Relatório Semestral ISH de Cibersegurança

O cenário por trás dos dados

SUMÁRIO

Introdução

O primeiro semestre de 2025 evidenciou o avanço do cibercrime em escala, sofisticação e precisão. Ataques estão mais direcionados, exploram vulnerabilidades conhecidas e afetam setores cada vez mais estratégicos. **Esse cenário exige uma postura diferente: proativa, coordenada e orientada por risco real.**

Neste e-book, você encontra uma análise aprofundada dos dados coletados pelas operações Heimdall CTI e SOC da ISH ao longo do primeiro semestre de 2025, com insights sobre grupos de ransomware em alta, setores mais visados, vulnerabilidades exploradas e falhas que ainda ampliam a exposição das empresas.

Mais do que números, este e-book propõe uma **leitura estratégica dos desafios atuais** e do que precisa ser feito — agora — para enfrentá-los com maturidade e inteligência.

1. Panorama global de vulnerabilidades e riscos emergentes

A análise das vulnerabilidades exploradas no primeiro semestre de 2025 revela uma realidade preocupante: ataques direcionados a falhas conhecidas e já divulgadas continuam entre **os vetores mais eficazes dos agentes de ameaça.**

Volume de vulnerabilidades

Entre janeiro e junho de 2025, a equipe de Inteligência de Ameaças da ISH Tecnologia, conhecida como Heimdall, identificou **mais de 20 mil vulnerabilidades** em uma ampla gama de produtos e serviços.

Esse cenário evidencia não apenas a crescente sofisticação das ameaças cibernéticas, mas também **o ritmo acelerado com que novas fragilidades estão sendo descobertas** em softwares amplamente utilizados no mercado.

Gravidade das vulnerabilidades identificadas

A classificação de severidade das vulnerabilidades detectadas entre janeiro e junho de 2025 mostra que **mais de 10 mil falhas foram consideradas de alto ou crítico impacto**, segundo a escala CVSS. Esse número representa **mais da metade do total observado no período** — o que reforça o volume expressivo de brechas com alto potencial de exploração.

GRAVIDADE	VULNERABILIDADES
Baixo (0.0 a 3.9)	708
Médio (4.0 a 6.9)	9.829
Alto (7.0 a 8.9)	7.448
Crítico (9.0 a 10.0)	2.873

Tabela 1 – Vulnerabilidades publicadas no período da pesquisa de acordo com a gravidade.

Embora vulnerabilidades críticas mereçam atenção imediata, os dados mostram que o **maior volume se concentra em falhas médias**, que muitas vezes passam despercebidas — mas podem ser exploradas em cadeia, com impactos significativos quando combinadas a outros vetores de ataque.

Tendência mensal de publicação (2025)

MÊS	2024	2025
Janeiro	2647	3904
Fevereiro	2906	3060
Março	3352	3344
Abril	3735	3580
Maio	5103	3251
Junho	3173	2982
Total	20.916	20.121

Tabela 1 – Vulnerabilidades publicadas no período da pesquisa de acordo com a gravidade.

