3]

As observações distintas de cartões por emissor somam 920 no conjunto limitado de observações de cartões de pagamento. A soma não conta cartões únicos entre emissores, clientes, contas ativas ou perdas. Não deve ser somada às associações de dispositivos ou credenciais. [S4]

ESCOPO DOS NÚMEROS DOS CARTÕES

Estes números descrevem um conjunto limitado de observações de cartões de pagamento da Brandefense. Não estabelecem validade atual, titulares únicos, roubo nacional de cartões ou perdas por fraude.

Encaminhe evidências de funcionários para dispositivos e identidades. Encaminhe evidências de clientes para fraude e proteção dos clientes após validação. Mantenha o mesmo registro delimitado entre equipes, sem presumir que as populações representam as mesmas pessoas.

PRINCIPAIS CONCLUSÕES

01

Cliente, banco, fornecedor e infraestrutura de pagamentos têm limites diferentes.

02

Inventarie e revogue identidades transacionais com o responsável pelo pagamento.

03

Concilie beneficiários, atualizações do incidente e exceções antes do encerramento.

CAPÍTULO 10

# Regulação e resposta nacional

10

ESTE CAPÍTULO RESPONDE

Quais decisões de comunicação a equipe deve preparar antes de um evento?

## 3 dias úteis

prazo geral da ANPD, com escopo e exceções


10.1 Aplicabilidade antes dos prazos 92
10.2 A sequência da ANPD 93
10.3 A ciência do fornecedor é uma dependência operacional 93
10.4 Comunicação às pessoas precisa de responsável próprio 94
10.5 Sanções não são estimativa de perda do incidente 94
10.6 Exercite uma cronologia para vários canais 95

CAPÍTULO 10

# Regulação e resposta nacional

EM RESUMO

Incidentes com dados pessoais, interrupções financeiras e incidentes de telecomunicações têm canais diferentes. Na regulação citada da ANPD, o prazo geral é de três dias úteis após o controlador saber que dados pessoais foram afetados. Escopo, dano relevante e exceções ainda exigem avaliação. Registre essa ciência, identifique a entidade responsável e exercite as comunicações à autoridade e às pessoas afetadas com o fornecedor pertinente.

O capítulo apoia o planejamento e não determina as obrigações de uma organização. Leia o instrumento atual aplicável e obtenha orientação para a entidade, atividade e fatos reais.

## 10.1 Aplicabilidade antes dos prazos

| Marco | Escopo relevante | Requisito sustentado | Responsável |
|---|---|---|---|
| LGPD, artigos 46–48 | Tratamento sujeito à lei | Medidas de segurança e comunicação se houver risco ou dano relevante às pessoas [S10] | Controlador e proteção de dados |
| Resolução ANPD 15/2024 | Incidente relevante de dados pessoais | Comunicação à autoridade e às pessoas, ciência e registro [S11][S12] | Controlador, jurídico e liderança do incidente |
| Resolução CMN 4.893/2021 | Instituições dentro do escopo atual | Política cibernética e requisitos de processamento, armazenamento e nuvem [S14] | Conformidade financeira e gestão responsável |
| R-Ciber de telecomunicações | Prestadoras e deveres aplicáveis no texto consolidado | Comunicação de incidentes relevantes; ANATEL quando houver comunicação obrigatória à ANPD [S13] | Segurança e assuntos regulatórios |
| Estratégia nacional de cibersegurança | Coordenação estratégica nacional | Proteção de cidadãos, resiliência de serviços, cooperação e governança [S21] | Liderança e coordenação |

O instrumento do CMN exclui categorias específicas sujeitas a regulação do Banco Central. Não se deve aplicá-lo a toda organização classificada analiticamente como financeira. A regra de um provedor de pagamentos precisa ser estabelecida separadamente. [S14]

O texto de telecomunicações também tem disposições gerais, exceções e obrigações específicas entre portes. O artigo 2-C exige comunicação à ANATEL quando a comunicação à ANPD é obrigatória. O artigo 17 trata separadamente de incidentes relevantes que afetem substancialmente redes e dados de usuários. [S13]

## 10.2 A sequência da ANPD

A Resolução 15 entrou em vigor na publicação em 26 de abril de 2024. O prazo geral corre da ciência pelo controlador de que o incidente afetou dados pessoais. Legislação setorial pode estabelecer outro prazo. [S11]

| Etapa | Regra geral | Registro operacional |
|---|---|---|
| Avaliar escopo | Determinar incidente, dados e risco ou dano relevante | Fatos, categorias, pessoas e incertezas |
| Comunicar à autoridade | Em 3 dias úteis, sujeita a legislação específica | Ciência, prazo e comprovante de envio |
| Comunicar às pessoas | Em 3 dias úteis da ciência pertinente | Mensagem acessível e prova da comunicação |
| Complementar à autoridade | Complementação fundamentada em até 20 dias úteis após a comunicação | Questões pendentes e envio atualizado |
| Guardar registro | Pelo menos 5 anos do registro, com exceções previstas | Registro do incidente e decisão de retenção |

Agentes de pequeno porte elegíveis têm prazos dobrados nas disposições indicadas. A elegibilidade precisa ser verificada no marco específico. O relatório não presume que toda organização pequena se qualifique automaticamente. [S11]

Para entidades públicas abrangidas pelo artigo 23 da LGPD, há exceção particular de retenção ligada aos documentos permanentes aplicáveis. Outros deveres podem exigir guarda maior. Não aplique os cinco anos sem verificar essas condições. [S11]

A avaliação de risco relevante considera efeitos significativos sobre interesses e direitos junto com critérios de dados ou populações. Dados sensíveis, autenticação, finanças e pessoas vulneráveis podem ser pertinentes. Devem entrar na avaliação sem virar previsão não sustentada de uso indevido. [S11]

## 10.3 A ciência do fornecedor é uma dependência operacional

A ANPD orienta o operador a informar o controlador sem demora injustificada e fornecer as informações necessárias. A obrigação legal de comunicação do controlador não é transferida apenas porque o tratamento ocorre em fornecedor. [S12]

O contrato precisa dar a isso um caminho operacional. Defina contato monitorado, alternativa, responsável técnico e autorização de escalonamento fora do expediente. Teste com uma comunicação simulada e incompleta.

A primeira mensagem pode não estabelecer todas as pessoas ou categorias afetadas. Preserve o que estabelece e atribua as perguntas restantes. O jurídico deve avaliar a ciência com a informação real, sem esperar um relatório final conveniente.

## 10.4 Comunicação às pessoas precisa de responsável próprio

A Resolução 15 pede linguagem simples e compreensível e comunicação direta e individual quando as pessoas forem identificáveis. A alternativa pública tem condições, visibilidade e duração próprias. Não presuma que nota à imprensa seja suficiente. [S11]

Separe envio regulatório e mensagem ao cliente. A descrição técnica pode conter detalhe necessário à autoridade e ser inadequada para quem decide se deve confiar em uma ligação. Ambas precisam preservar os mesmos fatos estabelecidos.

O atendimento deve explicar processos genuínos de pagamento, recuperação e suporte. Use canal estabelecido e evite pedir mais dados sensíveis apenas para informar se a pessoa foi afetada. Escale relatos de fraude imediata ou dano pessoal.

## 10.5 Sanções não são estimativa de perda do incidente

O artigo 52 prevê várias sanções administrativas. A multa simples pode chegar a 2% do faturamento brasileiro da entidade privada, grupo ou conglomerado, excluídos tributos, limitada a R$50 milhões por infração. Aplicabilidade e processo importam. [S10]

A lei prevê conjunto diferente de sanções aplicáveis aos órgãos públicos. Um incidente não gera automaticamente multa máxima, e a perda relatada não é cálculo da penalidade. O relatório não conclui sobre conformidade ou responsabilidade nos casos.

O processo de saúde e a ação corretiva municipal da ANPD em 2026 tratam de eventos anteriores. Ilustram acompanhamento após o incidente original. Não viram novas invasões de 2026 porque houve atualização regulatória neste ano. [S114][S125]

## 10.6 Exercite uma cronologia para vários canais

| Situação simulada | Decisão necessária | Evidência de conclusão |
|---|---|---|
| Fornecedor relata cadastros copiados | Qual controlador e quais pessoas? | Avaliação de escopo e fundamento da ciência |
| Serviço de pagamento indisponível | Qual canal financeiro ou operacional se aplica? | Classificação por entidade e contato |
| Incidente telecom afeta dados | Há deveres perante ANPD e ANATEL? | Decisões e comprovantes separados |
| Fatos incompletos | O que comunicar agora e complementar depois? | Comunicação inicial fundamentada e responsáveis pelas lacunas |
| Canal indisponível | Qual alternativa confiável alcança as pessoas? | Canal testado e mensagem aprovada |
| Não há obrigação de comunicação | Por que se chegou à conclusão? | Fatos, fundamento e decisão de retenção |

O teste de conclusão é um registro utilizável. Deve mostrar quem decidiu, quando soube, qual canal usou e quais evidências faltaram. Um quadro de prazos sem responsáveis não é uma resposta exercitada.

PRINCIPAIS CONCLUSÕES

**01**

Determine entidade, tratamento e escopo antes de aplicar um prazo.

**02**

Preserve a ciência e separe comunicações à autoridade, às pessoas e ao setor.

**03**

Registre o fundamento mesmo quando não houver notificação.

CAPÍTULO 11

# Perspectivas e planejamento condicional

11

ESTE CAPÍTULO RESPONDE

Quais avaliações apoiam o planejamento e o que as mudaria?

**4**

cenários condicionais com condições explícitas de resposta


11.1 Avaliações principais 97

11.2 Sinais que devem mudar a resposta 97

11.3 Cenários condicionais 98

11.4 O que as evidências não permitem projetar 98

CAPÍTULO 11

# Perspectivas e planejamento condicional

EM RESUMO

Planeje para abuso de identidade, autorização de pagamentos, cópia de dados e continuidade. As listagens sustentam preparação de recuperação; casos públicos exigem respostas próprias aos clientes e à operação. As evidências não estabelecem probabilidade nacional de ataque ou próximo ator bem-sucedido. Use os cenários como premissas de planejamento. Mude a resposta quando mudarem as evidências de contas próprias, as categorias confirmadas ou as medidas de impacto do serviço.

## 11.1 Avaliações principais

| Avaliação | Confiança e base | Limite | Decisão |
|---|---|---|---|
| Validação de identidade deve acompanhar fraude | Alta para a necessidade; cadastros divulgados e pesquisa de sessões [S126][S127][S19][S20] | Sem origem comum ou transação bem-sucedida estabelecida | Definir responsáveis por identidade e clientes |
| Autorização de pagamento exige mais que senhas | Alta para o planejamento; guias alteradas e pesquisa financeira [S233][S18] | Sem prevalência nacional ou operador comum inferido | Testar assinaturas, aprovações e beneficiários |
| Recuperação inclui tarefas empresariais e dos clientes | Alta para a distinção documentada; atualizações de Santos [S128][S229][S230] | Capacidade mantida é afirmação da autoridade, sem medir tempo de todos os usuários | Exercitar alternativas e conciliação |
| Preparação para extorsão deve abranger muitos rótulos | Alta para a composição das listagens [S2] | Listagem não confirma invasão nem criptografia | Testar restauração e perda de dados sem depender do ator |
| Linguagem política precisa de avaliação própria | Alta para o limite analítico | Sem previsão de violência, impacto eleitoral ou direção estatal | Vincular atribuição pública à fonte real |

A confiança pertence à proposição da linha. Não certifica cada afirmação de grupo, pesquisador ou instituição. A mesma evidência pode apoiar um controle e deixar o mecanismo de invasão sem resposta.

## 11.2 Sinais que devem mudar a resposta

Um anúncio ganha relevância operacional quando a organização valida informação atual própria que o anunciante não deveria possuir. A data da alegação não basta. Diferencie reconhecer registro antigo e encontrar conta ou sessão ainda ativa.

Um incidente muda quando muda a função afetada. Se uma indisponibilidade administrativa passa a impedir tarefa crítica, o responsável deve reavaliar a alternativa. Use evidência atual do serviço, sem depender do rótulo inicial.

Um caso de dados pessoais muda quando categorias, pessoas ou provável dano ficam mais claros. Informação adicional pode exigir nova comunicação. Uma categoria suspeita pode ser excluída por avaliação posterior. Preserve a atualização e sua data de vigência.

Para atores, exija conexão concreta antes de unir campanhas. Técnica, referência nacional ou data próxima não estabelece controle comum. Infraestrutura compartilhada real ou relação sustentada pela fonte justificaria ligação mais restrita e documentada.

## 11.3 Cenários condicionais

São premissas de planejamento, sem previsões ou probabilidades de ataque.

| Se | Consequência possível | Primeira validação | Responsável e resposta |
|---|---|---|---|
| Uma credencial privilegiada atual for validada | O acesso pode ir além do aplicativo inicialmente citado | Verificar conta, privilégio, acessos e sessões | Identidade e resposta contêm o acesso validado |
| Fornecedor confirmar cópia de cadastros | Falsificação contextual pode continuar durante a recuperação | Estabelecer categorias, população e contato genuíno | Proteção de dados e atendimento coordenam orientações |
| Guia ou assinatura mudar sem aprovação | Instruções legítimas na aparência podem enviar recursos ao destino errado | Verificar beneficiário, histórico e intervalo | Tesouraria e fraude suspendem o fluxo inseguro conforme o procedimento |
| Alegação pública coincidir com degradação | Clientes podem confundir interrupção com roubo comprovado | Confirmar tarefas essenciais e separar acesso | Operação mitiga; comunicação publica status delimitado |

No cenário de pagamentos, não presuma fraude em toda transferência do intervalo. No cenário do fornecedor, não presuma categorias iguais para todos os clientes. A resposta deve diminuir ou ampliar conforme o responsável estabelece os fatos.

## 11.4 O que as evidências não permitem projetar

Volume de publicações não prevê perdas ou probabilidade de ataque a uma organização. Preços pedidos não estabelecem receita criminosa. Listagens não determinam se o próximo incidente terá criptografia, roubo, ambos ou nenhum.

O conjunto de domínios também não classifica a segurança dos setores brasileiros. A seleção não é representativa. O indicador nacional do Atlas sustenta priorização dentro do conjunto, sem medir probabilidade de invasão ou eficácia dos controles dos setores brasileiros.

Mantenha um registro breve de avaliações: proposição, evidência, alternativa plausível, condição para mudar e responsável. Reveja após incidente relevante, aviso de fornecedor ou exposição atual validada, sem reagir apenas a outra vanglória de ator.

PRINCIPAIS CONCLUSÕES

**01**

Use cenários como premissas condicionais, sem probabilidades.

**02**

Mude a resposta quando mudarem evidências atuais de conta, dados ou serviço.

**03**

Mantenha responsáveis e condições de revisão junto de cada avaliação.

CAPÍTULO 12

# Plano de ação

12

ESTE CAPÍTULO RESPONDE

Quem deve agir nos próximos 90 dias e o que demonstra a conclusão?

**30 / 60 / 90**

dias para validação, controles exercitados e revisão da gestão


12.1 O plano de 30/60/90 dias 101
12.2 Responsabilidades por função 103
12.3 Quadro de acompanhamento da liderança 104
12.4 Como a Brandefense pode ajudar 104

CAPÍTULO 12

# Plano de ação

EM RESUMO

Comece definindo responsáveis por identidades, autorização de pagamentos, fornecedores críticos e serviços mínimos. Teste os controles que diferenciam alegação externa e incidente confirmado. Complete o programa com exercícios observados de recuperação, atendimento e comunicação. O plano é condicional: contenha rapidamente acesso inseguro validado e registre por que evidências históricas ou não relacionadas foram encerradas. Apresente à gestão evidências de conclusão e exceções pendentes.

## 12.1 O plano de 30/60/90 dias

Os períodos são metas de gestão deste plano, sem substituir prazos legais. Deveres urgentes e acesso inseguro validado exigem a resposta imediata aplicável.