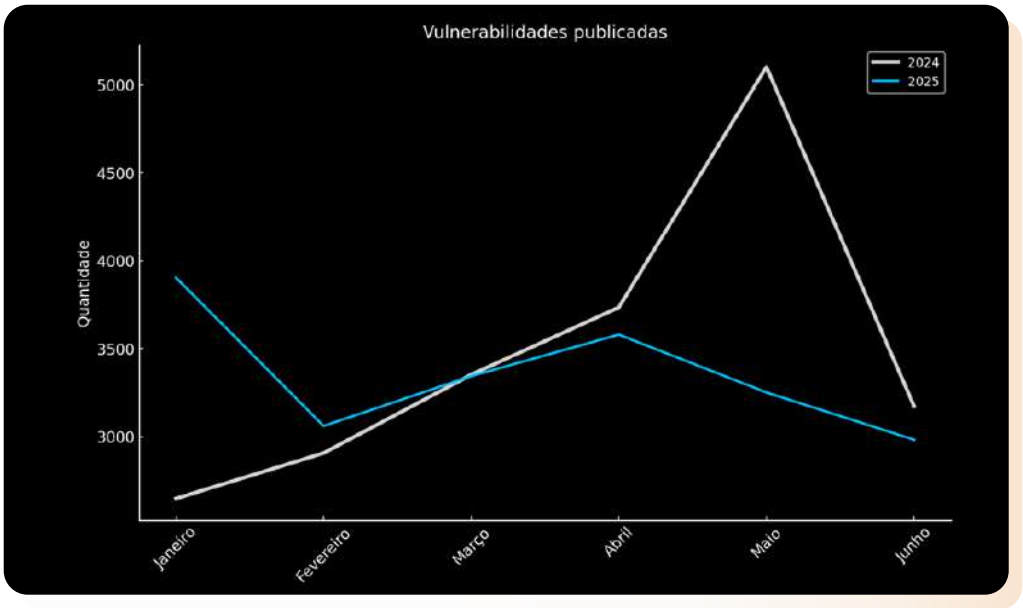


Gráfico 1 – Gráfico relacionado a dados e números de vulnerabilidades divulgadas mensalmente.

Janeiro foi o mês com o maior número de vulnerabilidades, com aumento de 47,5% em relação ao mesmo mês de 2024. Já o mês com menor variação foi **março**, com queda leve de 0,24% em relação ao ano anterior.

2. Vulnerabilidades exploradas no semestre

A exploração ativa de vulnerabilidades por agentes de ameaça ao longo do primeiro semestre de 2025 reforça um ponto crítico: **sem prevenção, não há defesa que sustente o impacto.**

Os dados mostram que falhas conhecidas - muitas já documentadas e corrigidas - continuam sendo exploradas com sucesso por grupos de cibercriminosos. Isso evidencia a urgência de manter **programas contínuos de gestão de vulnerabilidades,** aliados a processos de **detecção e resposta em tempo real.**

O Heimdall CTI mapeou as principais vulnerabilidades exploradas em 2025:

CVE-2025-31324

• Permite execução remota de código não autenticada no SAP NetWeaver Visual Composer, via upload de arquivos ao endpoint, com invasores implantando **web shells** e obtendo controle total do sistema.

• Grupos: BianLian, RansomEXX e RRA (Storm2460), frequentemente vinculados a campanhas de ransomware e espionagem.

CVE-2025-22457

• Vulnerabilidade de buffer overflow (CVSS 9.0) no Ivanti Connect Secure VPN.

• Implantação de malwares como **TRAILBLAZE, BUSHFIRE** e componentes do ecossistema SPAWN.

• Grupo: UNC5221, ligado à espionagem baseada na China.

CVE-2025-3248

• Falha de **execução remota de código (RCE)** em Langflow (<1.3.0)

• Instalação da botnet Flodrix para DDoS e exfiltração.

CVE-2025-30066

• Comprometimento na **supply chain** do GitHub Action tj actions/changed files (v≤45.0.7).

• Vazamento de segredos e credenciais de CI/CD.

CVE-2025-33053

• Controle externo de nome/caminho de arquivo em arquivos de atalho da **Internet (WebDAV)** no Windows.

• Permite que um atacante execute código remoto via malwares distribuídos por WebDAV.

CVE-2025-32756

• Buffer overflow crítico (CVSS 9.6) explorado em FortiVoice e FortiMail.

• Permite execução remota de código sem autenticação.

Outras vulnerabilidades exploradas

Nesta seção, reunimos outras vulnerabilidades identificadas, os atores de ameaça que as exploram e um panorama de suas motivações e estratégias, oferecendo uma visão clara sobre seu modo de atuação. Confira:

CVE-2025-42999

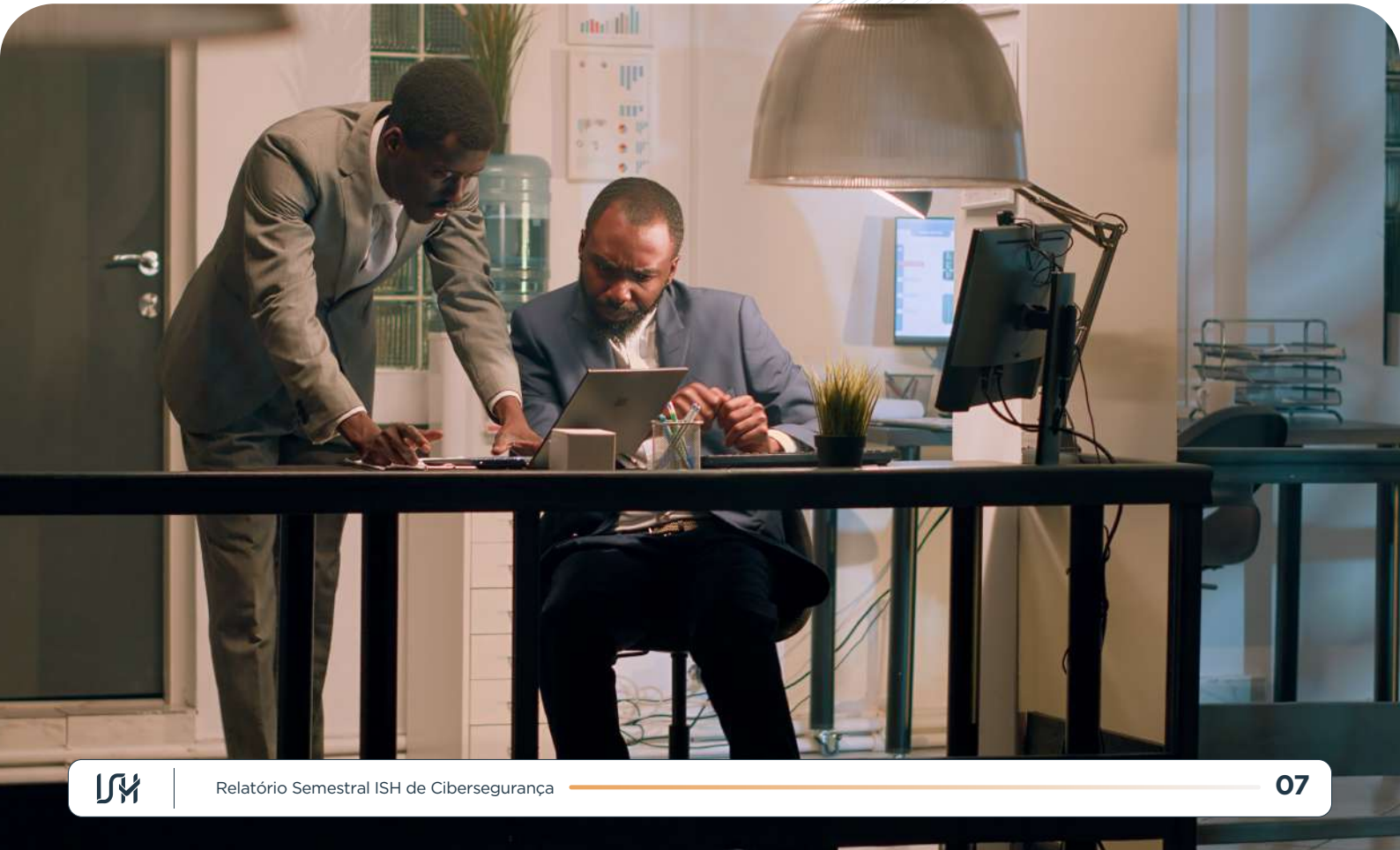
• Falha crítica de **desserialização** no Visual Composer da SAP, associada à CVE-2025-31324.

CVE-2025-22224

• Vulnerabilidade de **race condition (TOCTOU)** no **VMware ESXi e Workstation,** resultando em escrita fora de limites e execução de código no host, a partir de uma VM comprometida.

CVE-2025-0411

• Vulnerabilidade no **7-Zip** por bypass do **Mark-of-the-Web (MOTW)**, usada para ocultar a origem de arquivos extraídos.



3. Top 05 vulnerabilidades do mês de julho

As vulnerabilidades mais críticas identificadas em julho de 2025 envolvem **execução remota de código, falsificação de identidade e vazamento de credenciais** — muitas vezes com **baixa complexidade de exploração e alto potencial de impacto operacional.**

A seguir, veja um panorama técnico das 5 falhas que exigem **atenção imediata das equipes de segurança:**

1

CVE-2025-53770
Microsoft SharePoint Server

Vulnerabilidade crítica no Microsoft SharePoint Server que permite execução remota de código (RCE) por meio de desserialização insegura de dados, explorável via payloads manipulados autenticados.

2

CVE-2025-53771
Microsoft SharePoint Server

Vulnerabilidade de falsificação (spoofing) no Microsoft SharePoint Server. Um invasor autenticado pode explorar essa falha para falsificar solicitações em nome de outro usuário, enganando o sistema de forma que aceite informações manipuladas.

3

CVE-2025-47812
Wing FTP Server

Falha grave no Wing FTP Server que permite upload arbitrário de arquivos maliciosos, explorável via endpoint, permitindo execução remota não autenticada com simples requisição HTTP.

4

CVE-2025-5777
CitrixBleed 2

Nova variante da vulnerabilidade "CitrixBleed", afetando NetScaler ADC/Gateway, explorável via buffer leak não autenticado, permitindo exfiltração de tokens de sessão e posterior RCE com escalonamento.

5

CVE-2025-47981
Windows SPNEGO / NEGOEX

Vulnerabilidade em componente SPNEGO (NEGOEX) do Windows que permite RCE com privilégio SYSTEM, via exploração de cadeia no protocolo de autenticação Kerberos.

4. Ransomware em números: o balanço do 1º semestre

Ataques de ransomware continuam sendo uma das principais ameaças cibernéticas no mundo. Entre janeiro e junho de 2025, **3.617 empresas** foram anunciadas publicamente como vítimas — um aumento de **25,7% em relação ao mesmo período de 2024.**

A maioria dessas ofensivas foi conduzida por grupos com estruturas bem definidas, táticas de dupla extorsão e foco em setores estratégicos.

MÊS	2023	2024	2025
Janeiro	147	292	509
Fevereiro	221	407	943
Março	437	424	643
Abril	480	738	491
Maio	396	595	556
Junho	400	421	475
Total	2.081	2.877	3.617

Total de empresas anunciadas durante os anos de 2023, 2024 e 2025.

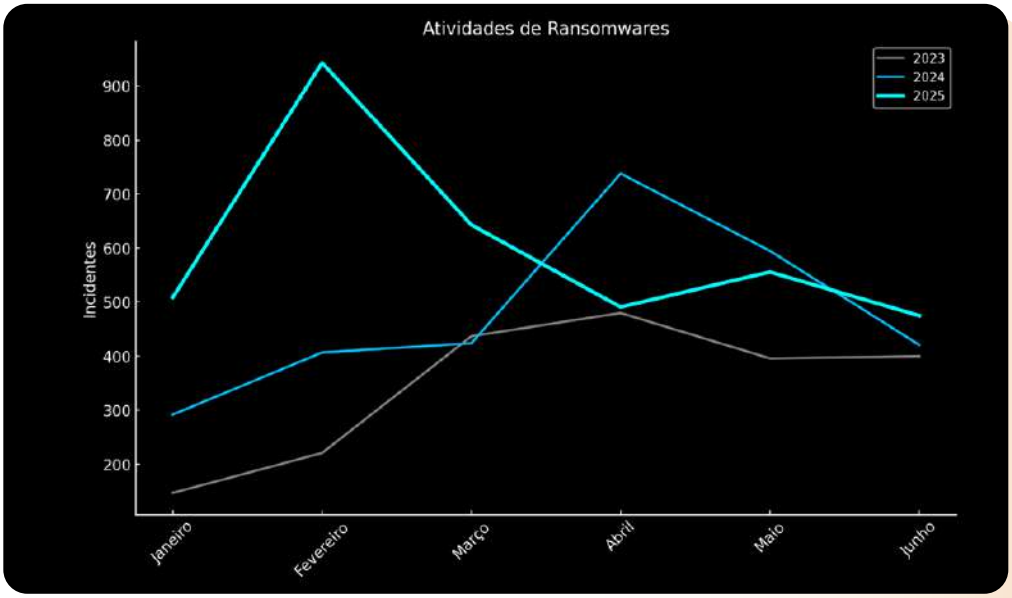


Gráfico relacionado a principais atividades de grupos de ransomware em comparação mês a mês dos anos de 2023, 2024 e 2025.

O comparativo revela uma tendência clara de crescimento, com destaque para o primeiro trimestre de 2025, que concentrou os maiores picos.

O comportamento sazonal ainda se repete — com aumentos em fevereiro e março —, mas os números absolutos têm crescido significativamente ano após ano. Essa escalada reflete a **sofisticação crescente das ameaças, a profissionalização das quadrilhas e a urgência de medidas preventivas contínuas.**

5. Protagonistas: grupos de ransomware mais ativos em 2025

No primeiro semestre de 2025, o cenário de ransomware foi liderado por grupos altamente organizados, com operações globais e capacidade de impactar centenas de empresas em poucos dias.