### 30 dias

Definir responsável e triagem para alertas de credenciais e acesso

RESPONSÁVEL
CISO e identidade

EVIDÊNCIA DE CONCLUSÃO
Contato, inventário e vocabulário de decisões

Validar titularidade, idade, situação e correção de evidências novas

RESPONSÁVEL
Operações de identidade

EVIDÊNCIA DE CONCLUSÃO
Decisão datada e revisão de acesso

Mapear assinaturas, contas de serviço e aprovação de pagamentos

RESPONSÁVEL
Pagamentos e tesouraria

EVIDÊNCIA DE CONCLUSÃO
Mapa aprovado com contatos de revogação

Definir processo genuíno de pagamento e recuperação dos clientes

RESPONSÁVEL
Fraude e atendimento

EVIDÊNCIA DE CONCLUSÃO
Canal de verificação e roteiro aprovado

Mapear fornecedores por serviço, controlador, categorias e contato alternativo

RESPONSÁVEL
Compras e proteção de dados

EVIDÊNCIA DE CONCLUSÃO
Registro utilizável e contato testado

### Determinar comunicações por entidade e atividade

RESPONSÁVEL
Jurídico e regulação

EVIDÊNCIA DE CONCLUSÃO
Escopo, destinatários, ciência e decisores

### Verificar aplicabilidade da vulnerabilidade Windows citada

RESPONSÁVEL
Endpoints e tecnologia de pagamentos

EVIDÊNCIA DE CONCLUSÃO
Avaliação de ativos e versões e correção pertinente

## 260 dias

### Implantar autenticação resistente a phishing na população privilegiada e remota priorizada

RESPONSÁVEL
Identidade e infraestrutura

EVIDÊNCIA DE CONCLUSÃO
Cobertura, recuperação testada e exceções

### Revogar sessões inseguras validadas e revisar recuperação e delegações

RESPONSÁVEL
Identidade e resposta

EVIDÊNCIA DE CONCLUSÃO
Teste de invalidação e avaliação das alterações

### Simular alteração de destino com instruções fictícias

RESPONSÁVEL
Tesouraria e fraude

EVIDÊNCIA DE CONCLUSÃO
Verificação independente, escalonamento e decisão de interrupção

### Restringir instalação desnecessária de suporte remoto e extensões

RESPONSÁVEL
Endpoints e serviços

EVIDÊNCIA DE CONCLUSÃO
Lista aprovada e exceção testada

### Rever segredos de contas de serviço e assinaturas nos fornecedores críticos

RESPONSÁVEL
Pagamentos e engenharia

EVIDÊNCIA DE CONCLUSÃO
Lista verificada e exercício de rotação e revogação

### Testar modo manual ou alternativo de serviço crítico

RESPONSÁVEL
Continuidade e operação

EVIDÊNCIA DE CONCLUSÃO
Exercício observado e plano de conciliação

### Simular aviso incompleto do fornecedor e ciência do controlador

RESPONSÁVEL
Jurídico, proteção de dados e fornecedor

EVIDÊNCIA DE CONCLUSÃO
Cronologia, comunicação inicial e responsáveis pelas lacunas

Testar mensagens públicas com alegação e interrupção simuladas

RESPONSÁVEL
Comunicação e serviço

EVIDÊNCIA DE CONCLUSÃO
Declaração que separa impacto, dados e atribuição

## 390 dias

Restaurar serviço crítico com identidades de recuperação separadas da produção

RESPONSÁVEL
Infraestrutura e responsável pelo negócio

EVIDÊNCIA DE CONCLUSÃO
Restauração observada, integridade e aprovação operacional

Exercitar atendimento após cópia de cadastros

RESPONSÁVEL
Fraude e atendimento

EVIDÊNCIA DE CONCLUSÃO
Resultados, contato confiável e escalonamento

Rever decisões de alertas e titularidades pendentes

RESPONSÁVEL
CISO e identidade

EVIDÊNCIA DE CONCLUSÃO
Amostra encerrada, fila e responsáveis pelas exceções

Apresentar resultados testados e dependências à gestão

RESPONSÁVEL
CISO e patrocinador executivo

EVIDÊNCIA DE CONCLUSÃO
Registro de decisões, recursos, responsáveis e novas datas

O plano se liga às evidências, sem depender da reputação do ator. Identidade sustenta revisão de contas e sessões. O caso municipal sustenta beneficiários. Santos sustenta serviço mínimo e conciliação. As listagens sustentam preparação de recuperação. [S18][S19][S20][S233][S229][S2]

## 12.2 Responsabilidades por função

**Liderança e CISO.** Aprove quais interrupções criariam consequência inaceitável. Financie a resposta ligada a esses serviços. Exija responsável e alternativa exercitada, sem aceitar uma política não testada como conclusão.

**Identidade e resposta a incidentes.** Estabeleça se a evidência externa corresponde a identidade atual da organização. Reveja privilégios, sessões e recuperação. Registre decisão mesmo para evidência histórica, não relacionada ou já corrigida.

**Pagamentos e tesouraria.** Proteja autorização transacional e aprovação independente. Saiba quem pode enviar instruções, alterar credenciais e revogar autorização. Teste beneficiários sem usar recursos reais de clientes.

**SOC e endpoints.** Investigue suporte remoto suspeito, mudanças em extensões e atividade relevante. Use o contexto para distinguir administração autorizada e abuso. O nome da ferramenta não deve decidir sozinho.

**Proteção de dados e jurídico.** Preserve a ciência, determine o controlador e avalie risco ou dano relevante. Separe autoridade, pessoas afetadas, setor e polícia. Garanta informação suficiente nos avisos do fornecedor.

**Atendimento e comunicação.** Ofereça verificação confiável de contatos e pagamentos. Explique categorias confirmadas e estado do serviço em linguagem simples. Preserve incertezas, sem adotar quantidade de ator ou garantia preliminar sem data.

**Compras e responsáveis pelos fornecedores.** Mantenha contatos utilizáveis fora das condições normais. Exercite troca de escopo, registros e impacto nos clientes. Registre o que não foi estabelecido e quem acompanha.

## 12.3 Quadro de acompanhamento da liderança

| Área de decisão | Evidência a apresentar | Evite substituir por |
|---|---|---|
| Identidade | Alertas com decisões validadas e responsáveis pendentes | Volume total de registros expostos |
| Autorização de pagamento | Identidades aprovadas e teste de alteração concluído | Quantidade de produtos de segurança |
| Fornecedores | Contatos e comunicação delimitada exercitados | Número de contratos |
| Recuperação | Serviço mínimo observado e restauração aprovada | Contagem de backups bem-sucedidos |
| Proteção dos clientes | Exercício da equipe e verificação confiável | Número de avisos enviados |
| Comunicação regulatória | Cronologia, aplicabilidade e comprovantes | Prazo universal de notificação |

Use denominadores próprios de cada decisão. Cobertura de autenticação trata da população priorizada de contas. Restauração trata de serviço definido. Atendimento trata de cenário específico. Não combine tudo em probabilidade inventada de incidente nacional ou empresarial.

Reveja pendências junto do trabalho concluído. A exceção precisa de responsável, motivo, compensação e próxima data. O quadro deve permitir decidir recursos, sem premiar maior volume de alertas.

## 12.4 Como a Brandefense pode ajudar

A Brandefense oferece Cyber Threat Intelligence, Digital Risk Protection e External Attack Surface Management. As capacidades podem apoiar monitoramento, investigação e resposta a exposições relevantes. Não substituem validação de contas, decisões de incidente ou deveres legais. [S22]

Leve um processo concreto à conversa: alerta de domínio próprio, dependência de fornecedor, fila de falsificação de marca ou cenário de proteção de clientes. Combine evidência, responsável e teste de encerramento antes de avaliar pelo volume de alertas.

Solicite uma demonstração da Brandefense.

PRINCIPAIS CONCLUSÕES

**01**

Valide identidades e autorização transacional com responsáveis definidos.

**02**

Teste comunicação de fornecedores, serviço mínimo e recuperação com cenários simulados.

**03**

Apresente resultados observados e exceções até o dia 90.

APÊNDICES

# Apêndices

A–D

ESTE CAPÍTULO RESPONDE

Quais datas, populações e limites acompanham as conclusões?