Abaixo, você confere **os 10 principais agentes por volume de vítimas** — um retrato da escala e agressividade das ameaças que desafiaram empresas dos mais diversos setores:

GRUPO	VÍTIMAS
Clop	403
Akira	357
Qilin	351
Ransomhub	233
Play	231
Safepay	204
Lynx	174
Incransom	152
Medusa	105
FOG	91
Outros	1519

Estatísticas de grupos de ransomware em 2025.

Em 2025, os grupos **Clop, Akira** e **Qilin** lideraram as ofensivas de ransomware, acumulando, juntos, mais de mil vítimas apenas no primeiro semestre. O destaque vai para o Clop, que se manteve como o grupo mais ativo, com **403 ataques registrados.** Grupos em ascensão, como **Ransomhub, Play** e **Safepay**, também demonstraram forte atuação, ampliando seu alcance global.

Somados, os dez grupos mais atuantes foram responsáveis por **2.830 ataques**, enquanto os demais — classificados como "Outros" — totalizaram **1.519 ocorrências**, evidenciando a pulverização e o dinamismo do ecossistema de ameaças.

Setores na mira: os alvos mais visados do ransomware

Grupos de ransomware têm concentrado seus esforços em setores de Tecnologia, Manufatura e Serviços Empresariais, que são considerados críticos. Juntos, eles somaram **mais de 1.200 ataques apenas no primeiro semestre.**

SEGMENTO	ATAQUES
Tecnologia	501
Manufatura	492
Business Services	273
Healthcare	272
Serviços financeiros	200
Serviços ao consumidor	199
Transporte/ Logística	187
Setor Público	171
Educação	166
Construção	156

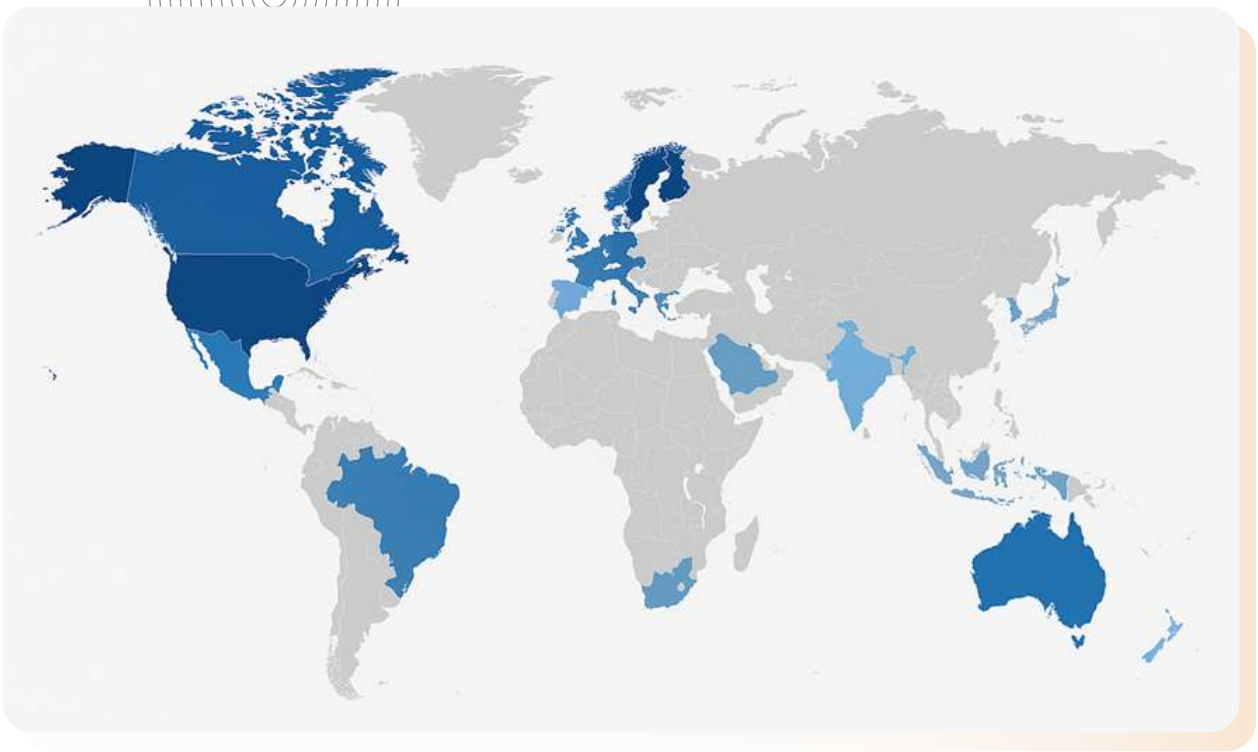
Ataques de ransomware identificados por segmentos em 2025.