## Separados

publicações, listagens, casos, domínios, registros e resultados financeiros


Apêndice A. Escopo e limites das evidências 107

Apêndice B. Registro de evidências 112

Apêndice C. Fontes 117

Apêndice D. Glossário 122

# Apêndice A. Escopo e limites das evidências

Os países de comparação foram selecionados como exemplos apenas para fornecer contexto; a sua escolha não implica uma classificação nem uma avaliação política.

## A.1 Período observado e data de corte

O período solicitado é de 1 de janeiro a 22 de novembro de 2026. Observações clandestinas usam a publicação do post. A Ransompedia usa a data da listagem. Relatos públicos separam incidente, descoberta, divulgação, operação e atualização quando disponíveis. [S1][S2]

A data de corte das observações foi 22 de novembro de 2026; a verificação das fontes continuou em 23 de novembro. O dia de corte ainda estava em andamento quando as observações terminaram. O relatório não afirma um censo completo até o fim do dia. A atividade recente cobre 8 a 22 de novembro e inclui atualizações, pesquisas e operações sobre condutas anteriores.

A modificação de uma página pode diferir da publicação original. Migrações oficiais podem atualizar muitas páginas juntas. Essas datas não criam um mês de incidente. Data de divulgação não resolvida permanece não resolvida.

## A.2 Populações das fontes

| População | O que descreve | Limite essencial |
|---|---|---|
| Publicações clandestinas | Observações associadas ao Brasil e trechos autênticos selecionados [S1] | Associação ao país não significa necessariamente direcionamento |
| Listagens de ransomware | Alegações públicas de extorsão associadas ao país [S2] | Sem confirmação independente de criptografia, roubo ou pagamento |
| Conjunto selecionado | 250 domínios principais avaliados em dez grupos [S3] | Titularidade e independência não validadas; sem inferência de prevalência nacional |
| Observações de cartões | Conjunto limitado de observações de cartões de pagamento associados ao Brasil [S4] | Sem estimativa nacional de exposição ou perda |
| Divulgações oficiais | Conclusões de organização ou autoridade | Confirmação limitada à proposição e à data |
| Comunicados policiais | Investigações, suspeitas e intervenções | Busca ou prisão não implica condenação |
| Pesquisa técnica | Conclusões atribuídas sobre campanha ou vulnerabilidade | Geografia, período e confiança pertencem à fonte |

As populações não são somadas em um total de ataques brasileiros. Um evento pode gerar vários posts, listagem, comunicado, processo regulatório e operação posterior. Muitos eventos podem nunca ser divulgados.

## A.3 O que uma comparação entre países sustenta

A comparação usa Argentina, Chile, Colômbia e México como comparadores regionais. Todos têm relações regionais significativas em serviços, indústria ou infraestrutura. A tabela fornece contagens absolutas de listagens na mesma fonte e data de corte. [S2]

Não controla população, economia, organizações, divulgação ou visibilidade dos atacantes. Não sustenta classificação da segurança nacional. Valores anuais de 2025 e parciais de 2026 preservam períodos diferentes.

Os totais brasileiros por grupo e mês conciliam com 206 listagens. Nomes são rótulos registrados e não estabelecem identidades jurídicas, membros comuns ou continuidade de operadores. Categorias de atividade descrevem a população da fonte, sem prevalência setorial nacional.

## A.4 Limites do conjunto e dos controles passivos

Os 250 domínios foram selecionados intencionalmente e abrangem serviços importantes públicos e privados. Não formam classificação oficial por receita. Domínios ou entidades relacionados podem compartilhar operador, e domínio principal candidato não comprova independência jurídica. [S3]

O retrato da exposição foi lido em 22 de novembro de 2026. O Atlas fornece indicador nacional de 80/100 (F) para o conjunto selecionado. Somente essa nota nacional é publicada. Contagens setoriais anônimas descrevem populações distintas de sinais, sem notas de organizações ou classificação setorial de segurança. [S3]

Leia o campo `orgs_listed_for_sale_now` do CSV setorial como "Domínios com ofertas atuais de credenciais". Sua unidade é um domínio selecionado com uma credencial associada atualmente anunciada à venda. Não conta organizações oferecidas à venda nem anúncios individuais.

Não há conjunto completo de higiene passiva nem índice de higiene disponível. Observações ausentes de configuração continuam indisponíveis e não estabelecem falha de e-mail ou ausência de proteção.

Se uma associação de conta for validada posteriormente, registre categoria e data. Funcionário, prestador, cliente e relação não resolvida têm implicações diferentes. Credenciais históricas, ofertas atuais, dispositivos e documentos não são medidas intercambiáveis.

## A.5 Escopo dos cartões de pagamento

ESCOPO DOS NÚMEROS DOS CARTÕES

Estes números descrevem um conjunto limitado de observações de cartões de pagamento da Brandefense. Não estabelecem validade atual, titulares únicos, roubo nacional de cartões ou perdas por fraude.

Observar um cartão não estabelece pessoa única, conta ativa, autorização bem-sucedida ou origem do roubo. O status anunciado permanece uma alegação até validação pelo emissor responsável. Não são publicados identificadores por emissor nem dados pessoais de cartões. [S4]

Os números globais da pesquisa de terminais pertencem a outra população. Não são somados aos agregados de cartões de pagamento da Brandefense nem apresentados como total brasileiro. [S232]

## A.6 Cobertura de incidentes e descobertas não resolvidas

O registro inclui divulgações confirmadas, campanhas atribuídas, investigações, anúncios, contexto e exclusões. As categorias não formam denominador único de incidentes confirmados. Os identificadores organizam o relatório, sem constituir numeração nacional de incidentes.

A revisão oficial abrange CTIR Gov/GSI, CERT.br, ANPD, PF, Banco Central, ANATEL e fontes selecionadas de polícias estaduais. Notícias em português, inglês, espanhol e russo acrescentam descobertas e corroboração. A cobertura varia entre arquivos e idiomas.

Vários arquivos, comunicados e descobertas recentes não puderam ser completamente estabelecidos. A cobertura estadual não enumera cada arquivo de cada mês e estado. Item ausente significa falta de evidência sustentada naquela parte, sem significar zero incidentes no país.

Algumas notícias reproduzem declaração empresarial sem comunicado oficial diretamente revisado. Os sujeitos permanecem genéricos ou fora dos casos nomeados. Duplicações de agregadores e datas incertas não entram como totais confirmados.

## A.7 Linguagem de evidência e confiança

| Rótulo | Significado no relatório |
|---|---|
| Observação | Registro retido sustenta a publicação ou quantidade indicada |
| Alegação | Fonte afirma posse, acesso ou impacto não estabelecido independentemente |
| Confirmação oficial | Organização ou autoridade confirma o fato específico indicado |
| Pesquisa atribuída | Pesquisador identificado fornece conclusão com escopo e confiança próprios |
| Inferência analítica | Interpretação fundamentada, com evidência e alternativa |
| Modelo analítico | Relação ou cenário de planejamento sem operador compartilhado comprovado |

Alta confiança se aplica a uma proposição específica. Não autentica todas as afirmações de ator ou instituição. Não verificado não significa falso. Um incidente pode estar confirmado enquanto entrada, ator e pessoas afetadas continuam sem resposta.

Uma conta atual validada exige resposta diferente de registro antigo reconhecido em anúncio. A certeza da fonte não é a certeza do relatório. A diferença acompanha o caso, sem ficar apenas neste apêndice.

## A.8 Nomes, privacidade e neutralidade

Um sujeito é nomeado em incidente somente quando confirmação oficial e ampla cobertura sustentam o caso específico. O registro público documenta a base. Autoridades de orientação e pesquisadores citados não recebem automaticamente aprovação como vítimas nomeadas.

Os demais sujeitos recebem papéis amplos que podem descrever vários órgãos. Títulos e endereços que revelariam a identidade são abreviados na bibliografia. Os trechos de apoio permanecem no registro privado.

Trechos mantêm palavras autênticas com omissões e redações entre colchetes. Não contêm dados pessoais, credenciais ativas, contatos criminosos ou detalhes de acesso às vítimas. Traduções em português são identificadas e mantêm o original.

O relatório não toma posição sobre governos, partidos, tribunais, eleições, sanções, tarifas ou relações exteriores. Associações estatais ou motivos permanecem avaliações atribuídas quando necessários. Insultos, acusações e recrutamento de atores são omitidos.

## A.9 Verificação jurídica e de vulnerabilidades

O capítulo jurídico separa entidade aplicável, condição, ciência e canal. Não determina responsabilidade nem certifica conformidade. É necessário verificar o instrumento atual para a entidade e o incidente reais. [S10][S11][S12][S13][S14]

A vulnerabilidade foi verificada na NVD, com versões afetadas e correção vinculada do fornecedor. A CVE-2024-49138 trata de elevação de privilégios Windows. Sua presença na pesquisa não estabelece exploração em organização brasileira nomeada. [S5][S232]

Por exemplo, o registro identifica Windows 10 22H2 anterior a 10.0.19045.5247, Windows 11 23H2 anterior a 10.0.22631.4602 e Windows Server 2022 anterior a 10.0.20348.2966. São limites selecionados, sem lista completa de aplicabilidade. [S5]

O responsável deve conferir a versão real e a orientação atual do fornecedor. Nome genérico do produto não basta para decidir se um dispositivo está afetado ou corrigido. A confirmação da atualização deve integrar o registro do endpoint.

## A.10 Integridade das edições

A edição brasileira foi traduzida do original inglês e está marcada "Traduzido com IA". Preserva números, identificadores de casos, fontes e diretivas. A edição em inglês prevalece em divergências.

Verificações de consistência validam referências internas e limites declarados. Não estabelecem cobertura nacional exaustiva, validam alegações anônimas ou constituem aprovação de publicação. A situação da revisão e liberação fica fora das conclusões analíticas.

# Apêndice B. Registro de evidências

## B.1 Vinte e seis casos e seus limites

O registro resume dez alegações e dezesseis casos de divulgação ou investigação. Não descreve vinte e seis invasões confirmadas. Vários casos têm múltiplas datas ou resultados pendentes.

| Caso | Data ou etapa | Setor | Evidência e limite |
|---|---|---|---|
| A | Publicação em 3 de janeiro | Administração pública | Arquivo incompleto alegado; conteúdo e acesso atual não verificados |
| B | Publicação em 4 de janeiro | Varejo | Contatos, pedidos e entregas alegados; origem e população não verificadas |
| C | 14 de janeiro e publicações relacionadas | Serviços municipais | Alegações fiscais; linhas e bases não contam incidentes independentes |
| D | Publicação em 2 de fevereiro | Educação | Oferta de dados familiares e financeiros; registros não são pessoas únicas |
| E | 6 de fevereiro e circulação posterior | Serviços financeiros | Assistente virtual; data final posterior à publicação armazenada |
| F | Publicação em 11 de novembro | Bancos | Contatos alegados; atualidade, obtenção e venda não verificadas |
| G | Publicação em 17 de novembro | Pagamentos | Oferta explicitamente de 2025; sem nova invasão de 2026 estabelecida |
| H | Publicação em 19 de novembro | Software empresarial | Tabela alegada; acessos do fornecedor e clientes não verificados |
| I | Publicação em 24 de março | Serviços de pagamento | Oferta de certificados e rede; sem autorização verificada de transferência |
| J | Publicação em 6 de julho | Infraestrutura financeira | Acesso alegado; ambiente, permissões e impacto não verificados |
| K | Descoberta em 6; nota em 12 de novembro | Seguros | CVP confirma cópia de cadastros; exclusões preliminares datadas |
| L | Descoberta em 4; nota em 13 de novembro | Administração pública | Tesouro identifica duas populações; sem total combinado de pessoas |

| Caso | Data ou etapa | Setor | Evidência e limite |
|---|---|---|---|
| M | 14–16 de novembro; atualizações posteriores | Pagamentos municipais | Guias alteradas; bloqueio e início das devoluções, sem conclusão estabelecida |
| N | Janeiro; relatório posterior do semestre | Bancos | Suspensão do Pix; resultados institucionais e dos clientes separados |
| O | 6–19 de novembro | Administração portuária | Incidente e recuperação; capacidade atribuída à APS |
| P | Evento em junho; nota em setembro | Administração pública | Cadastro histórico; sem invasão do cadastro atual estabelecida |
| Q | Comunicados em junho | Alertas públicos | Mensagens falsas e canais alternativos; sem ator ou motivo político |
| R | Evento em julho; nota policial em outubro | Serviços institucionais | Investigação de roubo e extorsão; sem família, criptografia ou condenação |
| S | Nota policial em fevereiro | Dados de saúde | Suposto uso não autorizado e comercial; investigação não é condenação |
| T | Nota em 14 de novembro | Saúde | Unimed Natal confirma resposta e atendimento; sem conclusão de roubo ou recuperação final |
| U | Evento em outubro; nota em 19 de novembro | Benefícios de saúde | Comunicado indexado; apenas prestadores pessoa jurídica, texto completo não revisado |
| V | 1–9 de novembro | Administração da saúde | Incidente estadual e licenciamento compartilhado; sem segunda invasão municipal |
| W | 22–24 de março | Bancos | Carta da instituição em cópia e cobertura ampla; resultados de clientes e instituição separados |
| X | Descoberta em 21 de setembro; notícia em outubro | Projetos de saúde | Investigação oficial de possível acesso; sem uso público indevido estabelecido |

| Caso | Data ou etapa | Setor | Evidência e limite |
|---|---|---|---|
| Y | Evento em 2 de novembro; documento em 12 de novembro | Ativos digitais | Cópia de documento do investidor; efeito financeiro não estimável com confiabilidade |
| Z | Evento em 4 de outubro | Serviços financeiros de projetos | Nota oficial; data de publicação e recuperação concluída incertas |

Os primeiros dez são observações de alegações. Os demais preservam o status da fonte: divulgação organizacional, relato de autoridade ou investigação policial. Confirmar uma investigação não estabelece cada alegação.

## B.2 Fichas de publicações originais

| Ficha | Caso | Data da publicação | Proposição retida |
|---|---|---|---|
| B01 | A | 2026-01-03 | Autor descreve arquivo documental associado a órgão público |
| B02 | B | 2026-01-04 | Vendedor lista contatos, pedidos e entregas |
| B03 | C | 2026-01-14 | Narrativa anuncia bases fiscais municipais |
| B04 | D | 2026-02-02 | Vendedor alega dados de responsáveis e finanças educacionais |
| B05 | E | 2026-02-06 | Narrativa parcial contém datas inconsistentes |
| B06 | F | 2026-11-11 | Vendedor oferece contatos bancários integrais ou segmentados |
| B07 | G | 2026-11-17 | Anúncio Pix identifica explicitamente material de 2025 |
| B08 | H | 2026-11-19 | Alegação de software identifica tabela de clientes |
| B09 | I | 2026-03-24 | Oferta de certificados e, separadamente, rede interna |
| B10 | J | 2026-07-06 | Publicação anuncia acesso a infraestrutura financeira |

Os dez trechos usam fragmentos autênticos em inglês. Colchetes indicam omissões ou redações. A edição portuguesa oferece tradução identificada junto do original. O trecho não é amostra autenticada dos dados anunciados. [S1]

## B.3 Campanhas e comunicados públicos

| Família de evidências | Fonte de apoio | Proposição e limite |
|---|---|---|
| Composição de ransomware | Ransompedia [S2] | 206 listagens, sem resultados de invasão verificados |
| Campanha de pagamentos | Google [S18] | Identidades e fornecedores investigados; sem ligação com os vendedores selecionados |
| Malware bancário | Elastic [S19] | Comportamentos; domínios monitorados não são bancos vítimas |
| Roubo no navegador | IBM [S20] | Dispositivos e sessões de clientes; sem inferência sobre infraestrutura bancária |
| Espionagem e roubo de informações | Kaspersky [S161] | Brasil incluído; atribuição moderada ao Armored Likho, sem patrocinador estatal |
| Redirecionamento de pagamentos | Kaspersky [S105] | Contexto de mecanismo GoPix; sem taxa nacional de fraude |
| Ameaça bancária regional | Kaspersky [S106] | Contexto JanelaRAT; quantidade brasileira pertence a 2025 |
| Alertas públicos | CTIR [S147][S148][S149][S150][S151][S152][S153] | Mecanismos e campanhas possíveis; números de recomendações não são incidentes |
| Pesquisa de terminais | Cybernews e NVD [S232][S5] | Quantidades globais e limites de versões; sem total brasileiro de vítimas |

## B.4 O que justificaria ligar registros

Um nome comum não basta para ligar anúncio, comunicado e listagem. Datas podem coincidir, e um ator pode copiar detalhes públicos. A ligação exige evidências do mesmo evento e declaração explícita do que está conectado.