Saúde e Serviços Financeiros também estão entre os segmentos mais visados, refletindo a busca por **alvos com alta dependência digital e baixa tolerância a interrupções** — fatores que aumentam significativamente o potencial de impacto e a pressão por pagamento.

Alvos no mapa: distribuição global de ransomware em 2025

A análise por país mostra que os grupos de ransomware continuam concentrando suas ações nos grandes centros econômicos. **Os Estados Unidos seguem liderando o ranking de vítimas**, com um volume de ataques muito superior ao de qualquer outro país. Em seguida, **Canadá, Reino Unido e Alemanha** também registram altos índices de incidentes.

PAÍS	ATAQUES
EUA	1.785
Canadá	227
Reino Unido	164
Alemanha	160
Itália	92
França	79
Brasil	74
Espanha	70
Australia	68
Índia	52



Indicadores relacionados a atividades de ransomware por país.

Insights ISH

O Brasil aparece entre os 10 países mais atacados, com dezenas de empresas impactadas — um indicativo claro de que a **América Latina está cada vez mais no radar dos cibercriminosos**. Esse cenário reforça a necessidade de estratégias de defesa mais robustas, baseadas em **visibilidade contínua, detecção em tempo real e respostas rápidas a qualquer sinal de comprometimento.**

PASSWORD
123456
qwerty123
qwerty1
123456789
12345678
12345
102030
admin
Brasil
Qwerty123

6. Senhas fracas ainda são um convite para o cibercrime

Mesmo com o avanço das ameaças e o aumento da conscientização sobre segurança digital, **o uso de senhas fracas continua sendo uma das brechas mais comuns — e perigosas — nas empresas brasileiras.**

As 10 senhas mais encontradas em bases de vazamentos no Brasil, em 2025, mostram um padrão preocupante de repetição e simplicidade.

Além dessas, combinações como **consulta123, secret** e **password** também aparecem com frequência, reforçando a urgência de políticas mais rigorosas de autenticação.