Uma republicação pode repetir alegação genuína sem demonstrar nova invasão. Preserve sua data e relação com a fonte e vincule à narrativa existente quando sustentado. Não acrescente outra organização afetada.

Um evento de fornecedor pode afetar vários clientes, mas exige evidência específica de cada um. O catálogo do fornecedor não fornece a lista ausente. Isso importa especialmente em pagamentos, educação e software empresarial.

A declaração hospitalar na tabela adicional e o dossiê policial de extorsão mantêm datas relatadas distintas. Não são ligados como mesmo incidente. [S181][S122] Na declaração do setor financeiro, a data do HTML prevalece sobre a data inconsistente do PDF. [S177]

## B.5 Registro de decisões e correções

Cada conclusão importante tem entrada no livro de evidências com fonte, tipo, confiança, alternativa e ação responsável. O registro de cobertura indica inclusão, menção, contexto ou exclusão e permanece no registro privado de evidências.

Uma correção futura deve identificar a proposição alterada, a nova fonte e a data. Deve atualizar as duas edições, fichas de evidências e explicações agregadas conjuntamente. Nova atribuição não deve revisar silenciosamente resultados anteriores.

# Apêndice C. Fontes

Cada entrada informa a data de revisão. Endereço abreviado protege um sujeito genérico e vem identificado. Trecho indexado é distinguido explicitamente de documento completo revisado.

**S1:** Odin by Brandefense. Retained Brazil-associated post observations, 1 January–22 November 2026. Verificado em 2026-11-22.

**S2:** Ransompedia. Brazil and four regional peers, dated listing observations. Verificado em 2026-11-22.

**S3:** Odin by Brandefense. Atlas exposure snapshot and selected 250-domain portfolio, read 22 November 2026. Verificado em 2026-11-22.

**S4:** Odin by Brandefense. Limited Brazil-associated payment-card observation set. Verificado em 2026-11-22.

**S5:** NIST National Vulnerability Database. CVE-2024-49138 record and affected-version boundaries. Verificado em 2026-11-22.

**S10:** Presidência da República. Lei 13.709/2018, consolidated LGPD, Articles 46–52. Verificado em 2026-11-22.

**S11:** ANPD. Resolution 15 of 24 April 2024, regulatory-process copy; published 26 April 2024. Verificado em 2026-11-23.

**S12:** ANPD. Comunicação de Incidente de Segurança: procedure and questions. Verificado em 2026-11-22.

**S13:** ANATEL. Resolution 740/2020, consolidated telecom cybersecurity regulation. Verificado em 2026-11-22.

**S14:** Banco Central do Brasil. CMN Resolution 4.893 of 26 February 2021, current consolidated text. Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S16:** DataReportal. Digital 2027: Brazil, October 2026 contextual figures. Verificado em 2026-11-22.

**S17:** Tribunal Superior Eleitoral. Eleições 2026: confira as principais datas do calendário eleitoral. Verificado em 2026-11-22.

**S18:** Google Threat Intelligence Group / Mandiant. Financially Motivated Threat Actor BREEZE COMET Targets Brazil, 1 September 2026. Verificado em 2026-11-22.

**S19:** Elastic Security Labs. TCLBANKER: Brazilian Banking Trojan Spreading via WhatsApp and Outlook, 7 May 2026. Verificado em 2026-11-22.

**S20:** IBM Trusteer. UnregStealer: Human-operated browser credential theft targeting Brazilian banking, 16 June 2026. Verificado em 2026-11-22.

**S21:** Câmara dos Deputados. Decree 12.573 of 4 August 2025, original national cybersecurity strategy. Verificado em 2026-11-22.

**S22:** Brandefense. Request a Demo. Verificado em 2026-11-22.

**S23:** Kaspersky GReAT. BeatBanker: um trojan de dupla função para Android, 10 March 2026. Verificado em 2026-11-22.

**S24:** Kaspersky GReAT. A VBScript campaign distributed through WhatsApp deploying RMM software, 22 June 2026. Verificado em 2026-11-22.

**S25:** Check Point Research. Gaming the system: Brazilian government sites and SEO fraud, 2 September 2026. Verificado em 2026-11-22.

**S26:** MITRE ATT&CK. Spearphishing Attachment. Verificado em 2026-11-22.

**S27:** MITRE ATT&CK. PowerShell. Verificado em 2026-11-22.

**S28:** MITRE ATT&CK. System Information Discovery. Verificado em 2026-11-22.

**S29:** MITRE ATT&CK. Screen Capture. Verificado em 2026-11-22.

**S30:** Receita Federal. Inscrever Entidade no Cadastro Nacional de Pessoas Jurídicas. Verificado em 2026-11-22.

**S101:** Banco do Nordeste. Banco do Nordeste market notice, 26 January 2026. Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S102:** Polícia Federal. A health-data service provider; 2026-02-04. Verificado em 2026-11-22.

**S103:** Official source. An interstate electronic-fraud investigation; 2026-02-24. Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S104:** Polícia Federal. A payment-service-provider fraud investigation; 2026-03-16. Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S105:** Kaspersky GReAT. Gopix banking malware; 2026-03-16. Verificado em 2026-11-22.

**S106:** Kaspersky GReAT. Janelarat banking malware; 2026-04-13. Verificado em 2026-11-22.

**S107:** Official source. An sms impersonation fraud campaign; 2026-05-14. Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S108:** Official source. A false bank-manager fraud campaign; 2026-05-18. Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S110:** Official source. A bank-insider fraud investigation; 2026-05-22. Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S112:** El País. A bank communication error; 2026-06-12 (endereço do artigo omitido). Verificado em 2026-11-22.

**S113:** Fonte oficial (endereço omitido; mantido no registro privado de evidências). A public warning platform; 2026-06-20. Verificado em 2026-11-23.

**S114:** ANPD. A multi-state healthcare operator; 2026-07-08 (endereço do artigo omitido). Verificado em 2026-11-22.

**S115:** Polícia Federal. A bank-insider investigation; 2026-07-16. Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S116:** Polícia Federal. A social-account insider investigation; 2026-07-31 (endereço do artigo omitido). Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S117:** Polícia Federal. A cross-border laundering investigation; 2026-08-13. Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S119:** Official source. A federal regulatory agency; 2026-09-03 (endereço do artigo omitido). Verificado em 2026-11-22.

**S120:** CTIR Gov / GSI. Government website search poisoning; 2026-09-08. Verificado em 2026-11-22.

**S122:** Polícia Federal. An institutional extortion investigation; 2026-10-07. Verificado em 2026-11-22.

**S124:** Official source. A federal agency preventive service suspension; 2026-10-21 (endereço do artigo omitido). Verificado em 2026-11-22.

**S125:** ANPD. A municipal health-data publication case; 2026-10-26 (endereço do artigo omitido). Verificado em 2026-11-22.

**S126:** Caixa Seguridade. Caixa Seguridade: CVP market notice, 12 November 2026. Verificado em 2026-11-22.

**S127:** Ministério da Fazenda / Tesouro Nacional. Tesouro Nacional incident notice, 13 November 2026. Verificado em 2026-11-23.

**S128:** Autoridade Portuária de Santos. Santos partial administrative recovery, 16 November 2026. Verificado em 2026-11-22.

**S129:** Polícia Federal. An international digital-fraud operation; 2026-11-17. Verificado em 2026-11-22.

**S130:** Polícia Federal. A social-benefit digital-account fraud investigation; 2026-11-17. Verificado em 2026-11-22.

**S131:** CNN Brasil. A large bank; 2026-11-18 (endereço do artigo omitido). Verificado em 2026-11-22.

**S132:** Viva. A delivery platform; 2026-11-19 (endereço do artigo omitido). Verificado em 2026-11-22.

**S133:** Official source. A telephone-message fraud facility; 2026-11-19. Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S134:** Banco Central do Brasil. A financial institution; not resolved; indexed current registry (endereço do artigo omitido). Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S135:** Banco Central do Brasil. A financial institution; not resolved; PDF indexed around April 2026 (endereço do artigo omitido). Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S136:** Banco Central do Brasil. A public-sector institution; not resolved; current registry (endereço do artigo omitido). Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S137:** Banco Central do Brasil. A public-sector institution; not resolved; current registry (endereço do artigo omitido). Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S138:** Banco Central do Brasil. A financial institution; not resolved; current registry (endereço do artigo omitido). Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S139:** Banco Central do Brasil. A public-sector access incident; 2025; registry updated in 2026 (endereço do artigo omitido). Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S147:** CTIR Gov / GSI. An official campaign warning; 2026-05-21. Verificado em 2026-11-22.

**S148:** CTIR Gov / GSI. An official campaign warning; 2026-05-21. Verificado em 2026-11-22.

**S149:** CTIR Gov / GSI. An official campaign warning; 2026-05-21; recommendation03 updated 2026-06-17. Verificado em 2026-11-22.

**S150:** CTIR Gov / GSI. An official campaign warning; 2026-05-21. Verificado em 2026-11-22.

**S151:** CTIR Gov / GSI. An official campaign warning; 2026-05-21. Verificado em 2026-11-22.

**S152:** CTIR Gov / GSI. An official campaign warning; 2026-05-21. Verificado em 2026-11-22.

**S153:** CTIR Gov / GSI. An official campaign warning; 2026-06-24. Verificado em 2026-11-22.

**S154:** Polícia Federal. An infostealer distribution investigation; 2026-08-04 12:23. Verificado em 2026-11-22.

**S155:** Polícia Federal. A bank-fraud proceeds investigation; 2026-11-09 14:54. Verificado em 2026-11-22.

**S156:** Polícia Federal. An electronic bank-fraud investigation; 2026-11-11 07:59. Verificado em 2026-11-22.

**S161:** Kaspersky GReAT. An attributed information-theft and espionage campaign; 2026-07-03. Verificado em 2026-11-23.

**S165:** Fonte oficial (endereço omitido; mantido no registro privado de evidências). A public-sector health-program portal; 2026-11-19 notice. Verificado em 2026-11-23. Trecho oficial indexado lido; texto completo não revisado.

**S166:** Unimed Natal. A regional healthcare cooperative; 2026-11-14 primary notice; 2026-11-18 FAQ index. Verificado em 2026-11-22.

**S167:** Prefeitura de Cuiabá. A shared state sanitary-surveillance platform; 2026-11-02 16:27 state primary; 2026-11-09 09:52 municipal follow-up. Verificado em 2026-11-22.

**S169:** Investor-authored financial statement. Subsequent-event note 16, financial statements authorised 12 November 2026; third-party-hosted copy (endereço do artigo omitido). Verificado em 2026-11-22.

**S170:** Agência Brasil. Public-benefits query-service reporting, 26 May 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S171:** Convergência Digital. Operator statement on attack attempts, 5 November 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S172:** Fonte oficial (endereço omitido; mantido no registro privado de evidências). Project-portal incident notice; incident identified 4 October 2026. Verificado em 2026-11-22.

**S173:** Diário do Comércio. Digital-commerce platform notification reporting, 13 November 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S174:** Fonte oficial (endereço omitido; mantido no registro privado de evidências). Cooperative security notice; incident identified 1 June 2026. Verificado em 2026-11-22.

**S175:** Fonte oficial (endereço omitido; mantido no registro privado de evidências). Judicial-deposit platform continuity notices, September 2026. Verificado em 2026-11-22.

**S177:** Fonte oficial do setor financeiro (endereço omitido; mantido no registro privado de evidências). Incident statement, updated 5 November 2026. Verificado em 2026-11-23.

**S178:** Fonte oficial (endereço omitido; mantido no registro privado de evidências). Shared publication and messaging systems notice, 21 September 2026. Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S179:** CNN Brasil. Court file-exposure reporting, 16 November 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S180:** Diário de Pernambuco. Operator-authored portal statement, 27 October 2026; reproduced by original recipient (endereço do artigo omitido). Verificado em 2026-11-22.

**S181:** Mobile Time. Hospital-authored patient-data statement, 8 October 2026; reproduced by original recipient (endereço do artigo omitido). Verificado em 2026-11-22.

**S182:** Fonte oficial (endereço omitido; mantido no registro privado de evidências). An examination-services provider; chronology and scope review. Verificado em 2026-11-22.

**S183:** Attributed public reporting. A financial-services provider; chronology and scope review (endereço do artigo omitido). Verificado em 2026-11-22.

**S184:** Attributed public reporting. A university; chronology and scope review (endereço do artigo omitido). Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S185:** Fonte oficial (endereço omitido; mantido no registro privado de evidências). A state-court electronic case-service platform; chronology and scope review. Verificado em 2026-11-22.

**S186:** Fonte oficial (endereço omitido; mantido no registro privado de evidências). State public-sector systems investigated for unauthorized access; chronology and scope review. Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S187:** Attributed public reporting. A public warning platform; chronology and scope review (endereço do artigo omitido). Verificado em 2026-11-22. Trecho oficial indexado lido; texto completo não revisado.

**S188:** Fonte oficial (endereço omitido; mantido no registro privado de evidências). A bank-workers union virtual voting platform; chronology and scope review. Verificado em 2026-11-22.

**S189:** Attributed public reporting. A fictitious banking-dispute example; chronology and scope review (endereço do artigo omitido). Verificado em 2026-11-22.

**S190:** Attributed public reporting. A utility; chronology and scope review (endereço do artigo omitido). Verificado em 2026-11-22.

**S191:** Attributed public reporting. A diagnostics group; chronology and scope review (endereço do artigo omitido). Verificado em 2026-11-22.

**S192:** Attributed public reporting. A healthcare operator; chronology and scope review (endereço do artigo omitido). Verificado em 2026-11-22.

**S193:** Fonte oficial (endereço omitido; mantido no registro privado de evidências). A logistics operator; chronology and scope review. Verificado em 2026-11-22.

**S194:** CNN Brasil / Estadão. Bank customer-notice excerpts, 18–19 November 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S195:** Viva. Delivery-platform company-notice account, 19 November 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S196:** Fonte oficial (endereço omitido; mantido no registro privado de evidências). Academic-data investigation notice, 17 November 2026. Verificado em 2026-11-22.

**S197:** BNews Alagoas. Public-portal possible-incident press note, 20 November 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S201:** Estadão / UOL. Banco do Nordeste temporary Pix suspension, 27 January 2026. Verificado em 2026-11-22.

**S226:** Agência Brasil. Caixa Seguridade incident reporting, 12 November 2026. Verificado em 2026-11-22.

**S227:** CNN Brasil. Treasury personal-data disclosure reporting, November 2026. Verificado em 2026-11-22.

**S228:** Folha de S.Paulo. Santos administrative-system recovery reporting, 16 November 2026. Verificado em 2026-11-22.

**S229:** Autoridade Portuária de Santos. Terminal consultation and recovery update, 17 November 2026. Verificado em 2026-11-22.

**S230:** Autoridade Portuária de Santos. Security contingency update, 19 November 2026. Verificado em 2026-11-22.

**S231:** Banco do Nordeste. First-half 2026 management report: January incident loss and recovery. Verificado em 2026-11-23. Trecho oficial indexado lido; texto completo não revisado.

**S232:** Cybernews original investigation. Multicountry point-of-sale malware investigation; August 2026 discovery. Verificado em 2026-11-23.

**S233:** Prefeitura de Belo Horizonte. Payment-guide incident statement, updated 19 November 2026. Verificado em 2026-11-23.

**S234:** Diário do Comércio. Belo Horizonte incident reporting, 16 November 2026. Verificado em 2026-11-22.

**S266:** BNews RN. Unimed Natal care continuity and system recovery reporting, 19 November 2026. Verificado em 2026-11-22.