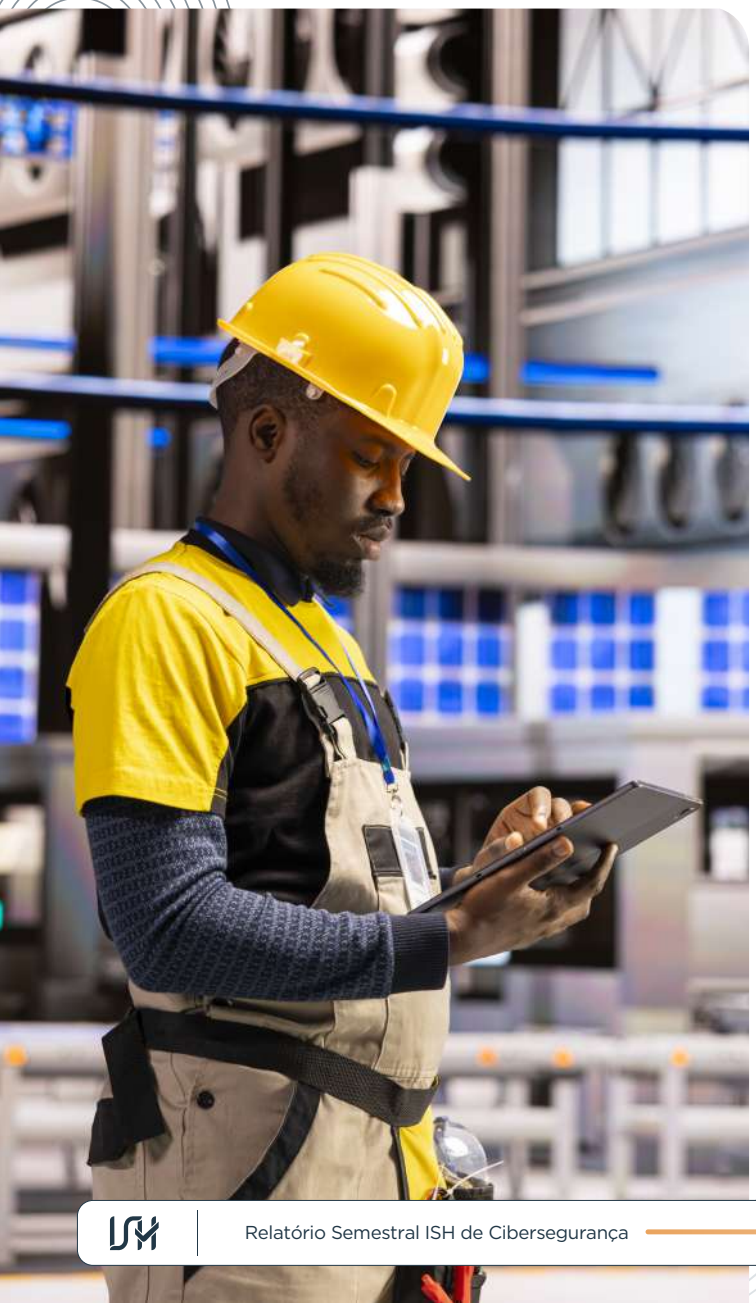
Insights ISH

Senhas simples são facilmente quebradas por ferramentas automatizadas de força bruta e dicionário. Em poucos segundos, um atacante pode obter **acesso total a sistemas sensíveis** e iniciar movimentações laterais dentro da rede.

Recomendações básicas de segurança:

- Ativar autenticação multifator (MFA)
- Forçar complexidade mínima de senha
- Aplicar expiração periódica
- Utilizar cofres de senha e ferramentas de IAM

Proteção de verdade começa pelo básico. **Senhas fortes** ainda são a primeira **linha de defesa.**



7. Onde o risco é constante: o que a detecção ativa revela

Violações registradas por setor

Embora grupos de ransomware tenham setores preferenciais para suas ofensivas, o cenário das **violações de segurança** revela uma dinâmica diferente.

A equipe de SOC da ISH mapeou os segmentos com maior volume de violações no segundo trimestre de 2025, oferecendo uma visão complementar à dos ataques efetivamente consumados.

VIOLAÇÕES POR SETOR

Finanças e Seguros	29.279	22,35%
Serviços	20.558	15,70%
Indústria	15.131	11,55%
Governo	11.536	8,81%
Agricultura	8.627	6,59%
Energia	6.614	5,05%
Saúde	6.170	4,71%
Comércio	5.452	4,16%
Logística	4.089	3,12%
Educação	4.076	3,11%
Alimentação	3.425	2,61%
Tecnologia	2.739	2,09%
Saneamento	2.113	1,61%

Insights ISH

Uma violação de segurança não representa, necessariamente, um incidente ou ataque confirmado. Ela diz respeito **à tentativa de infiltração e exfiltração de dados**, muitas vezes detectada e contida antes de causar impacto direto.

Entre abril e junho de 2025, a operação do SOC da ISH registrou:

• Volume significativo de **tickets (ocorrências) de severidade crítica.**

• Alta incidência nos segmentos de **finanças, serviços e indústria.**

• Comportamentos que incluem **execução remota, exploração de vulnerabilidades conhecidas e acessos não autorizados.**

O aumento no número de ocorrências reforça a eficiência de soluções como o Vision MDR e Vision MEDR na contenção de ameaças.

8. Quando a segurança vira prioridade, o impacto muda

Não é a falta de ferramentas que compromete a segurança das organizações. É a ausência de visibilidade, coordenação e prioridade.

Os dados reunidos neste relatório mostram que o cenário de ameaças evolui rapidamente, mas os pontos de fragilidade seguem os mesmos: senhas fracas, vulnerabilidades não corrigidas, ambientes mal monitorados e respostas tardias. É justamente aí que os agentes de ameaça encontram espaço.

Fortalecer a segurança cibernética começa com o reconhecimento de que ataques não acontecem apenas com “as outras empresas”. Eles ocorrem **todos os dias,** e só não geram impacto **quando são antecipados ou neutralizados a tempo.**

A maturidade digital está em levar a sério cada sinal de risco. E empresas que fazem isso antes da crise conseguem **agir com inteligência, proteger sua reputação e garantir a continuidade do negócio.**

Na era digital, a segurança não é apenas uma necessidade — é o que define a continuidade e o crescimento do seu negócio.

A **ISH** está na linha de frente da cibersegurança, unindo inovação, inteligência e confiança para proteger empresas de todos os portes e setores.

Fale com nosso time de consultores e descubra como implementar uma estratégia de segurança personalizada, eficaz e alinhada aos desafios do seu mercado.