**S268:** SES-MT / Secom Mato Grosso. SES trabalha para restabelecer sistemas após novo ataque hacker, 2 November 2026. Verificado em 2026-11-22.

**S269:** CNN Brasil. Secretaria de Saúde de MT é alvo de ataque; sistemas suspensos, 3 November 2026. Verificado em 2026-11-22.

**S270:** Registro do Dia. Cuiabá extends licensing deadlines after shared SES incident, 10 November 2026. Verificado em 2026-11-22.

**S300:** BTG Pactual. Issuer-authored letter to CVM, 24 March 2026; third-party-hosted copy. Verificado em 2026-11-22.

**S301:** TI Inside. BTG Pactual temporary Pix suspension, 22 March 2026. Verificado em 2026-11-22.

**S302:** Hospital Sírio-Libanês. Official information-security incident questions and answers. Verificado em 2026-11-22.

**S303:** UOL. Sírio-Libanês report-system investigation, 16 October 2026. Verificado em 2026-11-22.

**S304:** Elastic Security Labs. KREMLIN browser-extension and banking-session research, 14 September 2026. Verificado em 2026-11-22.

**S305:** ANY.RUN. PhantomEnigma investigation, 16 July 2026. Verificado em 2026-11-22.

**S306:** Supremo Tribunal Federal. Press note on a tax-record access investigation, 17 February 2026 (endereço do artigo omitido). Verificado em 2026-11-23.

**S307:** Fonte oficial (endereço omitido; mantido no registro privado de evidências). Court statement on document-borne AI instructions, 20 May 2026. Verificado em 2026-11-22.

**S308:** Fonte oficial (endereço omitido; mantido no registro privado de evidências). Preventive service restrictions, 22 October 2026. Verificado em 2026-11-22.

**S309:** CNN Brasil. Education website attack-attempt reporting, 15 November 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S310:** UOL. Financial-service security incident reporting, 21 April 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S311:** Baguete. Retail financial-services restrictions, 27 July 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S313:** Socket. Malicious banking SDK and certificate theft research, 28 May 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S314:** Cemig. Material fact: personal-data exposure, 14 May 2026. Verificado em 2026-11-23.

**S315:** Diário do Comércio. Cemig personal-data incident reporting, 15 May 2026. Verificado em 2026-11-22.

**S316:** CTIR Gov / GSI. Provider-data and source-code exposure warning, 21 May 2026. Verificado em 2026-11-22.

**S317:** CTIR Gov / GSI. Provider-system technical recommendation, 22 May 2026. Verificado em 2026-11-22.

**S318:** CTIR Gov / GSI. Cloud-resource abuse and cryptojacking warning, 24 June 2026. Verificado em 2026-11-22.

**S319:** CTIR Gov / GSI. Website alteration and framework security warning, 14 August 2026. Verificado em 2026-11-22.

**S320:** CTIR Gov / GSI. Content-management security guidance; updated 10 November 2026. Verificado em 2026-11-22.

**S321:** CTIR Gov / GSI. Mail-client security guidance; updated 16 November 2026. Verificado em 2026-11-22.

**S322:** CTIR Gov / GSI. Web-server security guidance; updated 19 November 2026. Verificado em 2026-11-22.

**S323:** Folha de S.Paulo. Public-safety platform data-disclosure investigation reporting, 13 November 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S324:** Banco Central do Brasil. Financial Stability Report, October 2026, section2.5, pages79–84. Verificado em 2026-11-22.

**S325:** Folha C-Level. Independent bank customer-notice coverage, 19 November 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S326:** Canaltech. Delivery-platform population-specific notice coverage, 19 November 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S327:** Itatiaia. University academic-data inquiry and separate hardware outage, 21 November 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

**S328:** Jornal Extra Alagoas. Public-portal official press-note reproduction, 20 November 2026 (endereço do artigo omitido). Verificado em 2026-11-22.

# Apêndice D. Glossário

| Termo | Significado simples |
|---|---|
| Decisão sobre a conta | Registro que classifica uma conta como ativa, contida, corrigida, histórica ou não pertencente à organização |
| Comunicação às pessoas afetadas | Informação sobre incidente de dados pessoais e medidas de proteção pertinentes |
| Modelo analítico | Relação de planejamento fundamentada que não é conexão operacional comprovada |
| Autenticação | Verificação de que pessoa, dispositivo ou serviço é a identidade declarada |
| Autorização | Permissão para a identidade realizar determinada ação |
| Banking as a service | Funções financeiras fornecidas por serviço e permissões de outra organização |
| Validação de beneficiário | Verificação de que o destino é o recebedor pretendido e autorizado |
| Extensão de navegador | Software adicionado ao navegador que pode acessar navegação ou atividade de contas |
| Revogação de certificado | Encerramento da confiança em certificado antes do vencimento normal |
| Alegação | Afirmação de fonte cujo acesso, posse ou impacto não está estabelecido independentemente |
| Controlador | Entidade responsável pelas decisões de tratamento conforme a lei aplicável |
| CPF | Identificador individual brasileiro; conhecê-lo não estabelece permissão de uso da conta |
| CNPJ | Cadastro e identificador brasileiro de empresas, associações e outras pessoas jurídicas [S30] |
| Credencial | Informação ou material usado para autenticar uma identidade |
| Categoria de dados | Tipo de informação, como contato, finanças ou autenticação |
| Associação de dispositivo | Observação que conecta dispositivo e domínio; titularidade e situação atual exigem validação |
| Data de divulgação | Quando o evento se tornou público, possivelmente depois de ocorrido |
| Carregamento de DLL | Programa Windows carrega componente compartilhado; sua origem importa |

| Termo | Significado simples |
|---|---|
| DDoS | Negação de serviço distribuída, voltada a impedir uso legítimo por tráfego ou esgotamento de recursos |
| DMARC | Padrão de política e relatórios de domínio de e-mail baseado em autenticação de remetente |
| Extorsão | Cobrança acompanhada de ameaça, como divulgação de dados; não exige criptografia |
| Ciência do incidente | Momento relevante em que a entidade responsável conhece os fatos do incidente |
| KYC | Informações ou verificações de identidade conhecidas como conheça seu cliente |
| Listagem | Entrada pública que alega vítima ou oferece material; sem confirmação independente de incidente |
| MFA | Autenticação multifator, com mais de um tipo de evidência de identidade |
| TLS mútuo | Autenticação por certificados em que os dois lados da conexão se autenticam |
| NFSe | Registro de nota de serviço usado em processos fiscais municipais |
| Operador | Entidade que trata dados em nome do controlador no marco aplicável |
| Chave Pix | Identificador para localizar recebedor; não autoriza uma transferência sozinho |
| Privilégio | Permissão ou nível de autorização de uma conta ou serviço |
| Ransomware | Malware ligado à negação coercitiva de acesso, geralmente por criptografia |
| Conciliação | Verificação de concordância entre registros e transações após interrupção ou processo manual |
| Sessão | Interação autenticada que pode continuar válida separadamente da senha inicial |
| Material de assinatura | Identidade digital usada para autorizar ou validar operação assinada |
| Engenharia social | Engano para induzir divulgação de informação ou ação insegura |
| Limite do fornecedor | Divisão de sistemas, dados e autorização entre organização e prestador |
| Token | Material digital que representa decisão de autenticação ou autorização |

| Termo | Significado simples |
| --- | --- |
| Canal alternativo confiável | Caminho prévio para verificar mensagens ou manter serviço quando o principal não é confiável |
| Não verificado | Não estabelecido independentemente neste relatório; não significa fabricado |

O glossário explica termos da análise. Definições regulatórias preservam o escopo dos instrumentos, especialmente controlador, operador e decisões de comunicação. [S10][S11][S12]

ABOUT BRANDEFENSE

# Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS

**4.7** / 5

COVERAGE

**3** pillars

CTI, DRPS, EASM

MONITORING

**24** / 7

Open, deep and dark web

REQUEST A DEMO

## Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

# Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.




### Top InfoSec Innovator

2026




### Deloitte Technology Fast 500 EMEA

2024




### Global InfoSec Awards

2025




### Cybersecurity Excellence Awards

2025

## See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

# See what attackers see. Before they act.


UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO