SEK Security Ecosystem Knowledge

THINK AHEAD REPORT 2025

ÍNDICE

Sobre a SEK 3

Introdução 4

O que aconteceu no ano de 2024? 10

As ameaças cibernéticas de 2025 27

- A nova era dos ataques com IA 28
- Guerra de influência movida por IA 29
- Ransomware 3.0 31
- Infostealers 2.0 34
- Exploração de dispositivos de borda e ORBs 36

As tecnologias de cibersegurança em 2025 38

- Preparação para a era pós-quântica 39
- Os riscos da inação 40
- Cloud Security First 42
- Plataformização da cibersegurança 45
- Machine Identity 49
- AI-driven Cybersecurity 52
- Governança de IA 55
- O fim da segurança por obscuridade em OT 58
- O futuro do hardware de IA 61
- Regulamentação e geopolítica 63

Estratégias práticas e recomendações 68

- Melhores práticas para CISOs gerirem riscos e defenderem seus orçamentos 69
- Como diferentes setores podem se preparar para os desafios? 74

Conclusão 80

Referências 82

SOBRE A SEK

Liderando um futuro digital resiliente

A transformação digital traz inovação e desafios complexos. Há mais de 20 anos, a SEK se posiciona como um ***trusted advisor*** em cibersegurança ao combinar tecnologia, expertise humana e inteligência estratégica para antecipar ameaças e proteger negócios. Unimos ***expertise local e* alcance global** para oferecer segurança inteligente e adaptável.

Segurança integrada para um mundo conectado

A cibersegurança exige uma abordagem estruturada que conecte proteção, eficiência e evolução. Nossa metodologia ***Resilience Acceleration Program (RAP)*** acelera a maturidade cibernética por meio de três pilares.

Diagnóstico e planejamento estratégico (advise)
Identificamos riscos e desenvolvemos um plano alinhado ao negócio.

Execução e integração de controles (implement)
Implementamos estratégias e controles de defesa eficazes.

Monitoramento contínuo (manage)
Ajustamos continuamente as estratégias para garantir resiliência e segurança.

Nosso portfólio

Para fortalecer a resiliência cibernética, a SEK oferece um portfólio completo de serviços e soluções que abrangem desde a estratégia até a execução e monitoramento contínuo.

- Strategy & Risk
- Exposure Management
- Tecnologias e soluções
- Managed Detection & Response e SOC-as-a-Service

Construindo o futuro da cibersegurança

Mais do que tecnologia, segurança digital é vantagem estratégica. Além de proteger organizações, a SEK impulsiona seu crescimento seguro e sustentável. Com um olhar voltado para o futuro, investimos em pesquisa, inovação e parcerias para antecipar tendências e transformar desafios em oportunidades.

Como trusted advisor, estamos ao lado de nossos clientes, construindo um mundo mais seguro, resiliente e preparado para o amanhã.

SEK Security Ecosystem Knowledge

Introdução

A história da humanidade é marcada por revoluções que redefiniram os limites do possível. A descoberta do fogo, a invenção da escrita, a Revolução Industrial — cada uma dessas transformações trouxe consigo novas formas de poder, riscos e oportunidades. Hoje, vivemos outra dessas encruzilhadas, impulsionada por algoritmos que aprendem, computadores que decifram códigos e redes neurais capazes de imitar a cognição humana. Cada vez mais, a cibersegurança deixa de ser um campo técnico restrito a especialistas para se tornar uma questão central da sobrevivência organizacional, da estabilidade geopolítica e da própria noção de confiança em um mundo cada vez mais hiperconectado.

A inteligência artificial, outrora confinada a laboratórios e cenários hipotéticos, agora alimenta tanto a defesa quanto o ataque cibernético. Criminosos usam *deepfakes* tão convincentes que desafiam a percepção da realidade; sistemas autônomos de *ransomware* exploram vulnerabilidades em segundos (não mais em dias); e a computação quântica ameaça desmantelar a criptografia que protege tudo, desde transações bancárias até segredos de Estado. Enquanto isso, bilhões de dispositivos de borda — de sensores industriais a assistentes virtuais — ampliam a superfície de ataque, transformando objetos cotidianos em portas de entrada para invasões catastróficas. **Neste cenário, a pergunta não é se uma organização será alvo, mas quando e como resistirá ao impacto.**

Este relatório não é um simples catálogo de ameaças. É um mapa para navegar um território onde a única constante é a **mudança acelerada**. Nas páginas seguintes, exploraremos como a convergência de tecnologias disruptivas, a evolução do crime cibernético e as tensões geopolíticas estão reescrevendo as regras da segurança digital. Mas, antes de mergulhar nas tendências específicas, é essencial compreender as forças maiores que moldam este novo mundo — e por que 2025 será um ano decisivo para aqueles que desejam não apenas sobreviver, mas **prosperar.**

Inteligência Artificial

Oportunidades e desafios

A IA é a metáfora perfeita para nossa era, e uma tecnologia que espelha tanto o melhor quanto o pior da humanidade. Em 2025, sistemas baseados em aprendizado de máquina serão responsáveis por **detectar 85% das ameaças cibernéticas em tempo real**, segundo projeções do Google Cloud. Ao mesmo tempo, esses mesmos algoritmos alimentarão **ataques de *phishing* tão personalizados** que até os colaboradores mais cautelosos poderão ser enganados.

Considere o caso dos ***deepfakes***. No ano passado, em Hong Kong, um funcionário de uma empresa transferiu US$ 25 milhões para criminosos após uma videoconferência falsa com diversos participantes. Em 2025, tais golpes continuarão evoluindo e criminosos não medirão esforços para conseguirem o que querem.

Alguns dos objetivos escusos incluem manipular eleições, fraudar mercados financeiros e minar a credibilidade de instituições. A ironia é cruel: a mesma tecnologia que permite diagnósticos médicos revolucionários também ameaça corroer a confiança na verdade factual.

Para empresas, isso significa que a segurança não pode mais depender apenas de firewalls ou senhas complexas. A batalha ocorrerá em um nível mais profundo: na capacidade de distinguir o real do artificial, o humano do algorítmico. Soluções como as de **Identidade Digital** da SEK, que usam IA para detectar e bloquear ameaças em tempo real garantem que apenas usuários legítimos acessem sistemas. Plataformas de autenticação multifator resistentes a deepfakes, sistemas de detecção de anomalias baseados em IA e treinamentos contínuos de conscientização serão essenciais. Mas mesmo essas medidas são insuficientes se não forem acompanhadas por uma reflexão ética mais ampla: **como garantir que a IA seja uma aliada, e não uma adversária, na defesa do espaço digital?**

Computação quântica

O fim da criptografia (como a conhecemos)

Enquanto a IA redefine o presente, a computação quântica remodela o futuro. Em 2025, os primeiros computadores quânticos práticos começarão a **desafiar a criptografia assimétrica** — o alicerce que protege comunicações sigilosas, transações financeiras e dados sensíveis. O risco não está no que esses computadores farão, mas no que já estão fazendo: criminosos e Estados-nação acumulam dados criptografados hoje, sabendo que poderão decifrá-los amanhã. É a era do "*Harvest Now, Decrypt Later*" — **uma ameaça silenciosa, mas existencial**.

Setores inteiros estão em risco. Bancos que dependem do RSA para proteger transações, governos que armazenam segredos de defesa em nuvens "seguras", e até mesmo hospitais que guardam registros médicos sob criptografia — todos enfrentarão um dilema: migrar para algoritmos pós-quânticos ou arriscar expor dados que hoje parecem invioláveis. O *National Institute of Standards and Technology (NIST)* já definiu padrões para essa transição, **mas apenas 30% das empresas iniciaram a jornada**. A procrastinação é um convite ao desastre.

O paradoxo da conectividade

Quando a inovação se torna vulnerabilidade

A Internet das Coisas (IoT) prometeu um mundo de conveniência: geladeiras que pedem comida, carros que evitam acidentes, fábricas que se autoajustam etc. Em 2025, essa promessa colidirá com uma realidade incontornável: cada dispositivo conectado é um potencial cavalo de Troia. Ataques a roteadores, firewalls e até sistemas SCADA industriais já não exigem hackers de elite — ferramentas open source e tutoriais na *dark web* democratizaram o crime cibernético.

O caso do aeroporto de Seattle é emblemático. Dias antes do feriado de *Labor Day*, um ataque de ransomware paralisou sistemas de check-in, deixando milhares de passageiros presos.

Em 2025, incidentes como esse se multiplicarão, atingindo desde usinas de energia até redes de transporte público. A lição é clara: com tudo tão conectado, a segurança só é tão forte quanto seu elo mais fraco.

Para organizações, isso exigirá uma mudança de mentalidade. A segurança não pode ser um *afterthought* — mas deve ser integrada ao DNA de cada produto, serviço e processo. Modelos de *Zero Trust*, segmentação de redes e monitoramento contínuo de dispositivos de borda não são mais opcionais: são requisitos para a sobrevivência.

Geopolítica no ciberespaço

A nova Guerra Fria

Se o século XX foi marcado pela corrida armamentista nuclear, o XXI será definido pela batalha por supremacia digital. Em 2025, ataques cibernéticos patrocinados por Estados se tornarão armas estratégicas, visando não apenas infraestruturas críticas, mas a própria percepção pública da realidade. Grupos como o *Volt Typhoon*, vinculado à China, já se infiltraram em redes de energia e comunicações nos EUA por anos sem serem detectados. Enquanto isso, a Rússia e a Coreia do Norte refinam **táticas de desinformação em escala global**, usando IA para criar narrativas falsas que polarizam eleitores e desestabilizam mercados.

Essa "guerra híbrida" não se limita a nações. Empresas multinacionais tornam-se alvos colaterais — ou protagonistas involuntárias — em conflitos entre potências. Sanções tecnológicas, como as restrições à exportação de *chips* avançados, forçam organizações a reavaliarem cadeias de suprimentos e parcerias.

Neste contexto, a cibersegurança transcende a proteção de dados — torna-se uma questão de **soberania e resiliência nacional**. Empresas que operam globalmente precisarão navegar não apenas firewalls técnicos, mas também barreiras políticas e culturais.

A ascensão do cibercrime-como-serviço

Democratizando a destruição

O cibercrime já não é um domínio de hackers solitários em porões escuros. É uma indústria globalizada, com modelos de negócios tão sofisticados quanto os de qualquer *startup* do Vale do Silício. Plataformas de ***Ransomware-as-a-Service (RaaS)*** permitem que criminosos sem habilidades técnicas lancem ataques devastadores por uma fração dos lucros. Mercados clandestinos na Rússia vendem logs de infostealers com credenciais de milhões de usuários, enquanto fóruns na *dark web* oferecem tutoriais passo a passo para explorar vulnerabilidades em sistemas OT.

Em 2025, essa economia paralela atingirá um novo nível de maturidade. Ataques de *ransomware* sem criptografia — nos quais criminosos apenas ameaçam vazar dados — dominarão o cenário, tornando backups tradicionais obsoletos. *Infostealers* 2.0, equipados com IA, roubarão credenciais não apenas de usuários finais, mas de sistemas corporativos inteiros, permitindo acesso persistente e invisível. O resultado é um ambiente onde até pequenas empresas podem sofrer ataques dignos de filmes de espionagem.

A lição aqui é dupla. Primeiro, a segurança precisa ser **tão ágil e inovadora quanto os criminosos**. Segundo, a colaboração entre setores — compartilhamento de inteligência de ameaças, parcerias público-privadas — não é mais um ideal, mas uma necessidade prática.

O AMANHÃ É AGORA.

As tendências descritas neste relatório não são especulações distantes. Elas já estão em movimento, moldadas por decisões tomadas — ou adiadas — no presente.

Em 2025, a resiliência será a nova moeda. Empresas precisarão, como nunca, adotar uma postura proativa, e não reativa. Isso significa investir em criptografia pós-quântica agora, treinar equipes para reconhecer *deepfakes* hoje, e construir redes segmentadas que limitem o impacto de invasões antes que ocorram. Significa, acima de tudo, entender que **a cibersegurança não é um custo, mas um investimento na sobrevivência e na confiança do mercado**.

A SEK, ao longo deste relatório, oferece não apenas diagnósticos, mas caminhos práticos. Das estratégias de zero trust à governança de IA, cada capítulo é um convite à ação. Porque em um mundo onde máquinas aprendem, códigos se autodestroem e a verdade pode ser fabricada, apenas os mais preparados escreverão o próximo capítulo da história digital.

O futuro chegou, e está nas mãos de quem ousar enfrentá-lo.

Tendências para 2025

AMEAÇAS

A nova era dos ataques com IA

Ataques cibernéticos impulsionados por inteligência artificial se tornarão mais sofisticados, explorando *deepfakes*, engenharia social automatizada e vulnerabilidades em tempo recorde.

Guerra de influência movida por IA

O uso de IA para desinformação e manipulação digital crescerá, impactando eleições, mercados financeiros e a credibilidade de empresas e instituições.

Ransomware 3.0: o fim da criptografia e a era da extorsão de dados

O *ransomware* evoluirá para um modelo baseado exclusivamente na exfiltração e chantagem de dados, tornando a prevenção e a resposta a incidentes ainda mais críticas.

Infostealers 2.0: a nova era do roubo de credenciais

Malwares especializados no roubo de credenciais evoluirão, combinando inteligência artificial e automação para ataques direcionados.

Exploração de dispositivos de borda e ORBs

Roteadores, *firewalls*, VPNs e outros dispositivos de borda serão cada vez mais alvos de ataques persistentes, permitindo invasões furtivas em redes corporativas.

TECNOLOGIAS

Preparação para a era pós-quântica
A segurança digital será cada vez mais automatizada, com soluções preditivas baseadas em inteligência artificial, criptografia pós-quântica e monitoramento contínuo de ameaças.

Cloud Security First
Com o aumento dos ataques à nuvem e à cadeia de suprimentos digital, a segurança da infraestrutura em nuvem se tornará a principal prioridade para empresas de todos os setores.

Machine Identity
A gestão de identidades de máquina será crucial para evitar sequestros de credenciais, ataques de falsificação de identidade e comprometimentos em infraestruturas críticas.

AI-driven cybersecurity
A inteligência artificial será a protagonista da segurança cibernética, automatizando respostas a ataques, reduzindo o tempo de detecção e aumentando a eficácia das estratégias de defesa.

Governança de IA
Com regulamentações mais rígidas, as empresas precisarão adotar políticas robustas de governança de IA para garantir transparência, conformidade e ética no uso dessa tecnologia.

O fim da segurança por obscuridade em OT
A convergência entre IT e OT ampliará a superfície de ataque em infraestruturas industriais e críticas.

O futuro do hardware de IA
A evolução do hardware de IA será essencial para equilibrar desempenho e sustentabilidade, à medida que modelos de aprendizado de máquina exigem maior capacidade computacional.

Regulamentação e geopolítica
A cibersegurança estará cada vez mais atrelada a disputas geopolíticas e regulamentações globais, forçando empresas a adaptarem suas estratégias para garantir conformidade e resiliência.

O QUE ACONTECEU NO ANO DE 2024?

O ano de 2024 foi definitivamente um período de grandes acontecimentos no mundo da cibersegurança. Ataques sofisticados e operações criminosas atingiram governos, grandes empresas e infraestruturas críticas, além dos próprios usuários finais, evidenciando vulnerabilidades, desafios emergentes e causando vazamentos. Segundo o relatório anual da IBM Cost of a Data Breach, o custo médio de uma violação de dados saltou para **US$ 4,88 milhões** no ano passado.

Antes de abordarmos as tendências da SEK para 2025, falaremos sobre os principais acontecimentos que ganharam os holofotes da mídia internacional. Os eventos de 2024 devem servir de ensinamento para que companhias consigam se proteger contra ameaças semelhantes.

Ataques a infraestruturas críticas

Ataques cibernéticos contra infraestruturas críticas não são novidade. **Mas, em 2024, vimos que essas invasões estão cada vez mais capazes de desestabilizar setores**. De hospitais a aeroportos e sistemas governamentais, ficou evidente o quanto essas estruturas são vulneráveis.

O setor de saúde foi um dos mais afetados, sendo um alvo lucrativo tanto pela urgência dos serviços quanto pelo valor dos dados médicos. No **Brasil**, o ataque ao **Instituto Nacional de Câncer** (INCA) comprometeu o atendimento a pacientes oncológicos. Nos **EUA**, a investida contra **Change Healthcare**, subsidiária da **UnitedHealth**, foi **um dos maiores vazamentos de dados do setor**. A invasão do grupo de *ransomware* BlackCat paralisou a emissão de receitas e outros serviços no país. O sistema de saúde pública do Reino Unido (NHS) levou quatro meses para se recuperar de **um ataque do grupo Qilin ao seu fornecedor Synnovis**.

Infraestruturas de **transportes e governos** também foram alvos. O presidente da **Venezuela**, Nicolas Maduro, acusou Elon Musk de realizar um ataque hacker que desestabilizou o **Conselho Nacional Eleitoral** no dia da eleição no país. No final do ano, **sites do governo argentino** foram alvo de atacantes que suspenderam os funcionamentos e publicaram vídeos com críticas ao então presidente, Javier Milei.

Em julho, o Ministério da Gestão e Inovação em Serviços Públicos do Brasil (**MGI**) sofreu um incidente que afetou sistemas administrativos como o **SEI**, usado por ministérios e órgãos federais. No mês seguinte, o **aeroporto de Seattle** foi afetado por um **ataque de *ransomware*** dias antes do feriado de Labor Day, gerando certo caos para os passageiros.

Lição aprendida

Esses eventos deixam uma lição importante: Pagar o resgate não garante a recuperação dos sistemas. A título de exemplo, a Change Healthcare desembolsou cerca de 22 milhões de dólares em pagamento ao grupo criminoso responsável pelo ataque, mas sofreu outra invasão meses depois.

Além de fortalecer os criminosos, **não há garantia de que os dados serão devolvidos ou que novos ataques não ocorrerão**. A única forma de mitigar o impacto de um *ransomware* é a preparação prévia com **backups offline, segmentação de rede e um plano de resposta**. Com as soluções de Detecção e Resposta a Ameaças da SEK, empresas podem adotar uma postura proativa, monitorando atividades suspeitas em tempo real e automatizando a contenção de ameaças.

Ascensão das novas ameaças e golpes digitais

O cibercrime também é um jogo psicológico. Em 2024, vários ataques digitais exploraram a confiança de usuários e colaboradores de formas muito criativas. O objetivo foi burlar sistemas de segurança, obter dados e quantias monetárias por meio da manipulação de vítimas.

O ***deepfake*** foi um dos exemplos mais marcantes, uma tendência que vai continuar em 2025, como você verá neste relatório da SEK. Com inteligência artificial, criminosos criaram mídias realistas para se passar por executivos de grandes empresas, colegas e usuários de apps financeiros.

O **golpe das encomendas dos Correios** também mostrou como ataques de ***phishing*** podem ser extremamente eficazes. Criminosos usavam mensagens sobre supostas taxas para manipular as vítimas a fornecerem dados e pagarem boletos em sites falsos. Não foi preciso muita complexidade para que causassem danos.

Outra ameaça foi o **aumento dos *infostealers***, *malwares* projetados para roubo de dados sensíveis como credenciais. Segundo a **Check Point**, há mais de **10 milhões de *logs* de *infostealers*** disponíveis para compra no mercado russo. Na *dark web*, essas ferramentas são vendidas como ***malware-as-a-Service*** (MaaS), o que permite até criminosos sem tantos conhecimentos técnicos usarem as ferramentas com suporte profissional.

Lição aprendida

Os ataques de 2024 ensinaram algo que vai além do tradicional: **não podemos mais confiar no que interagimos digitalmente**. Ao longo dos anos, empresas podem ter focado em proteger sistemas contra invasões externas, mas a nova onda de ameaças comprova que é necessária **a proteção contra ameaças internas**. Um clique é tudo o que um atacante precisa para invadir.

Companhias precisam educar funcionários para que desconfiem até das interações mais banais, pois são elas que frequentemente abrem a porta para fraudes mais graves. Treinamentos contínuos, como os proporcionados pela solução de Strategy & Risk eleva a maturidade cibernética da organização ao capacitar todas as equipes para reconhecer e mitigar ameaças.

Vazamentos de dados

As exposições de informações ganharam protagonismo. Não à toa, já que os dados pessoais e corporativos são uma das moedas mais valiosas. O mercado clandestino de dados agora é uma economia paralela, com intermediários e plataformas próprias.

Neste ponto, os ***infostealers*** também fizeram uma aparição. Ator de ameaça teve acesso a dados sigilosos de empresas como **Ticketmaster, AT&T** e **Santander**. As informações foram obtidas por meio uma invasão na **plataforma Snowflake**, utilizada por essas companhias. Por sua vez, a invasão às contas foi efetuada por meio do **roubo de credenciais feito por um *infostealer***. Os atacantes conseguiram exportar dados de milhões de pessoas, de funcionários a clientes. A ação rendeu mais de US$ 2 milhões aos criminosos, que obtiveram dinheiro das companhias que pagaram o resgate.

Outro vazamento envolveu a gigante **Dell**, que sofreu a exposição de informações de aproximadamente **49 milhões** de seus consumidores. O ator de ameaça relatou em fórum hacker que havia dados como nomes e endereços completos.

O **Pix**, modo de transferência monetária instantâneo e eletrônico, também foi alvo de vazamentos. O sistema de pagamentos mais popular do país sofreu com **ao menos dez exposições** de chaves de clientes de diferentes organizações, como **99Pay, Caixa e Shopee**. A maior exposição estava relacionada a falhas nos sistemas da Qesh, que ocasionou o vazamento de dados cadastrais de **53 mil chaves**.

Lição aprendida

A SEK destaca que esses vazamentos comprovam que companhias devem prestar **atenção aos seus fornecedores**. Se provedores não conseguem proteger os dados que sua companhia compartilha com eles, então a empresa está sob risco de invasões por meio da cadeia de suprimentos. Não adianta se preocupar apenas com sua própria proteção enquanto outros atores na cadeia estão vulneráveis.

A **Gestão de Postura da SEK** auxilia empresas a monitorarem e garantirem que seus parceiros atendam aos padrões de segurança, reduzindo riscos provenientes da **cadeia de fornecimento**.
É importante certificar-se de que as organizações e seus fornecedores estejam blindados e de acordo com as melhores práticas da indústria.

Cibercrime no setor empresarial

Até mesmo empresas reconhecidas não estiveram imunes a problemas. Nomes como KnowBe4 e Banco do Brasil sofreram com falhas em seus próprios processos.

A **KnowBe4** protagonizou um incidente em 2024. A companhia contratou, sem saber, um **funcionário falso de TI norte-coreano** para sua vaga de Engenheiro de Softwares. O indivíduo, que usou uma identidade criada por IA, passou por todas as etapas de contratação, incluindo várias videoconferências, e conseguiu se infiltrar na organização. Ele passou a **transferir arquivos e executar softwares não autorizados**. O impacto poderia ter sido muito maior se a equipe de segurança da informação da gigante não tivesse bloqueado suas ações.

O Banco do Brasil também foi um exemplo. Em março de 2024, uma operação policial revelou a ação de uma quadrilha que fraudava o seu sistema. O grupo criminoso contou com a ajuda de funcionários da instituição, como gerentes e membros da equipe de TI. Esses facilitaram a inserção de *scripts* maliciosos nos sistemas, permitindo acesso remoto a informações sigilosas e a realização de transações bancárias em nome dos clientes.

Lição aprendida

Esses incidentes mostram que a segurança não se resume a implementar as melhores ferramentas. Ela também é a **capacidade de uma empresa de garantir a segurança de seus processos**, desde a contratação até a gestão de incidentes. É sobre **como uma organização lida com crises**, em vez de esperar que nunca aconteçam.

O que ocorre depois de um ataque, ou seja, a forma como a empresa se recupera, comunica-se com seus stakeholders e ajusta suas defesas, pode ser **mais importante do que o problema inicial.** Com soluções como o ***Resilience Acceleration Program*** (RAP) da SEK, empresas podem adotar uma abordagem estratégica para segurança, integrando pessoas, processos e tecnologias para fortalecer a capacidade de resposta e recuperação a incidentes, garantindo processos mais seguros.

Grandes operações criminosas

Operações em larga escala de cibercriminosos continuaram sendo um destaque em 2024. Ao redor do mundo, ameaças cibernéticas miraram incontáveis serviços e eventos, como as Olimpíadas de Paris de 2024. Mas esses grupos também foram alvo de operações policiais responsáveis por desmantelar seus funcionamentos.

A vitória temporária contra grupos como o **LockBit** foi um marco de 2024. Na Operação Cronos, autoridades de países como EUA, França e Canadá suspenderam a infraestrutura do grupo, dentre dezenas de servidores que armazenavam um site de vazamentos. No entanto, o ator de **ameaça criou nova estrutura** menos de uma semana depois. Vários membros da gangue foram identificados e presos ao longo do ano.

Outro exemplo alarmante foi a operação **ArcaneDoor**, descoberta pela Cisco Talos. Essa campanha **mirou dispositivos de rede de alto nível**, explorando vulnerabilidades para garantir acesso persistente e invisível a infraestruturas como telecomunicações e setores de energia.

Em 2024, a **França** virou um alvo muito interessante para cibercriminosos. O país foi vítima de mais de **140 incidentes** relacionados diretamente ao evento das **Olimpíadas de Paris**. O **Grand Palais**, centro de exposição que era usado para os Jogos, foi um dos locais afetados por um ataque de ***ransomware*** na época. Mas os ataques não se limitaram a sistemas relacionados ao esporte, porque afetaram também entidades governamentais e infraestruturas de transporte e telecomunicações.

Lição aprendida

A queda do LockBit e o surgimento de outras operações mostram que **não basta erradicar uma ameaça para garantir a segurança**. Quando um grupo é derrubado, seus métodos, ferramentas e contatos são rapidamente reciclados e redistribuídos, muitas vezes com melhorias, em novas operações criminosas.

A questão é que o cibercrime não depende de um único operador para funcionar, então, é preciso dificultar a vida de criminosos, seja por meio do não pagamento de resgates, da denúncia ou das boas práticas de prevenção de ataques. Soluções de ***Threat Intelligence*** da SEK permitem que empresas monitorem ameaças emergentes antes que elas se tornem ataques direcionados, garantindo uma postura mais proativa e resiliente contra o cibercrime.

Ciberataques geopolíticos

A ciberespionagem tem sido uma das grandes protagonistas quando o assunto é conflitos geopolíticos. Tanto que não foi diferente no ano de 2024. O Fórum Econômico Mundial (WEF) já vem alertando sobre o aumento dos confrontos geoeconômicos ao redor do mundo. Assim, enquanto governos como China e EUA trocam acusações, a espionagem também é utilizada como uma peça estratégica.

Autoridades dos **Estados Unidos** afirmaram, neste ano, que o grupo **Volt Typhoon**, vinculado à **China**, teria se infiltrado em infraestruturas críticas. Por supostamente **mais de cinco anos**, o ator de ameaça teria sido capaz de espionar setores de comunicações, energia, transporte e saneamento. Tudo isso sem ser identificado. De acordo com o governo americano e seus aliados, a ação visava **destruir serviços críticos** do país em uma época em que já há uma tensão entre as duas nações.

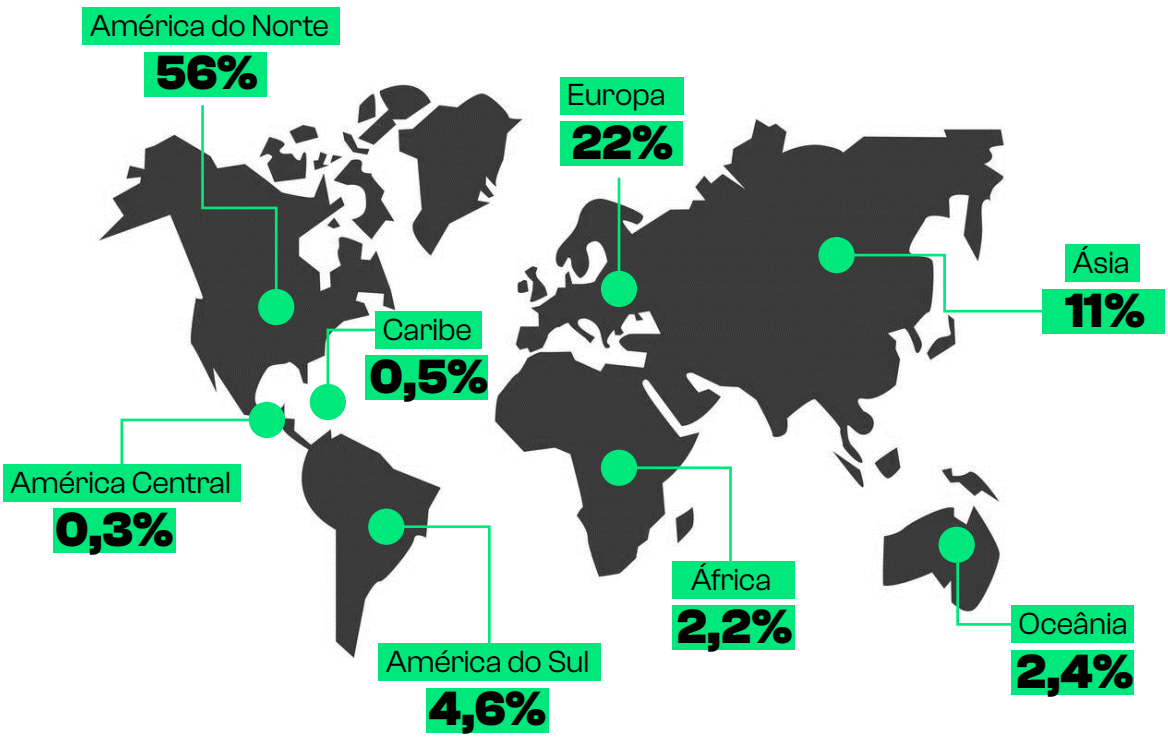
No fim do ano, outro grupo foi acusado pelos americanos. **Salt Typhoon**, também de origem chinesa, teria conduzido uma **campanha de espionagem** contra oficiais do governo por meio do comprometimento de provedores de comunicação. As campanhas dos então candidatos à presidência **Donald Trump** e **Kamala Harris** tinham sido alguns dos alvos.

Lição aprendida

A descobertas dessas operações de ciberespionagem deixou claro que muitos grupos invadem redes e sistemas com o objetivo de obter informações da forma mais sigilosa possível. Eles se infiltram, estudam, aprendem e esperam. Quando um ataque desse tipo vem a público, o mais provável é que ele tenha começado anos antes.

É fundamental que companhias usem **ferramentas de *threat hunting*** eficientes, buscando sinais de presença adversária antes que seja tarde demais.

Ataques de ransomware em todo o mundo em 2024



**Fonte: investigações da equipe de Cyber Threat Intelligence da SEK e dados do Data Breaches Digest*

De acordo com pesquisas exclusivas da SEK, em 2024, a distribuição global dos ataques de *ransomware* evidenciou uma concentração significativa na **América do Norte**, que respondeu por **56% dos incidentes registrados**. Este dado reforça a posição da região como o principal alvo desses grupos criminosos, possivelmente em razão do alto grau de digitalização das organizações locais e do maior potencial financeiro das vítimas, fatores que tornam os ataques mais lucrativos.

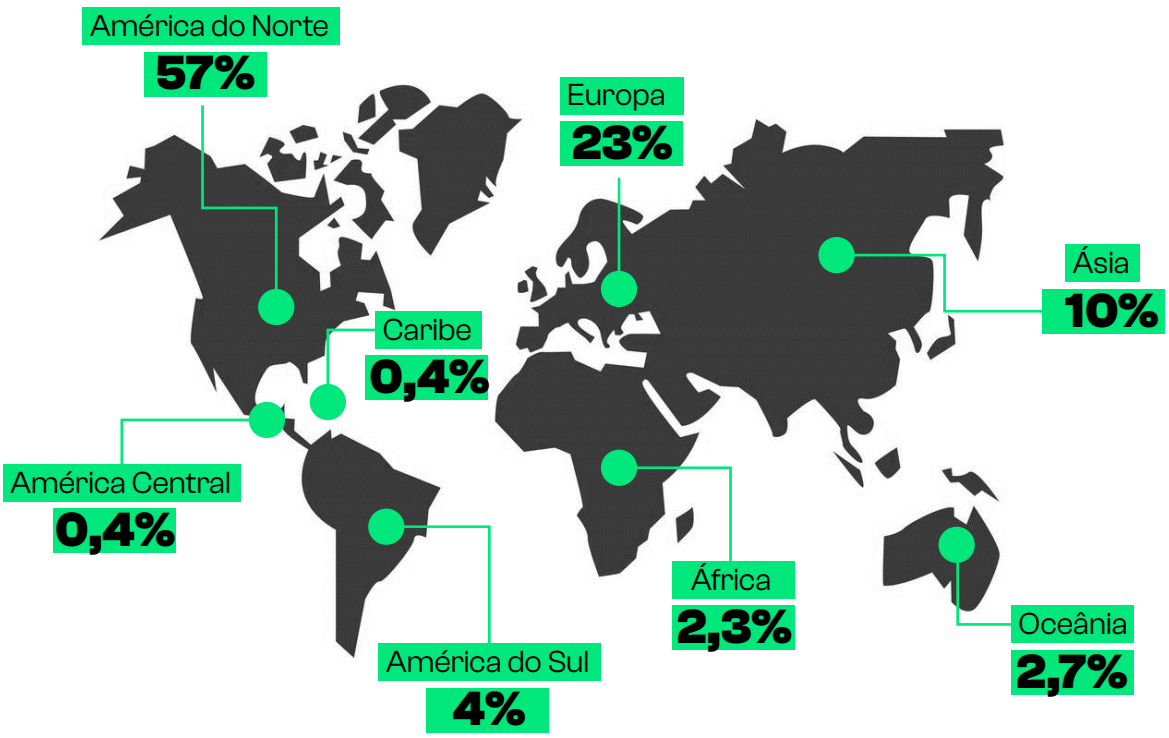
A **Europa**, com **22% dos casos**, manteve-se como uma região de alta relevância para os operadores de *ransomware*, especialmente em países com forte presença de setores críticos e empresas multinacionais, que oferecem oportunidades atrativas para extorsão.

Na **Ásia**, observou-se uma participação de **11% nos ataques**, indicando um crescimento progressivo da ameaça no continente. Este movimento pode estar relacionado ao aumento das **tensões geopolíticas**, que frequentemente impactam o cenário de ciberameaças.

A América do Sul representou 4,6% dos ataques em 2024. Embora esse percentual pareça modesto em comparação, ele reflete uma tendência de crescimento em comparação com anos anteriores, com destaque para incidentes significativos envolvendo órgãos governamentais e infraestruturas críticas, como os casos ocorridos na Argentina e no Instituto Nacional de Câncer (INCA), no Brasil.

As demais regiões apresentaram percentuais mais baixos: Oceania (2,4%), África (2,2%), Caribe (0,5%) e América Central (0,3%). Ainda que menos visadas em termos absolutos, essas regiões não estão imunes aos efeitos do *ransomware*. Em muitos casos, os impactos são potencialmente mais severos, uma vez que as organizações locais tendem a estar **menos preparadas** para responder a esse tipo de ameaça, o que amplia a vulnerabilidade e os danos causados pelos ataques.

Vazamentos de dados em todo o mundo em 2024



**Fonte: investigações da equipe de Cyber Threat Intelligence da SEK e dados do Data Breaches Digest*

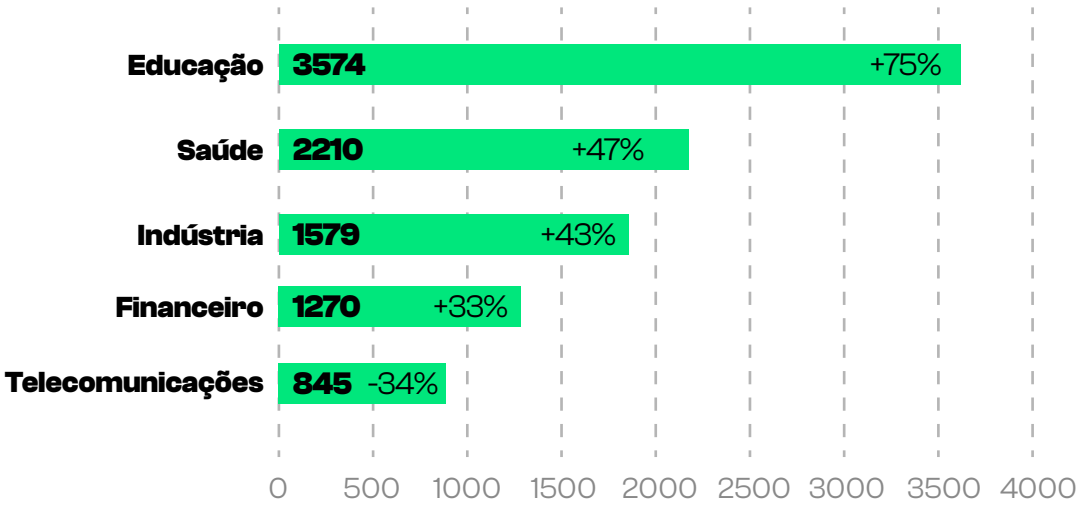
As pesquisas da SEK também analisaram **a distribuição global de vazamentos de dados em 2024**, responsável por evidenciar uma **concentração expressiva na América do Norte**, que conta com 57% dos incidentes registrados no período. Esse percentual reflete o elevado volume de informações comprometidas, especialmente nos Estados Unidos, onde grandes corporações e infraestruturas críticas permanecem entre os principais alvos de agentes maliciosos.

A **Europa ocupa a segunda posição**, com 23% dos casos, resultado não apenas da frequência de ataques, mas também da maior transparência imposta por regulamentações como a GDPR, que exige a **notificação obrigatória de incidentes** de segurança envolvendo dados pessoais.

A **Ásia**, com 10%, manteve um índice relevante, impulsionado por vazamentos em empresas de grande porte, especialmente nos setores de tecnologia e comércio eletrônico. Na **América do Sul**, os vazamentos corresponderam a 4% do total global. Esse número representa uma **tendência de aumento na exposição de dados** na região, com destaque para os setores financeiro e governamental.

África (2,3%) e Oceania (2,7%) apresentaram percentuais inferiores, o que não implica necessariamente um menor risco. Em muitos casos, essas regiões podem enfrentar maiores dificuldades na detecção, resposta e mitigação de incidentes. América Central e Caribe, com 0,4%, registraram os menores índices, possivelmente em decorrência de uma menor superfície de ataque ou de uma subnotificação ou falta de visibilidade sobre os incidentes ocorridos.

Aumento dos ataques cibernéticos por setor em 2024



**Fonte: Check Point

Em 2024, atores de ameaça visaram diferentes setores ao longo do ano. Recomendações específicas para cada um desses alvos estarão disponíveis no especial de "Como diferentes setores podem se preparar para os desafios?" deste Think Ahead Report.

De acordo com dados do relatório The State of Global Cyber Security 2025 Report, da Check Point, observou-se um aumento expressivo no volume de ataques cibernéticos por setor em 2024.
No total, houve um crescimento de 44% nos ciberataques em relação ao ano passado, o que já evidencia a necessidade de decisões mais estratégicas para melhorar a resiliência das organizações.

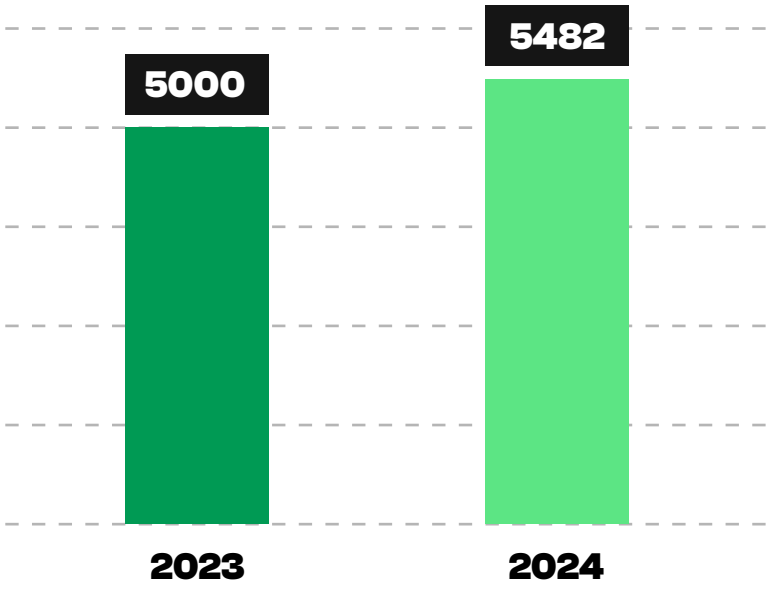
O setor de educação lidera o ranking, registrando 3.574 ataques semanais por organização — um crescimento de 75% em relação ao ano anterior. Esse avanço pode ser atribuído à intensificação da digitalização no setor e à ausência de investimentos robustos em cibersegurança, o que torna escolas e universidades alvos frequentes dos criminosos, dada sua infraestrutura geralmente limitada.

Na sequência, vem o setor de saúde, com média de 2.210 ataques semanais, um aumento de 47%. A atratividade desse setor para os atacantes está associada ao alto valor dos dados médicos no mercado negro e à baixa tolerância a interrupções, o que torna hospitais e clínicas alvos preferenciais para campanhas de ransomware.

O setor industrial registrou 1.579 ataques semanais, com um aumento de 43%. Esse crescimento reforça o interesse dos cibercriminosos em setores estratégicos, nos quais ataques podem provocar paralisações, vazamento de informações sensíveis e sabotagem.
Em quarto lugar, o setor financeiro também foi pressionado por cibercriminosos, registrando 1.270 ataques semanais — uma alta de 33%. O interesse contínuo nesse setor está relacionado à possibilidade de ganhos financeiros diretos, tanto por meio de fraudes quanto de extorsões.

Por fim, chama atenção o comportamento do setor de telecomunicações, que teve uma queda de 34% no volume de ataques em relação a 2023, com 845 ataques semanais. Essa redução pode estar relacionada a investimentos mais robustos em segurança ou à mudança no foco dos atacantes, que voltaram sua atenção a setores mais vulneráveis.

Incidentes mundiais de ransomware: uma comparação 2023 e 2024

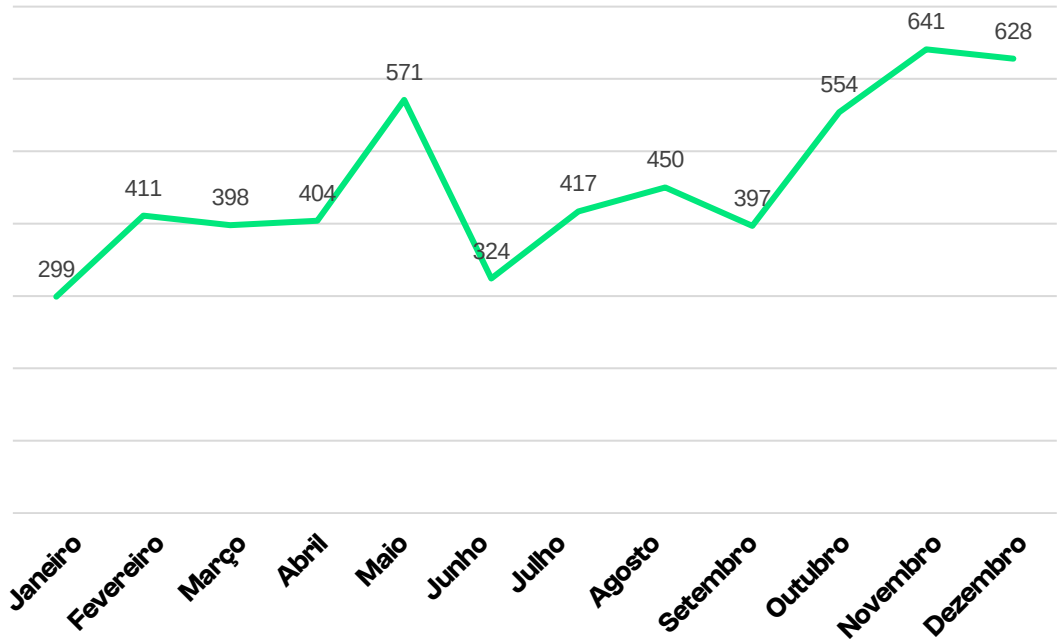


***Fonte: investigações da equipe de Cyber Threat Intelligence da SEK e dados do Data Breaches Digest*

Como já abordado neste artefato, houve **um aumento considerável entre ataques de *ransomware* no último ano**. Assim, a comparação entre os incidentes globais de ransomware registrados em 2023 e 2024 revela **um aumento de 9,6%**, com o número de casos passando de aproximadamente 5.000 para 5.482. Esse crescimento reforça a constatação de que os grupos especializados nesse tipo de ataque seguem operando com alta intensidade, adaptando-se rapidamente ao cenário tecnológico.

O avanço é indicativo da **contínua evolução nas táticas** utilizadas por esses agentes, que vêm explorando novas vulnerabilidades, diversificando os vetores de ataque e empregando métodos de extorsão cada vez mais sofisticados — incluindo a combinação de **criptografia de dados** com ameaças de vazamento de informações sensíveis. Abordaremos essas informações com mais detalhes nas seções sobre o mais recente *Ransomware 3.0*.

Ataques de ransomware no mundo em 2024

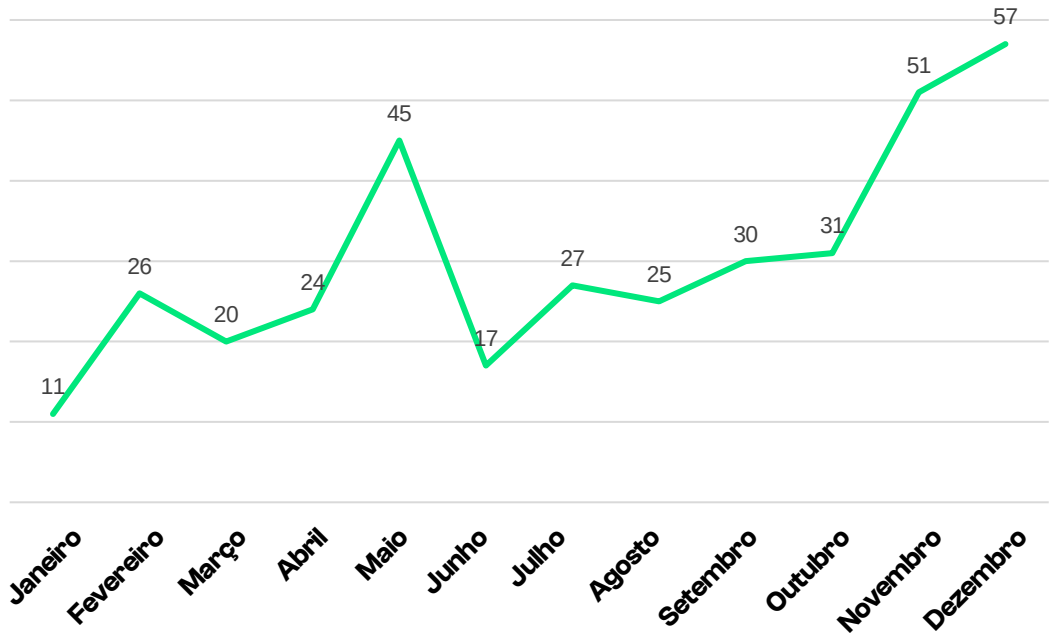


**Fonte: investigações da equipe de Cyber Threat Intelligence da SEK e dados do Data Breaches Digest*

Dentre essa quantidade expressiva de ataques de *ransomware* ao redor do globo, também aconteceu uma oscilação significativa ao longo do ano. O número de ataques passou de 299 em janeiro para 628 em dezembro, com destaque para um crescimento acentuado em maio (571 ataques), seguido por uma queda expressiva em junho (324 ataques), antes de retomar uma trajetória de alta nos meses subsequentes.

A análise dos dados indica um **comportamento cíclico** por parte dos grupos criminosos, que parecem adaptar suas estratégias de acordo com fatores operacionais e contextuais. A redução observada em junho pode estar relacionada a **operações de repressão conduzidas por autoridades**, como já abordado neste Think Ahead Report, ou a ajustes táticos realizados pelos próprios agentes, o que é comum após períodos de atividade intensa. Esse padrão evidencia a importância de uma postura de segurança cibernética reforçada nos períodos de maior exposição, com monitoramento contínuo, resposta ágil a incidentes e medidas preventivas específicas para mitigar riscos em momentos críticos do ano.

Ataques de ransomware na América Latina em 2024



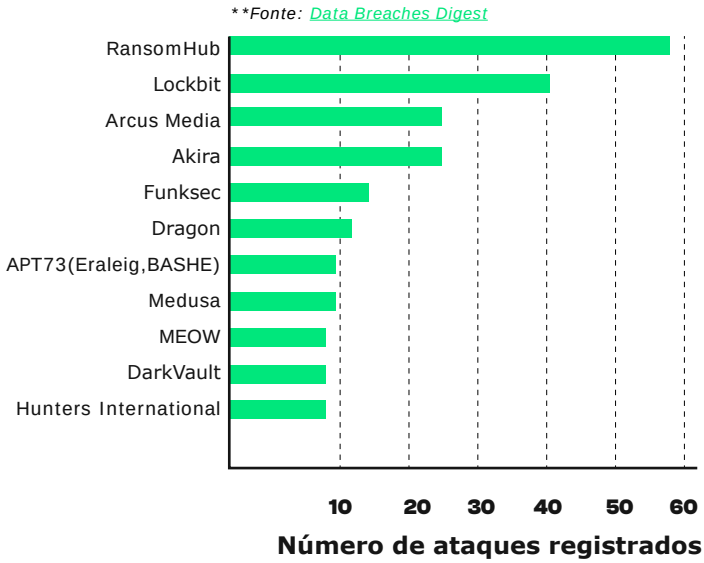
**Fonte: investigações da equipe de Cyber Threat Intelligence da SEK e dados do Data Breaches Digest*

Nesse mesmo sentido, a **América Latina também experienciou um ritmo de ataques parecido com o resto do mundo**. A evolução dos ataques no continente revelou uma tendência de crescimento progressivo ao longo do segundo semestre, com destaque para o mês de dezembro, que registrou o maior número de incidentes no ano (57 ocorrências). Em contraste com o cenário de 2023, quando o pico se deu em julho, o padrão observado em 2024 indica uma **intensificação mais tardia das atividades maliciosas** na região.

Nos primeiros meses do ano, o número de ataques apresentou variações, com um aumento inicial em maio (45 incidentes), seguido por uma queda acentuada em junho (17 incidentes). A partir de julho, no entanto, os registros voltaram a crescer de forma gradual e consistente até o final do ano.

Esse comportamento aponta para um período de **risco elevado no segundo semestre**, exigindo atenção redobrada por parte de empresas e instituições públicas ou privadas. A concentração de ataques nos últimos meses do ano pode estar associada a fatores como o **aumento da movimentação financeira, eventos comerciais de grande porte** — como Black Friday e Natal — **e períodos de recesso**, que muitas vezes resultam em estruturas de segurança e monitoramento mais fragilizadas.

Grupos de ransomware mais ativos na América Latina (2024)



Dentre as várias ameaças na América Latina, alguns **grupos de *ransomware*** ganharam destaque. Em 2024, os grupos de ransomware mais ativos na América Latina refletiram um cenário de diversidade e sofisticação nas operações cibercriminosas. De acordo com investigações da SEK, o **RansomHub** destacou-se como o mais atuante na região, com quase 60 ataques registrados, seguido pelo **LockBit,** já consolidado como uma das ameaças mais recorrentes no cenário global.

Também se observaram atividades relevantes por parte de outros grupos, como Arcus Media, Akira e Funksec, evidenciando a atuação de múltiplos agentes com diferentes perfis e metodologias na região.

Em termos geográficos, o Brasil foi o país mais afetado, com um total de 62 incidentes, sendo o principal alvo dos grupos **RansomHub, Arcus Media** e **Akira**. Em seguida, aparecem o México (20 ataques), Argentina (14), Peru (10), Colômbia (10) e Chile (9). A **predominância do Brasil como alvo** pode estar diretamente relacionada à sua posição como maior economia da região, além de sua infraestrutura digital desenvolvida, o que amplia a superfície de ataque e o potencial de retorno financeiro para os grupos criminosos.

Por conta de todo esse cenário, medidas como o monitoramento contínuo de ativos digitais, planos eficazes de resposta a incidentes e programas de capacitação para equipes técnicas e operacionais tornam-se cada vez mais essenciais para reduzir a exposição e mitigar os impactos desses ataques.

País /Grupo	RansomHub	LockBit	Arcus Media	Akira	Funksec	Total
Brasil	26	8	13	11	4	62
México	6	10	2	1	1	20
Argentina	3	4	1	4	2	14
Peru	3	3	1	2	1	10
Colômbia	3	3	4			10
Chile	4	3		1	1	9
Total	**45**	**31**	**21**	**19**	**9**	**125**

**Fonte: Data Breaches Digest

Os atores de ameaça chave na América Latina

Considerando a presença expressiva de alguns atores de ameaça específicos no continente em 2024, é fundamental que companhias compreendam como tais grupos operam seus ataques.

RansomHub

- Um dos grupos mais ativos da América Latina.
- Opera no modelo *Ransomware-as-a-Service* (RaaS), recrutando afiliados para expandir seus ataques.
- Explora vulnerabilidades conhecidas e credenciais comprometidas para acesso inicial.
- Tem como alvos principais os setores de saúde, financeiro, governamental e infraestrutura crítica.

LockBit

- Um grupo consolidado no cenário global de *ransomware*.
- Responsável por utilizar técnicas avançadas de criptografia e evasão para dificultar sua detecção.
- Seus ataques afetam empresas de vários setores ao redor do mundo.
- Está ligado a mais de 526 ataques confirmados em 2024.

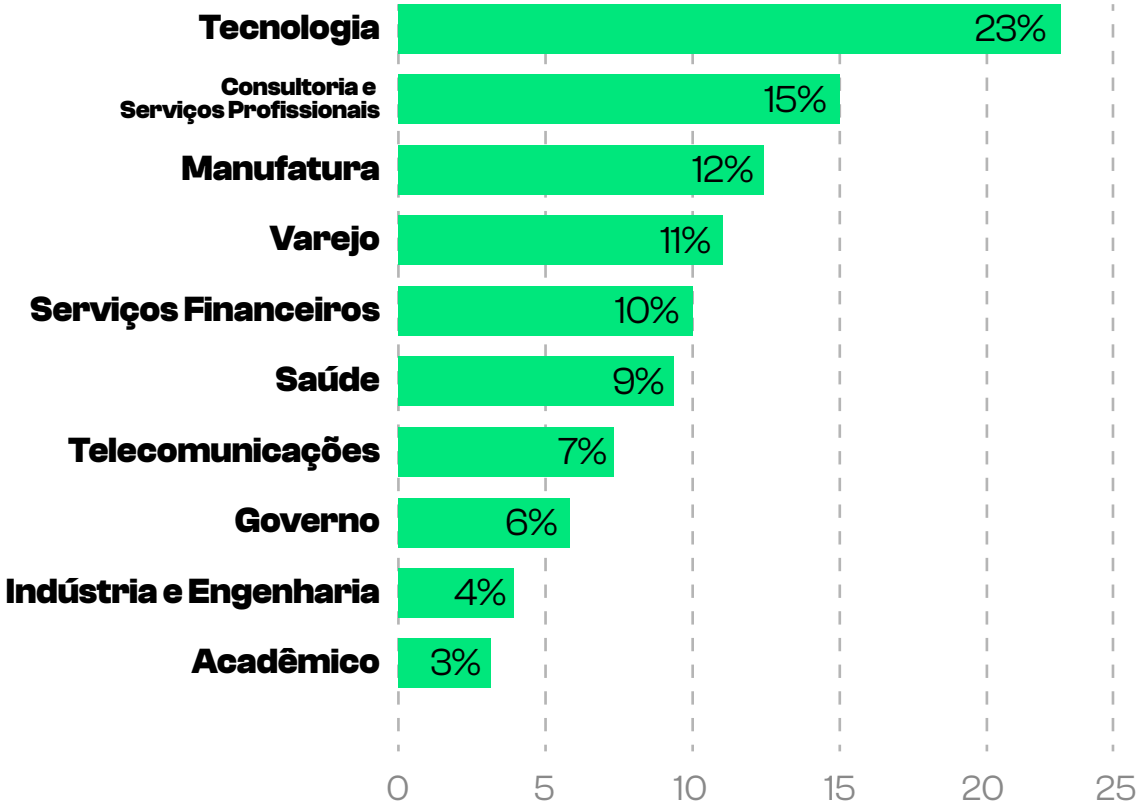
Arcus Media

- Grupo de *ransomware* que surgiu em maio de 2024, operando por meio do modelo *Ransomware-as-a-Service* (RaaS).
- Ainda há pouca informação técnica sobre suas táticas.
- Já atingiu setores como serviços empresariais, varejo e mídia.
- Associado a mais de 50 ataques confirmados.

Akira

- Explora VPNs da Cisco vulneráveis para obter acesso inicial.
- Além de criptografar, o grupo pode exfiltrar dados e exigir um resgate das vítimas em troca do não vazamento dessas informações.
- Visa grandes empresas na América do Norte, Europa e Austrália, focadas em educação, finanças, manufatura e saúde.

Setores mais afetados por intrusões interativas em 2024



**Fonte:investigações da equipe de Cyber Threat Intelligence da SEK e dados da CrowdStrike*

Dentro do período de 2024, vários setores também foram atingidos por outra ameaça: a **intrusão interativa**. Esse tipo de invasão caracteriza-se pelo uso de credenciais comprometidas e pela realização de movimentos laterais dentro das redes, permitindo que os atacantes mantenham acesso persistente e ampliem sua presença nos sistemas-alvo.

De acordo com dados do 2025 Global Threat Report da CrowdStrike, os setores mais afetados por essas instrusões interativas refletem um padrão de ataques direcionados a **ambientes corporativos com alto valor estratégico**. O setor de tecnologia liderou em número de incidentes, com 23 casos registrados, seguido pelos segmentos de consultoria e serviços profissionais (15), manufatura (12) e varejo (11). Esses setores compartilham características como grande volume de dados sensíveis, conectividade ampla com parceiros e clientes, e participação em cadeias de suprimentos críticas — o que os torna especialmente atrativos para agentes maliciosos.

Setores considerados críticos também figuraram entre os mais impactados: financeiro (10 incidentes), saúde (9) e telecomunicações (7). A presença desses setores no relatório evidencia o interesse dos atacantes em comprometer infraestruturas essenciais, muitas vezes visando espionagem, interrupção de serviços ou extorsão.

A **diversidade dos alvos** reforça a necessidade de controles de acesso robustos, monitoramento contínuo de credenciais e autenticação multifator como medidas fundamentais para prevenir esse tipo de ataque e mitigar o risco de movimentação lateral nas redes corporativas.

As principais vulnerabilidades de 2024

**Fontes: investigações da equipe de Cyber Threat Intelligence da SEK e dados da NVD.*

Em 2024, o volume de vulnerabilidades reportadas atingiu um novo recorde. De acordo com a National Vulnerability Database (NVD) do NIST, foram registrados mais de 40 mil CVEs ao longo do ano, representando um aumento de quase 39% em relação a 2023.

Esse crescimento expressivo evidencia a agilidade com que elas são exploradas por agentes maliciosos. À medida que a superfície de ataque se expande, os adversários demonstram cada vez menos tempo de latência entre a identificação de uma vulnerabilidade e sua exploração ativa.

A SEK comunicou 244 CVEs relevantes aos seus clientes durante esse período, com destaque a falhas críticas, como:

- **CVE-2024-50623 e CVE-2024-55956, em ferramentas de transferência de arquivos da Cleo.**
- **CVE-2023-46805, CVE-2024-21887 e CVE-2024-21893, que afetaram soluções de VPN da Ivanti.**
- **CVE-2024-12356 e CVE-2024-12686, associadas à plataforma BeyondTrust.**

Essas falhas apresentam pontuações elevadas no CVSS, indicando alto grau de criticidade e risco potencial para ambientes corporativos. Diante desse cenário, torna-se essencial manter processos de gestão de vulnerabilidades e aplicação de patches atualizados, além de reforçar o monitoramento contínuo dos ativos expostos, serviços já fornecidos aos clientes SEK.

AS AMEAÇAS CIBERNÉTICAS DE 2025

Mais rápidas, inteligentes e implacáveis

O cenário de ameaças digitais está evoluindo em um ritmo sem precedentes. Em 2025, ataques impulsionados por inteligência artificial, ransomware sem criptografia e *infostealers* avançados redefinirão a forma como empresas e governos devem se proteger. A sofisticação das táticas criminosas — combinada com novas formas de desinformação e exploração silenciosa de dispositivos de borda — exige uma postura de segurança mais proativa e adaptável. Nesta seção, exploramos as principais ameaças emergentes e o que sua organização pode fazer para não ser pega de surpresa.

A nova era dos ataques com IA

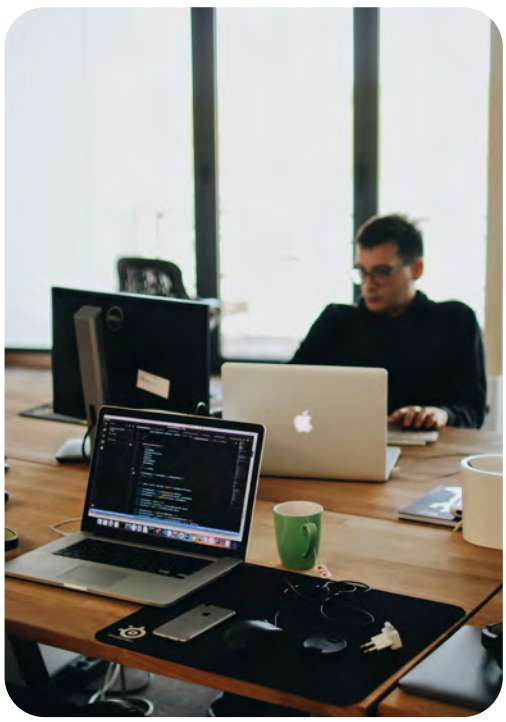
A ameaça invisível à segurança corporativa

O uso da inteligência artificial para aprimorar ataques cibernéticos está crescendo rapidamente. Em 2025, espera-se que ***phishing* automatizado, *deepfakes* realistas e *malware* inteligente** tornem-se armas comuns dos cibercriminosos.

Deepfakes avançados
78% das pessoas não conseguem distinguir um *deepfake* bem-feito de uma gravação real, facilitando fraudes financeiras e ataques a processos de autenticação.

Exploração acelerada de vulnerabilidades
O tempo médio para explorar falhas caiu de 32 para 5 dias, exigindo respostas mais rápidas das empresas.

Ataques mais acessíveis
O crescimento do crime cibernético "*as-a-service*" permite que hackers menos experientes executem operações sofisticadas.



Como se proteger?

Autenticação multifator
Resistente a *deepfakes* para evitar fraudes de identidade.

Ferramentas de IA
Para detecção de ameaças e identificação de padrões maliciosos.

Treinamento contínuo
Contra golpes de engenharia social aprimorados por IA.

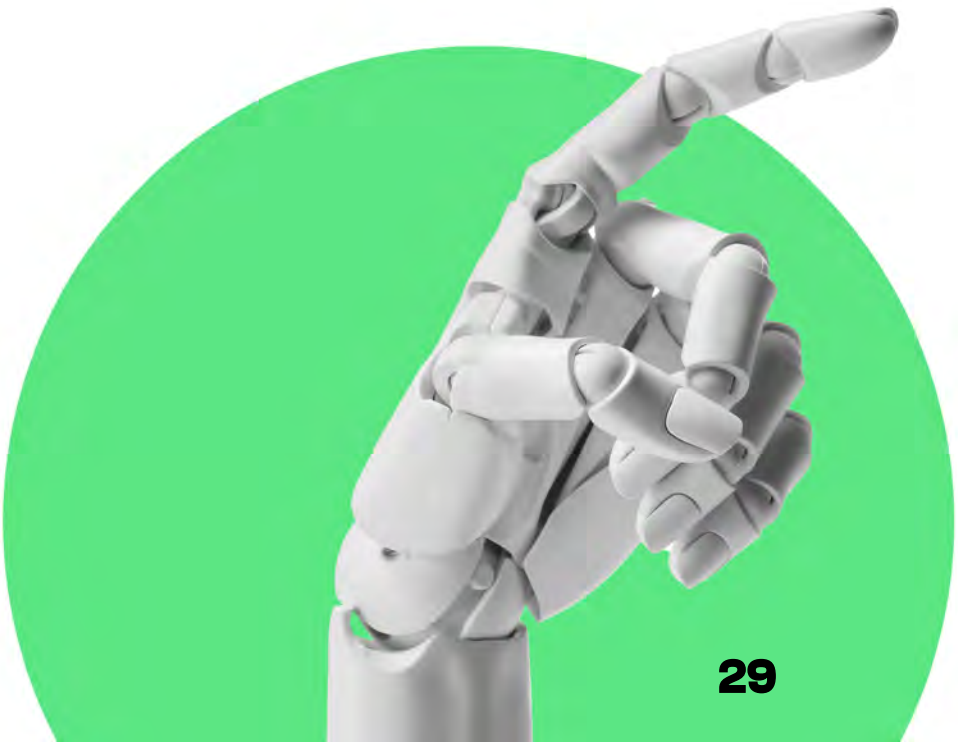
Com ataques cada vez mais sofisticados, a cibersegurança precisa evoluir junto com as ameaças.

Guerra de influência movida por IA

O avanço da inteligência artificial tem potencializado operações de desinformação em um nível sem precedentes. Em 2025, campanhas de influência movidas por IA serão capazes de manipular a opinião pública com alta precisão, impactando eleições, mercados financeiros e a credibilidade de organizações. Empresas e governos precisarão adaptar suas estratégias para mitigar os riscos desse novo cenário digital.

Evolução da tendência e impactos esperados

Nos últimos anos, ataques de influência evoluíram de simples disseminação de *fake news* para estratégias altamente sofisticadas, impulsionadas por *deepfakes* e aprendizado de máquina. Atores maliciosos agora utilizam IA para criar conteúdos personalizados, amplificar narrativas falsas e explorar vulnerabilidades cognitivas das audiências. Segundo a Gartner, em 2028, espera-se que 50% das empresas adotem tecnologias específicas para segurança contra desinformação, um crescimento substancial em relação aos menos de 5% em 2024.



Principais desafios e riscos

Eleições e democracia

Deepfakes e narrativas falsas podem minar a confiança no processo eleitoral, com evidências de que campanhas maliciosas já estão sendo conduzidas globalmente.

Manipulação de mercados

Relatórios indicam que deepfakes estão sendo utilizados para influenciar investidores e decisões estratégicas, ampliando riscos para o setor financeiro.

Fraudes corporativas

Empresas podem ser alvo de campanhas de desinformação destinadas a manipular valores de mercado e afetar sua reputação.

Recomendações para mitigação

- **Implementar plataformas de monitoramento de desinformação com IA forense.**
- **Investir em autenticação de conteúdo digital, utilizando blockchain e Content Credentials.**
- **Capacitar equipes para reconhecer sinais de manipulação digital e fortalecer práticas de alfabetização midiática.**
- **Fortalecer parcerias público-privadas para criar regulamentações eficazes contra a disseminação de deepfakes e conteúdos maliciosos.**

A guerra de influência movida por IA representa uma das maiores ameaças à cibersegurança global em 2025. Empresas e governos que não adotarem estratégias de defesa contra essa nova forma de manipulação digital estarão vulneráveis a ataques de grande escala.

Ransomware 3.0

O fim da criptografia e a era da extorsão de dados

O *ransomware* está passando por uma transformação radical. Em 2025, os ataques deixarão de depender exclusivamente da criptografia de arquivos e migrarão para um modelo de **extorsão baseada em exfiltração de dados** (*Data Exfiltration-Only Extortion* – DXF). Esse modelo já representou **65% dos ataques de *ransomware* em 2024**, permitindo que criminosos chantageiem as vítimas sem precisar se preocupar com descriptografia ou suporte técnico. Com o crescimento de plataformas clandestinas como **Bashe**, que facilitou a negociação de dados roubados e cresceu **300% em usuários em um ano**, espera-se que essa abordagem domine o cenário de ameaças em 2025.

A evolução da ameaça e seus impactos

O modelo tradicional de *ransomware* se baseava na criptografia de arquivos, mas com avanços em backups imutáveis e recuperação rápida, criminosos começaram a buscar novas formas de lucro. Grupos como **BianLian** e **Meow** abandonaram completamente a criptografia e passaram a operar apenas com **exfiltração e chantagem**, ameaçando vazar informações confidenciais. Além disso, **ataques a grandes empresas com faturamento acima de US$ 1 bilhão cresceram 87%**, indicando um foco maior em alvos estratégicos.

Principais desafios e setores mais impactados

A extorsão baseada em exfiltração traz desafios significativos, pois sua mitigação não depende apenas de backups. **Setores altamente regulamentados**, como saúde, financeiro e infraestrutura crítica, serão os mais afetados:

Setor de saúde

10%

de todas as vítimas de ransomware em 2024 estavam nesse setor, sendo que 65% dos casos ocorreram nos EUA.

Infraestrutura crítica

47%

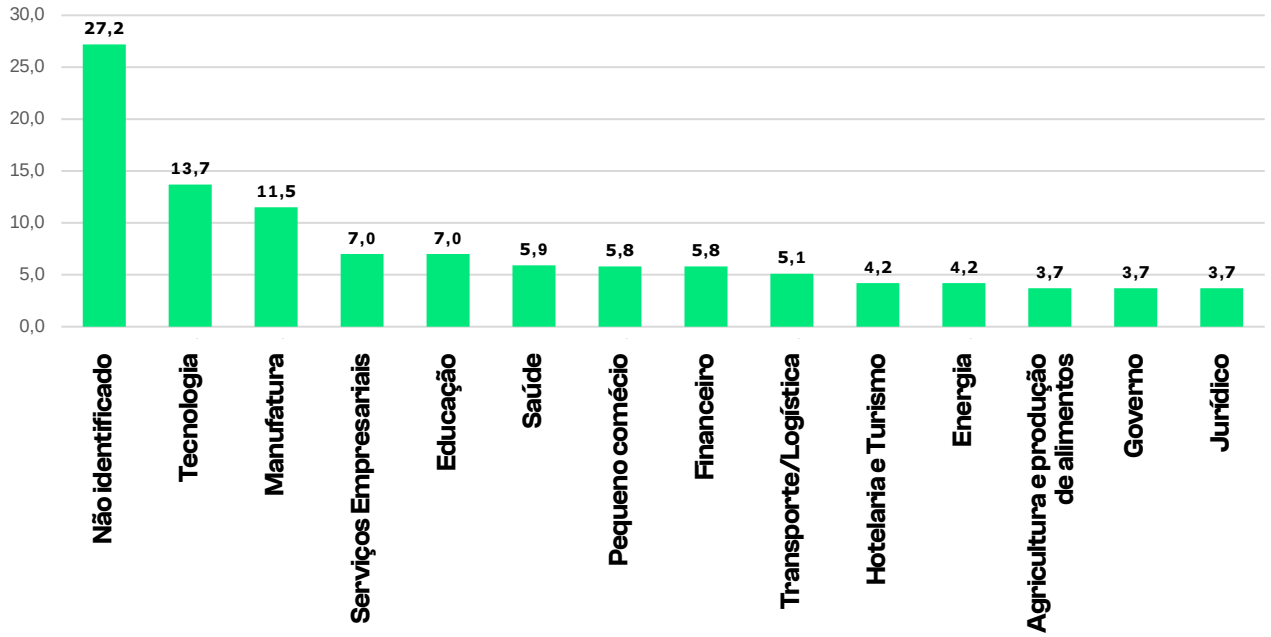
de aumento de ataques direcionados a energia e saneamento, em relação a 2023, aumentando os riscos de sabotagem.

Setor Financeiro

65%

das instituições financeiras relataram incidentes de ransomware com ameaça de vazamento de dados.

Como já está o cenário em 2025?



Fuentes: investigación del equipo de Cyber Threat Intelligence de SEK y datos de Ransomware.live.

Para compreender essa ameaça, também é importante demonstrar como os ataques de ransomware são realidade em todo o mundo neste ano. De acordo com investigações da SEK e de dados da plataforma Ransomware.live, a distribuição dessas invasões já revela a amplitude e a diversificação das operações de cibercriminosos.

O maior volume de ataques, correspondente a 27,2%, foi classificado como “não identificado”, o que pode indicar incidentes ainda em fase de investigação ou casos em que não foi possível associar o ataque a um setor específico.

Entre os setores com identificação clara, o segmento de tecnologia lidera com 13,7% dos ataques, seguido pela manufatura, com 11,5%. Ambos refletem um alto grau de exposição, seja pela dependência de sistemas digitais para suas operações, seja pelo valor estratégico das informações que armazenam. A interrupção de atividades nesses setores pode gerar impactos severos, o que os torna alvos atrativos para campanhas de extorsão.

Serviços empresariais e educação aparecem empatados com 7%, indicando um aumento na exploração de consultorias e instituições acadêmicas. O setor de saúde, com 5,9%, mantém relevância entre os mais visados, dada a sensibilidade e o valor dos dados médicos, além da urgência operacional característica dessas instituições.

Como as empresas podem se proteger?

Para mitigar essa nova geração de *ransomware*, organizações devem adotar uma abordagem focada na **prevenção e proteção de dados sensíveis**:

- **Adotar uma estratégia de zero trust, garantindo que o acesso a dados críticos seja restrito e monitorado.**
- **Investir em DLP (Data Loss Prevention) para identificar e bloquear transferências não autorizadas de informações sensíveis.**
- **Monitorar redes em tempo real para detectar atividades suspeitas antes que os dados sejam exfiltrados.**
- **Treinar colaboradores para identificar sinais de comprometimento e tentativas de phishing avançado, que aumentaram 3x com o uso de IA.**

O *ransomware* de 2025 não exigirá mais que os atacantes “trancem” seus dados — eles apenas precisarão roubá-los. Empresas que ainda baseiam suas defesas apenas em backups e recuperação rápida estão vulneráveis a essa nova realidade. A cibersegurança precisa evoluir, priorizando **proteção proativa, monitoramento contínuo e resiliência digital**.

É importante lembrar que **ataques humanos operados (HOR) estão crescendo 2,75x**, por isso, as empresas precisam se organizar para evitar que seus dados se tornem moeda de extorsão.

Infostealers 2.0

A nova era do roubo de credenciais

O roubo de credenciais sempre foi um dos principais vetores de ataque, mas em 2025, os ***infostealers*** (*malwares* especializados em capturar dados sensíveis) atingirão um novo nível de sofisticação. Com o avanço da economia do ***Cybercrime-as-a-Service*** (CaaS), qualquer cibercriminoso — mesmo sem habilidades avançadas — poderá acessar ferramentas automatizadas para invadir redes corporativas. Essa tendência ameaça a segurança de identidades digitais e impõe desafios inéditos para empresas e governos.

A evolução do infostealing e o que esperar em 2025

Os *infostealers* evoluíram rapidamente nos últimos anos, saindo do estágio de simples *keyloggers* para *malwares* avançados que capturam credenciais armazenadas em navegadores, cookies de sessão e dados financeiros. Segundo a Check Point em 2024, ataques envolvendo *infostealers* aumentaram **58%**, impulsionados pela disseminação do ***Cybercrime-as-a-Service*** (CaaS). O *malware* **AgentTesla** sozinho representou **43% das infecções globais** registradas. Além disso, o mercado clandestino Russian Market atualmente disponibiliza mais de **10 milhões de *logs* de *infostealers*** contendo credenciais roubadas.

Em 2025, essa ameaça se tornará ainda mais grave com a incorporação de **inteligência artificial**, permitindo ataques personalizados e maior automação. *Infostealers* como **Lumma, RedLine e StealC** estão cada vez mais utilizados para **roubar credenciais armazenadas e sequestrar sessões autenticadas**, permitindo que atacantes contornem medidas de segurança sem a necessidade de senhas.

Principais desafios e riscos

Ataques direcionados a empresas e setores críticos

Setores como financeiro, saúde e tecnologia serão os principais alvos. Atualmente, 90% das empresas que sofreram violações tiveram credenciais vazadas previamente em logs de infostealers, demonstrando seu papel crítico na cadeia de ataques.

Redução da eficácia de autenticação baseada em senhas

Com credenciais comprometidas circulando rapidamente em fóruns clandestinos, depender apenas de senhas se tornará um risco elevado.

Uso de IA para ataques mais sofisticados

Infostealers baseados em aprendizado de máquina poderão identificar alvos estratégicos e coletar informações de forma mais precisa e furtiva.

Como mitigar a ameaça?

- **Adotar autenticação multifator (MFA) e autenticação contínua para reduzir o impacto do roubo de credenciais.**
- **Implementar proteção avançada de endpoint (EDR/XDR) para detectar e bloquear infostealers em tempo real.**
- **Monitorar e revogar sessões suspeitas para evitar invasões por meio de cookies roubados.**
- **Treinar funcionários e fortalecer a postura de segurança contra ataques de phishing e engenharia social.**

O ano de 2025 marcará uma virada para a segurança digital, exigindo um **reposicionamento estratégico na proteção de credenciais e acessos**. À medida que os infostealers evoluem e se tornam mais acessíveis, a autenticação tradicional não será mais suficiente. Empresas e governos que não se adaptarem a essa nova realidade enfrentarão um risco crescente de invasões e vazamentos massivos de dados. **O futuro da segurança digital será definido pela capacidade de antecipar e neutralizar essas ameaças antes que causem danos irreversíveis.**

Exploração de dispositivos de borda e ORBs

O novo vetor de ameaças persistentes

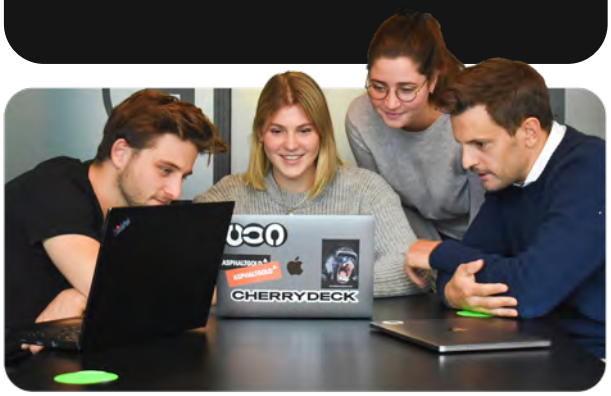
Os dispositivos de borda (roteadores, *firewalls*, *gateways,* VPN e IoT) estão se tornando um dos principais alvos para ameaças avançadas e persistentes (APT). Em 2025, espera-se que ataques direcionados a esses dispositivos aumentem exponencialmente, explorando configurações inadequadas e vulnerabilidades desconhecidas para obter acesso persistente e indetectável a redes corporativas.

Evolução da tendência e impactos esperados

Historicamente, os ataques se concentravam em endpoints e servidores. No entanto, em 2024, ameaças como a operação **ArcaneDoor** demonstraram que *firewalls* e VPNs podem ser comprometidos para espionagem e persistência prolongada.

Um estudo da Microsoft revelou que 75% das ameaças direcionadas a infraestruturas críticas em 2024 exploraram dispositivos de borda.

O relatório da Fortinet indicou um aumento de 68% nos ataques a VPNs e firewalls expostos na internet, com ataques provenientes principalmente de grupos estatais chineses e russos.



O uso de Operational Relay Boxes (ORBs) por grupos estatais chineses tem permitido ataques anonimizados e altamente sofisticados contra infraestruturas críticas, dificultando a atribuição das ameaças.

Principais desafios e riscos

Persistência silenciosa

Backdoors implantados nesses dispositivos são difíceis de detectar e remover.

Falta de visibilidade

60% das empresas monitoram apenas endpoints e servidores, negligenciando firewalls e roteadores, conforme apontado no Google Cloud Cybersecurity Forecast 2025.

Escassez de patches

Fabricantes muitas vezes demoram para corrigir vulnerabilidades críticas; segundo a Check Point, 43% dos dispositivos comprometidos em 2024 estavam rodando firmware desatualizado.

Uso em botnets

Redes de ORBs estão sendo utilizadas para ataques DDoS massivos e anonimização de operações maliciosas, conforme identificado pela Microsoft, que reportou um aumento de 82% no uso dessas redes para ofuscação de ataques.

Como mitigar a ameaça?

- **Implementar segmentação de rede para reduzir a exposição desses dispositivos.**
- **Adotar monitoramento contínuo e análise de comportamento para detectar anomalias.**
- **Atualizar regularmente firmware e aplicações de segurança.**
- **Utilizar princípios de zero trust para restringir acessos indevidos.**
- **Reforçar políticas de logging e auditoria de dispositivos de borda.**

A exploração de dispositivos de borda e ORBs representa uma mudança estratégica na paisagem das ameaças cibernéticas. Organizações que não adotarem medidas proativas correm o risco de sofrer comprometimentos silenciosos e devastadores.

AS TECNOLOGIAS DE CIBER-SEGURANÇA EM 2025

Mais avançadas, integradas e autônomas

A evolução das ameaças digitais exige respostas cada vez mais inovadoras. Em 2025, a cibersegurança será impulsionada por inteligência artificial e automação preditiva, redefinindo a maneira como empresas protegem seus dados e infraestruturas. Soluções como *zero trust* dinâmico, detecção autônoma de anomalias e criptografia pós-quântica estarão no centro das estratégias defensivas.

Nesta seção, exploramos as principais tendências tecnológicas que moldarão o futuro da segurança digital e como sua organização pode se antecipar às novas ameaças que surgem com a automação e a inteligência artificial, garantindo resiliência contra ataques cada vez mais sofisticados.

Preparação para a era pós-quântica

A computação quântica ameaça reescrever as regras da segurança digital

A criptografia que protege comunicações, transações financeiras e dados sensíveis pode estar com os dias contados. A ascensão da computação quântica promete avanços sem precedentes, mas também representa um dos maiores riscos para a segurança digital. Em 2025, empresas precisarão acelerar sua transição para criptografia pós-quântica (PQC) para evitar o cenário "***Harvest Now, Decrypt Later***" — no qual atacantes armazenam dados criptografados hoje para decifrá-los quando os computadores quânticos atingirem sua maturidade.

A Gartner prevê que, a**té 2029, a maioria dos métodos de criptografia assimétrica será considerada insegura**, tornando obsoletos protocolos como RSA e ECC. Com a expectativa de que computadores quânticos práticos surjam nos próximos **5 a 10 anos**, governos e empresas precisam agir agora para evitar uma crise global de segurança de dados.

Como a computação quântica está evoluindo

Nos últimos anos, grandes *players* como Google, IBM e governos ao redor do mundo têm investido bilhões de dólares na computação quântica. Com isso, a criptografia tradicional enfrenta um período crítico de transição.

O NIST finalizou os primeiros padrões de criptografia pós-quântica em 2024, estabelecendo diretrizes para uma migração segura. No entanto, a adoção ainda é desigual: **apenas 30% das empresas já começaram a implementar soluções pós-quânticas, enquanto 52% ainda estão avaliando sua exposição ao risco quântico.**

Além disso, especialistas apontam que a migração completa pode levar até cinco anos, tornando essencial que empresas iniciem agora suas estratégias de transição.

OS RISCOS DA INAÇÃO

Quem será mais impactado?

A ameaça quântica coloca em risco setores que dependem de sigilo e integridade de dados, como:

Bancos e fintechs

Mais de 80% das transações financeiras dependem de criptografia assimétrica que será vulnerável a ataques quânticos.

Saúde e farmacêutico

Dados de pacientes e propriedade intelectual podem ser comprometidos, impactando milhões de pessoas.

Setor governamental e Defesa

Informações estratégicas podem ser descriptografadas décadas depois, comprometendo a segurança nacional.

Empresas de tecnologia e telecom

Até 2027, a maioria dos protocolos de segurança na nuvem precisará ser substituída por algoritmos resistentes a ataques quânticos.

Estratégias para a Era Pós-Quântica

Mapeie sua dependência de criptografia
Identifique onde e como sua empresa utiliza criptografia hoje.

Implemente a "criptoagilidade"
Garanta que seus sistemas possam alternar rapidamente para novos algoritmos pós-quânticos.

Adote os padrões do NIST
As novas diretrizes já estão disponíveis e devem ser incorporadas na infraestrutura de segurança.

Reforce a gestão de chaves criptográficas
Apenas 25% das empresas revisam regularmente suas políticas de criptografia; a recomendação é que isso seja feito com maior frequência.

Acompanhe os avanços da computação quântica
O desenvolvimento dessa tecnologia está acelerado, e empresas precisam estar prontas para agir rapidamente.

A computação quântica ainda não tornou a criptografia convencional obsoleta — mas quando isso acontecer, será tarde demais para reagir. Empresas que não se preparam correm o risco de perder a integridade de seus dados e enfrentar violações catastróficas. A Gartner estima que **até 2029, os ataques quânticos serão uma ameaça real**, e a migração para criptografia pós-quântica pode levar anos.

Em 2025, a transição para criptografia pós-quântica não será apenas uma vantagem competitiva, será uma necessidade estratégica.

O futuro da cibersegurança depende das decisões tomadas hoje.

Cloud Security First

A nova prioridade para a proteção digital

A crescente adoção da computação em nuvem transformou a maneira como empresas operam, mas também ampliou a superfície de ataque cibernético. De acordo com a Fortinet, 78% das organizações usam estratégias de nuvem múltiplas ou híbridas. Com isso, dados críticos e infraestruturas importantes agora estão em um ecossistema potencialmente mais vulnerável. Em 2025, a segurança na nuvem não será apenas uma preocupação secundária — **será a prioridade número um para empresas que desejam sobreviver no cenário digital**.

O aumento de **ataques a identidades na nuvem, falhas na cadeia de suprimentos digital e *ransomware*** impulsiona essa mudança. Segundo o Microsoft Digital Defense Report 2024, os ataques diários contra identidades na nuvem já superam **600 milhões**, tornando esse vetor um dos alvos mais críticos para cibercriminosos.

Com a crescente interconexão das empresas, qualquer falha na segurança da nuvem pode resultar em ataques em cascata, comprometendo setores inteiros e forçando regulações mais rígidas e obrigatórias para proteção de dados.

O que está mudando para superfícies já existentes?

Inicialmente, muitas empresas migraram para a nuvem visando **escalabilidade** e **redução de custos**, mas frequentemente negligenciaram medidas de segurança adequadas. Isso resultou em **configurações incorretas, acessos privilegiados excessivos e vulnerabilidades** exploradas por hackers.

A segurança na nuvem já era uma prioridade, mas a **abordagem defensiva** das organizações precisa evoluir para que acompanhe essas ameaças mais sofisticadas neste ano. Em 2025, espera-se um cenário complexo:

Ataques baseados em IA
O uso de inteligência artificial pelos atacantes está tornando as invasões mais rápidas e eficazes, explorando credenciais comprometidas e vulnerabilidades em tempo real.

Ransomware na nuvem
Agora, os hackers visam ambientes multi-tenant, explorando dependências entre sistemas para maximizar danos.

E quanto às novas superfícies de ataque?

Por outro lado, a evolução da tecnologia em nuvem trouxe **novas superfícies de ataque** que exigem outras estratégias. Algumas dessas superfícies apresentam riscos específicos, como:

Computação sem servidor (serverless)
Aplicativos serverless estão cada vez mais populares, mas criminosos também podem explorar esses ambientes. A Cloud Security Alliance já listou alguns dos principais riscos.

Integração de IA generativa
Com a adoção crescente de IA em soluções empresariais, novas vulnerabilidades estão surgindo em modelos de aprendizado de máquina hospedados na nuvem.

Expansão do Shadow IT
O crescimento de aplicativos SaaS utilizados sem a visibilidade e aprovação de TI expande a superfície de ataque e dificulta o monitoramento.

Diante desse cenário, o pensamento de Cloud Security First deixa de ser um diferencial e passa a ser um requisito para garantir a continuidade dos negócios.

Principais desafios e riscos

A nova onda de ameaças impõe desafios que as empresas precisarão enfrentar para evitar desastres digitais:

Comprometimento de identidades na nuvem

Criminosos exploram credenciais roubadas para acesso persistente.

Expansão do Ransomware-as-a-Service (RaaS)

Ataques à nuvem aumentam, impactando serviços críticos.

Exposição da cadeia de suprimentos digital

ataques a fornecedores comprometem ecossistemas inteiros.

Um estudo recente da Radware revelou que **69% das empresas admitiram que sofreram vazamentos de dados por conta de variações nas configurações de segurança**.

Recomendações para mitigação

- **Adotar o modelo Zero Trust: nunca confiar, sempre verificar acessos na nuvem.**
- **Implementar autenticação multifator (MFA) obrigatória para todas as contas críticas.**
- **Monitorar continuamente a infraestrutura de nuvem com ferramentas de detecção de ameaças baseadas em IA.**
- **Fortalecer a segurança na cadeia de suprimentos digital, exigindo certificações e auditorias de provedores.**
- **Gerenciar privilégios de acesso para evitar que credenciais comprometidas causem danos sistêmicos.**

A segurança da nuvem **não pode mais ser tratada como uma responsabilidade secundária**. Em 2025, organizações que não adotarem uma abordagem *Cloud Security First* correm o risco de sofrer **ataques devastadores**, **perda de dados e danos à reputação**.

A pergunta não é se sua empresa será alvo, mas quando. O futuro da cibersegurança está na nuvem — e o momento de agir é agora.

Plataformização da cibersegurança

O caminho para a eficiência e resiliência

A crescente complexidade das infraestruturas de segurança cibernética tem levado as organizações a reavaliar suas estratégias. Com empresas utilizando, em média, **60 a 70 ferramentas de segurança** e lidando com **10 a 15 fornecedores diferentes**, a necessidade de simplificação e integração se tornou uma prioridade estratégica. Essa fragmentação não apenas aumenta os custos operacionais, mas também cria desafios significativos para monitoramento, resposta a incidentes e conformidade regulatória.

Evolução da tendência e impactos esperados

Inicialmente, a abordagem tradicional de segurança cibernética focava na adoção de soluções pontuais para problemas específicos. No entanto, essa fragmentação resultou em complexidade excessiva, dificultando a detecção e resposta a ameaças. Em 2025, espera-se uma forte migração para plataformas consolidadas, que oferecem:

- **Maior integração e visibilidade sobre os eventos de segurança, reduzindo pontos cegos e melhorando a detecção de ameaças.**
- **Automatização aprimorada para resposta rápida a incidentes, reduzindo o tempo médio de detecção e mitigação de ataques.**
- **Redução de custos e simplificação operacional, eliminando soluções redundantes e reduzindo a sobrecarga das equipes de segurança.**
- **Facilidade de conformidade regulatória, garantindo que todas as políticas de segurança e privacidade sejam implementadas de maneira consistente em toda a organização.**

O conceito de ***Cybersecurity Mesh Architecture (CSMA)*** se consolida como a base para essa transição, permitindo que organizações combinem diferentes soluções de segurança dentro de um ecossistema unificado e interoperável. A arquitetura *mesh* permite que as equipes adaptem suas estratégias conforme necessário, sem comprometer a segurança ou a eficiência operacional.

O papel fundamental do framework na plataformização

A adoção de plataformas consolidadas deve ser guiada por um ***framework* estruturado**, que forneça diretrizes claras para implementação, governança e gestão da segurança cibernética. Um *framework* bem-definido garante que a consolidação não resulte apenas em uma redução no número de ferramentas, mas também em uma **abordagem estratégica** que fortaleça a postura de segurança da organização.

Os principais elementos de um ***framework* para plataformização** incluem:

Definição de objetivos claros

A plataforma deve atender às necessidades específicas da organização, equilibrando integração, eficiência e segurança.

Critérios de seleção de fornecedores

Avaliar interoperabilidade, escalabilidade e capacidade de adaptação às mudanças do ambiente digital.

Padrões de governança e conformidade

Garantir que a transição para plataformas consolidadas esteja alinhada com normas regulatórias e melhores práticas do setor.

Automação e resposta a ameaças

Implementação de processos automatizados para reduzir o tempo de resposta a incidentes e minimizar o impacto de ataques cibernéticos.

Monitoramento contínuo e ajustes estratégicos

Um framework robusto deve incluir métricas de desempenho e processos de revisão para otimizar a segurança continuamente.

Principais desafios e riscos

Dependência de um fornecedor único

A consolidação excessiva pode resultar em pontos únicos de falha, tornando a organização vulnerável a interrupções ou falhas na plataforma escolhida.

Ajustes na cultura organizacional

A migração para plataformas integradas exige treinamento contínuo e adaptação das equipes para lidar com novos fluxos de trabalho.

Possível perda de funcionalidades especializadas

Embora as plataformas ofereçam soluções abrangentes, algumas funcionalidades específicas podem não alcançar o mesmo nível de profundidade que ferramentas especializadas.

Complexidade na transição

A migração para uma plataforma consolidada pode demandar tempo e recursos significativos, além de exigir uma estratégia clara para minimizar impactos na operação diária.

A fragmentação excessiva das ferramentas de segurança tem criado desafios operacionais e dificultado a detecção e resposta eficaz a ameaças. Para enfrentar essa complexidade, organizações estão adotando plataformas integradas que combinam automação e inteligência artificial. De acordo com o relatório da Gartner Top Trends in Cybersecurity for 2025, empresas que combinam plataformas integradas com automação e inteligência artificial podem reduzir em **40% os incidentes de cibersegurança causados por erro humano até 2026**, reforçando a necessidade de consolidar soluções dentro de um framework estratégico bem-definido.

Recomendações para mitigação

- **Adotar um framework estruturado para orientar a transição para plataformas consolidadas, garantindo que a consolidação não comprometa a eficácia da segurança.**
- **Avaliar criteriosamente os fornecedores, garantindo interoperabilidade e flexibilidade para futuras mudanças, evitando aprisionamento tecnológico (vendor lock-in).**
- **Implementar automação e IA para reduzir falhas humanas, otimizar a resposta a incidentes e melhorar a detecção de ameaças.**
- **Criar um plano de transição gradual, evitando impactos negativos na operação e garantindo que todas as áreas da empresa estejam preparadas para a mudança.**
- **Manter uma abordagem híbrida: enquanto a consolidação de plataformas é essencial, manter algumas soluções especializadas para necessidades críticas pode ser a melhor estratégia para equilíbrio entre segurança e flexibilidade.**

A segurança cibernética deve evoluir continuamente para acompanhar a crescente sofisticação das ameaças digitais.

Em 2025, empresas que não adotarem a plataformização com um framework bem-estruturado correrão o risco de enfrentar lacunas críticas na sua postura de segurança.

Machine Identity

O elo perdido da segurança digital

A rápida digitalização das empresas trouxe um aumento exponencial no número de dispositivos conectados, *workloads* na nuvem e processos automatizados. Cada um desses elementos opera como uma entidade dentro do ecossistema digital, exigindo uma identidade própria para autenticação e autorização segura. No entanto, enquanto a segurança da identidade humana tem recebido grande atenção com autenticação multifator e *zero trust*, a identidade de máquina continua sendo um elo fraco e muitas vezes negligenciado. De acordo com a Garner, **54% das organizações notaram um aumento de vazamentos relacionados à identidade**, com uma em cada três sendo atingida por crescimento em interrupções de negócios, perdas financeiras ou penalidades regulatórias.

O problema da má gestão de identidades de máquina

Diferente das identidades humanas, que são protegidas por senhas, biometria e tokens de autenticação, as identidades de máquinas (como APIs, *workloads*, contêineres, servidores e dispositivos IoT) geralmente dependem de chaves estáticas, certificados ou credenciais armazenadas de maneira insegura. Muitas empresas falham ao gerenciar essas identidades corretamente, deixando credenciais expostas em código-fonte, sem políticas de rotação ou monitoramento adequado. Essa vulnerabilidade abre portas para ataques como falsificação de identidade de máquina (*machine-in-the-middle attacks*), roubo de certificados digitais e sequestro de credenciais para movimentação lateral dentro de redes corporativas. A própria IBM já apontou que houve um **aumento de 71% nos ataques que utilizaram credenciais roubadas ou comprometidas**.

O que há de novo para superfícies já existentes?

Mesmo que não seja novo, os desafios para o conceito de *Machine Identity* cresceram com a adoção massiva de computação e automação. Alguns dos avanços e preocupações mais recentes incluem:

Ataques mais sofisticados
A utilização de IA para comprometer credenciais de máquina tornou os ataques mais difíceis de detectar e mitigar.

Expansão do uso de APIs
APIs expostas e mal gerenciadas se tornaram alvos fáceis para ataques de sequestro de identidade de máquina.

Falta de visibilidade
A Gartner já apontou que essas máquinas "estão sendo criadas — para todos os lados — por diferentes equipes, e a maioria das organizações não as gerencia adequadamente.

A evolução do Machine Identity

Nos últimos anos, a explosão da nuvem e do IoT transformou a identidade de máquina de um problema técnico para uma preocupação estratégica de segurança.

As empresas que não implementarem políticas de gerenciamento de identidades de máquina enfrentarão desafios como o aumento no roubo de credenciais de máquinas e regulamentações mais rígidas, que pressionarão setores para garantir o total controle de suas identidades.

Expansão do IoT industrial
A crescente interconexão de dispositivos em ambientes críticos amplia os riscos de sequestro de identidade de máquina.

Computação sem servidor (serverless)
Ambientes dinâmicos e efêmeros tornam a gestão de identidades de máquina mais desafiadora.

Automação baseada em IA
Sistemas que tomam decisões autônomas precisam de autenticação forte para evitar comprometimentos.

Machine Identity Management (MIM) e a necessidade de automação

Para mitigar esses riscos, as organizações precisam adotar *Machine Identity Management* (MIM) — um conjunto de práticas e tecnologias voltadas para gerenciar e proteger identidades de máquina de forma automatizada. Também com as soluções de **Identidade Digital** da SEK, organizações podem implementar um controle seguro de acessos eficaz em ambientes complexos.

Além disso, companhias podem realizar ações como:

Emissão e rotação automatizada de certificados digitais, garantindo que workloads e dispositivos utilizem credenciais seguras e atualizadas.

Gestão centralizada de chaves e credenciais, reduzindo a exposição de segredos em código-fonte ou configurações inseguras.

Monitoramento contínuo e resposta a anomalias, identificando usos suspeitos de credenciais de máquina e evitando comprometimentos.

Com o crescimento da computação distribuída e do uso de APIs, essa abordagem se torna essencial para reduzir a superfície de ataque e garantir a confiabilidade das operações digitais.

Integração com zero trust e segurança em nuvem

O modelo *zero trust* prega que nenhuma identidade — seja humana ou de máquina — deve ser confiável por padrão. Isso significa que *workloads*, contêineres e dispositivos IoT precisam ser autenticados continuamente, seguindo princípios como *least privilege access* e segmentação dinâmica. Nesse contexto, a identidade de máquina tem um papel crítico, garantindo que apenas entidades autorizadas consigam interagir dentro de um ambiente protegido.

Além disso, provedores de segurança na nuvem estão incorporando práticas avançadas de *Machine Identity Protection*, integrando gerenciamento de certificados digitais e autenticação baseada em identidades para *workloads cloud-native*. Empresas que implementam essas soluções reduzem significativamente o risco de ataques baseados em falsificação de identidade e acesso não autorizado.

AI-DRIVEN CYBERSECURITY

A revolução da Defesa Digital em 2025

A cibersegurança está entrando em uma nova era. No ano passado, segundo dados da IBM, empresas economizaram, em média, US$ 2,2 milhões no custo de violações de dados com a utilização de IA na prevenção de ciberataques. Em 2025, **a Inteligência Artificial não será apenas uma ferramenta auxiliar, mas um agente central na defesa digital**. Segundo especialistas do Google Cloud, este será o primeiro ano em que veremos a segunda fase da IA na cibersegurança, com sistemas mais autônomos e capazes de antecipar ataques em tempo real. Empresas que adotarem IA para automação e resposta a ameaças estarão um passo à frente dos atacantes, reduzindo riscos e tempo de resposta de maneira inédita. A SEK já incorpora inteligência artificial e automatizações em suas soluções, utilizando análises avançadas para identificar e mitigar riscos em tempo real.

Evolução da tendência e impactos esperados

Até recentemente, a IA era usada para tarefas pontuais, como análise de logs e detecção de anomalias. Em 2025, entraremos na era das **operações semiautônomas de segurança**, em que a IA não apenas identifica riscos, mas também **prioriza alertas, recomenda respostas e executa ações corretivas automaticamente**.

Paralelamente à automação das operações de segurança, surgem avanços significativos com a adoção dos modelos de linguagem treinados especificamente para domínios (*Domain-Specific Language Models* – DSLMs). Segundo projeções da Gartner, até 2028, esses modelos especializados estarão presentes em **75% das soluções de segurança**, superando os modelos genéricos graças à capacidade superior de identificar ameaças específicas, reduzir falsos positivos e acelerar o processo decisório das equipes de segurança. Ao utilizar bases de conhecimento profundamente alinhadas ao contexto de atuação, os DSLMs proporcionam um aumento significativo da eficiência e assertividade das respostas a incidentes, fortalecendo a capacidade preventiva das organizações diante do avanço contínuo das ameaças baseadas em IA.

Outro impacto relevante será a transformação na **autenticação digital**. A tradicional autenticação baseada em senhas se tornará obsoleta, dando espaço a modelos de **autenticação contínua e multifator baseada em IA**, reduzindo drasticamente o impacto de identidades comprometidas.

Outro desafio emergente, impulsionado pelo crescimento da IA generativa, é a **segurança contra a desinformação**. Segundo a Gartner, até 2028, pelo menos 50% das empresas adotarão produtos ou serviços específicos para segurança contra desinformação, frente a menos de 5% em 2024. Essas tecnologias incluem detecção de *deepfakes*, monitoramento automatizado de redes sociais, proteção de reputação, além de ferramentas de verificação de fatos alimentadas por inteligência artificial.

Além disso, a crescente escassez de profissionais qualificados em cibersegurança exigirá que as empresas utilizem IA para suprir essa lacuna, especialmente diante do impacto dessa escassez no custo da violação de dados. Segundo dados da IBM em seu relatório Cost of Data Breach, houve um aumento de 26,2% em relação à escassez de profissionais de cibersegurança em 2024, o que ocasionou uma média de US$ 1,76 milhões a mais em custos de violação de dados.

Ao mesmo tempo, estima-se que **quase 50% das vagas relacionadas à IA não poderão ser preenchidas** por falta de talentos, tornando a automação de segurança uma necessidade, e não apenas uma opção.

Ao mesmo tempo, **a IA está transformando a função de TI**. Com sua capacidade de automatizar tarefas repetitivas, otimizar custos na nuvem e até mesmo escrever código, a IA está permitindo que as equipes de segurança e tecnologia se concentrem em inovação e estratégia, em vez de apenas gerenciamento operacional.

Principais benefícios da IA na cibersegurança

Redução no tempo de detecção e resposta

Sistemas baseados em IA serão capazes de identificar e mitigar ataques em minutos, eliminando ameaças antes que causem danos.

Zero Trust Inteligente

Modelos avançados de *Zero Trust* utilizarão IA para avaliar continuamente o comportamento do usuário e ajustar permissões em tempo real.

Segurança Autônoma

Ferramentas de *Security AI Ops* automatizarão investigações e correções, permitindo que analistas se concentrem em ameaças mais complexas.

Proteção contra deepfakes e fraudes avançadas

A IA ajudará na autenticação de comunicações empresariais, evitando golpes sofisticados baseados em falsificação digital.

O ano de 2025 marcará a ascensão da IA como **protagonista da defesa digital**, possibilitando que organizações atuem de forma **preditiva e proativa contra ameaças cibernéticas**. **Além disso, a própria TI será redefinida, com a IA assumindo um papel cada vez mais estratégico na segurança, automação e inovação**. Empresas que implementarem IA de forma inteligente não apenas fortalecerão suas defesas, mas também transformarão sua infraestrutura tecnológica, ganhando uma vantagem competitiva no mercado.

Caso de uso na SEK

A SEK já está à frente dessa tendência. O nosso SOC implementa IA de forma prática e mensurável em suas operações de cibersegurança por meio de um ecossistema de agentes inteligentes que otimiza a triagem, classificação e resolução de incidentes em tempo real, trazendo ganhos significativos para a operação de segurança.

Impacto no SOC da SEK

92% DE REDUÇÃO NO TEMPO DE RESPOSTA(MTTR)
de 6 horas para 28 minutos.

94% DE ECONOMIA NO TEMPO DE RECONHECIMENTO (MTTA)
de 2h32 para 4 minutos.

95,3% DOS CASOS RESOLVIDOS POR IA
reduzindo a necessidade de intervenção humana e melhorando a escalabilidade.

10 VEZES MAIS PRECISÃO
nas análises, com uma taxa de erro de apenas 0,27%.

O futuro da cibersegurança não será uma disputa entre humanos e máquinas, mas uma aliança entre ambos.

Governança de IA

O pilar essencial para segurança e confiabilidade em 2025

O avanço acelerado da inteligência artificial (IA) tem impulsionado inovações em diversos setores, mas também gerado desafios críticos de segurança e ética. Em 2025, com a crescente adoção da IA em áreas altamente reguladas, surge uma demanda urgente por **plataformas de governança de IA**. Essas soluções garantem que os sistemas de IA sejam justos, transparentes e responsáveis, evitando riscos como viés algorítmico, uso indevido de dados e falta de conformidade regulatória.

Evolução da tendência e impactos esperados

Nos últimos anos, o crescimento exponencial da IA levantou questões sobre responsabilidade e confiabilidade. Empresas que implementaram modelos de IA para automação de processos e tomada de decisão enfrentam desafios para assegurar que essas tecnologias operem de forma ética. Em 2025, espera-se que novas regulamentações e padrões globais aumentem a necessidade de plataformas dedicadas à governança de IA, permitindo um controle mais rigoroso sobre o desenvolvimento, treinamento e uso dos modelos.

Fatores que impulsionam essa evolução:

Expansão regulatória
Em fevereiro de 2025, entrou em vigor o Regulamento de Inteligência Artificial da União Europeia, estabelecendo um marco significativo para equilibrar o desenvolvimento tecnológico com a proteção dos direitos fundamentais.

Aumento de riscos reputacionais
Empresas envolvidas em escândalos de viés algorítmico ou decisões errôneas baseadas em IA enfrentam danos severos à sua imagem.

Complexidade dos modelos de IA
O uso crescente de redes neurais profundas e IA generativa torna mais difícil auditar e interpretar as decisões tomadas por esses sistemas.

Principais desafios e riscos

Embora as **plataformas de governança de IA** sejam essenciais, sua adoção traz desafios significativos:

Falta de padronização

Empresas enfrentam dificuldades para adotar frameworks de governança aceitos globalmente.

Riscos de viés algorítmico

Mesmo com governança, modelos de IA podem apresentar viés oculto, resultando em decisões injustas.

Monitoramento contínuo

Sistemas de IA precisam ser auditados constantemente para garantir conformidade com novas regulações e mudanças nos dados utilizados.

Impacto na inovação

Algumas organizações temem que regras rigorosas desacelerem a inovação, criando um dilema entre regulação e crescimento tecnológico.

Setores mais impactados.

Financeiro

Instituições bancárias e de crédito precisam garantir que decisões automatizadas, como aprovações de empréstimos, sejam justas e transparentes.

Saúde

Algoritmos que auxiliam diagnósticos médicos necessitam de auditorias rigorosas para evitar erros críticos.

RH

Sistemas de recrutamento baseados em IA podem reforçar vieses inconscientes, prejudicando diversidade e inclusão.

Recomendações para mitigação

Para garantir uma governança de IA eficaz, empresas devem adotar medidas estratégicas, como:

- **Implementar frameworks de IA responsável**
  Assegurar conformidade com regulamentos emergentes.
- **Criar times dedicados à governança de IA**
  Garantir auditorias regulares e transparência nos processos.
- **Utilizar ferramentas de monitoramento contínuo**
  Detectar e corrigir vieses algorítmicos em tempo real.
- **Investir em treinamento para equipes**
  Promover a conscientização sobre os riscos e desafios éticos da IA.

A governança da IA será um diferencial competitivo em 2025. Empresas que não priorizarem transparência, conformidade e ética correm o risco de enfrentar sanções regulatórias, perda de confiança do cliente e danos reputacionais. Em um cenário em que a IA está cada vez mais integrada à tomada de decisão, garantir que essas tecnologias operem de forma justa e responsável não é mais uma opção — é uma necessidade.

O fim da segurança por obscuridade em OT

Por muitos anos, infraestruturas de Tecnologia Operacional (OT) foram consideradas relativamente seguras devido ao seu isolamento. A falta de conectividade externa e o uso de sistemas proprietários criaram uma falsa sensação de proteção, levando muitas indústrias a negligenciar a segurança cibernética. No entanto, esse cenário mudou drasticamente. A crescente convergência entre IT e OT, a adoção acelerada de tecnologias emergentes e o acesso facilitado a ferramentas de exploração tornaram o setor industrial um alvo prioritário para cibercriminosos. Em 2025, **a segurança por obscuridade deixará de ser uma barreira eficaz, exigindo uma nova abordagem para proteger infraestruturas críticas**.

OT sob ataque: o aumento da superfície de risco

A expansão das redes industriais para a nuvem, o uso de sensores IoT e a necessidade de integração com sistemas corporativos abriram portas para novas ameaças. Antes, atacar um sistema OT exigia conhecimento técnico avançado e acesso físico, mas hoje, qualquer cibercriminoso com acesso à internet pode encontrar ferramentas *open source* para explorar vulnerabilidades em redes industriais.

Ataques como os realizados pelo grupo Sandworm contra infraestruturas críticas já demonstraram que OT não é mais um território intocado. Em 2025, a expectativa é que essa tendência se intensifique, com **grupos de *ransomware* e APTs ampliando sua atuação para ambientes industriais**, visando interromper operações e extorquir empresas.

Ferramentas open source estão democratizando os ataques a OT

A segurança por obscuridade perdeu força porque as barreiras técnicas que dificultavam ataques a sistemas industriais não existem mais. Bibliotecas para exploração de protocolos OT, ferramentas de engenharia reversa e *exploits* já estão disponíveis em repositórios públicos, permitindo que até atacantes menos experientes desenvolvam malware direcionado para esse setor.

Isso significa que **o risco não está mais restrito a ataques altamente sofisticados**. Criminosos comuns agora podem explorar redes industriais da mesma forma que invadem sistemas corporativos, utilizando ferramentas como Metasploit, Wireshark e *scripts* específicos para dispositivos SCADA e PLCs.

A convergência IT/OT e a ampliação dos vetores de ataque

A integração de sistemas industriais com redes corporativas eliminou uma das principais camadas de proteção de OT: o isolamento físico. Hoje, ameaças comuns ao ambiente IT, como *phishing*, credenciais vazadas e *ransomware*, já são portas de entrada para ataques a infraestruturas industriais.

Se antes um ataque a um servidor corporativo impactava apenas dados administrativos, agora ele pode comprometer **operações inteiras**, interrompendo a produção, manipulando processos industriais e causando danos físicos a equipamentos e até riscos à segurança humana.

O que as indústrias precisam fazer?

Com a segurança por obscuridade eliminada, as empresas precisam adotar uma abordagem proativa para proteger seus ambientes OT. Algumas ações essenciais incluem:

Implementar segmentação de redes
Garantir que ambientes IT e OT estejam isolados para limitar movimentações laterais de atacantes.

Adotar um modelo de segurança zero trust
Cada acesso à rede deve ser verificado e monitorado, reduzindo riscos de intrusão.

Proteger a cadeia de suprimentos
Exigir padrões mínimos de segurança de fornecedores para evitar brechas que possam comprometer a infraestrutura industrial.

Monitoramento contínuo com inteligência artificial
Implementar soluções de detecção de anomalias para identificar ataques em tempo real.

Fortalecer a segurança de protocolos industriais
Reduzir o uso de credenciais padrão e adotar criptografia para evitar interceptação de dados.

Capacitar equipes para resposta a incidentes
Treinamento contínuo para que operadores reconheçam e mitiguem ameaças rapidamente.

A era da segurança por obscuridade chegou ao fim. Em 2025, empresas que ainda confiam no isolamento como única defesa estarão mais vulneráveis do que nunca. A segurança em OT deve ser tratada com o mesmo nível de criticidade que a segurança em IT, exigindo **monitoramento contínuo, investimentos em proteção avançada e uma cultura de cibersegurança industrial**.

O futuro da segurança industrial dependerá de quem conseguir **se antecipar às ameaças e fortalecer sua resiliência digital**.

O futuro do hardware de IA

Potência computacional com eficiência energética

A demanda por inteligência artificial está impulsionando uma revolução no hardware, mas essa evolução traz um desafio crítico: o consumo de energia. Em 2025, a necessidade de ***AI embedded hardware*** mais eficiente e sustentável se tornará uma prioridade estratégica para empresas que querem expandir suas capacidades de IA sem comprometer custos operacionais e metas de sustentabilidade.

Evolução da tendência e impactos esperados

Nos últimos anos, vimos uma explosão no uso de IA generativa e aprendizado de máquina, levando a um aumento significativo no processamento de dados. Para sustentar esse crescimento, ***chips* especializados, como NPUs (*Neural Processing Units*) e processadores neuromórficos, estão sendo adotados** para permitir o processamento local da IA em dispositivos de borda, reduzindo a dependência de*t*.

Ao mesmo tempo, a preocupação com o impacto ambiental da computação cresce. Em resposta, **novas arquiteturas de hardware estão sendo desenvolvidas para otimizar a eficiência energética**, utilizando desde **processadores de baixa potência até fontes renováveis para alimentar infraestruturas de IA**. Empresas que não acompanharem essa transição enfrentarão custos elevados e desafios de escalabilidade.

Principais desafios e riscos

Aumento da demanda energética

Modelos de IA cada vez mais complexos exigem mais energia, tornando a sustentabilidade um fator competitivo.

Infraestrutura obsoleta

Empresas que dependem de hardware tradicional enfrentarão dificuldades para rodar aplicações de IA de forma eficiente.

Risco regulatório

Governos ao redor do mundo estão estabelecendo diretrizes para eficiência energética em TI, pressionando empresas a se adequarem.

Recomendações para mitigação

- **Investir em AI Embedded Hardware**
  Adotar NPUs e chips especializados para reduzir a carga em data centers e melhorar o desempenho de IA localmente.
- **Otimizar data centers**
  Implementar soluções de resfriamento mais eficientes e fontes de energia renováveis para reduzir o consumo energético.
- **Adotar computação híbrida**
  Utilizar abordagens combinadas de processamento local e em nuvem para equilibrar desempenho e sustentabilidade.

Em 2025, **a eficiência energética será um diferencial competitivo tão importante quanto a potência computacional**. Empresas que não inovarem nessa área correm o risco de ficar para trás, tanto em custos operacionais quanto em sustentabilidade.

Regulamentação e geopolítica

O novo campo de batalha da segurança cibernética em 2025

A segurança cibernética nunca esteve tão interligada com a **regulamentação global e o cenário geopolítico** como em 2025. À medida que governos reforçam leis para proteger infraestruturas digitais e regular o uso de novas tecnologias, conflitos internacionais ampliam o uso de ciberataques como armas estratégicas.

Neste contexto, **empresas e governos precisarão navegar por um ambiente regulatório mais rígido e se preparar para uma nova onda de ameaças cibernéticas derivadas das tensões geopolíticas**.

01.
Regulamentações de 2025 e seu impacto na segurança cibernética

A **complexidade regulatória** está aumentando globalmente, trazendo desafios e exigências para organizações que operam em múltiplas regiões. Algumas das regulamentações mais impactantes incluem:

Regulamentação dos Direitos dos Titulares de Dados (ANPD – Brasil)

A Autoridade Nacional de Proteção de Dados (ANPD) está avançando na regulamentação dos direitos dos titulares de dados, com previsão de conclusão ainda em 2025. Essa nova regulamentação reforça:

Transparência em decisões automatizadas e no uso de dados pessoais.

Direitos ampliados para usuários, aumentando as obrigações das empresas em termos de segurança da informação.

Impacto na proteção de dados corporativos, exigindo maior conformidade para evitar vazamentos e violações.

Novas regulamentações da União Europeia

A União Europeia continua a moldar o cenário global com legislações rigorosas, incluindo:

Digital Services Act (DSA)
Impõe regras mais rígidas para plataformas digitais, exigindo maior controle sobre desinformação e segurança cibernética.

Digital Operational Resilience Act (DORA)
Define padrões para resiliência cibernética no setor financeiro, aumentando exigências de testes e resposta a incidentes.

EU AI Act
Primeira legislação ampla sobre IA, impondo regras para o desenvolvimento e uso de sistemas de IA, incluindo restrições para uso malicioso em ataques cibernéticos.

Regulamentação da Inteligência Artificial e seu impacto na cibersegurança

O aumento do uso de **IA para ataques cibernéticos sofisticados** levou governos a desenvolverem leis para regular sua aplicação. Além do **AI Act da UE**, medidas emergentes nos **EUA e na China** estabelecem requisitos para transparência, segurança de dados e mitigação de riscos de IA generativa usada para desinformação ou ataques avançados.

A crescente importância da privacidade e conformidade regulatória

Com um número crescente de leis de proteção de dados, como **GDPR, LGPD e CPRA**, espera-se um ambiente regulatório ainda mais rigoroso em 2025. Organizações precisarão investir mais em **governança de dados, monitoramento de compliance e estratégias para evitar penalidades severas por não conformidade**.

02.

Geopolítica e cibersegurança: o digital como arma de guerra

Conflitos internacionais e rivalidades tecnológicas estão transformando **o ciberespaço em um campo de batalha**, aumentando a sofisticação e a frequência de ataques cibernéticos.

Espionagem digital e conflitos regionais

Tensões geopolíticas, como a **guerra na Ucrânia e disputas no Oriente Médio**, impulsionam o aumento de operações de espionagem cibernética, mirando **infraestruturas críticas, cadeias de suprimento e redes corporativas**.

Principais riscos para empresas

Ataques direcionados a setores estratégicos, como energia, telecomunicações e finanças.

Manipulação de informações e desinformação digital, impactando eleições e decisões políticas.

Uso de IA para aprimorar táticas de espionagem e ataques cibernéticos patrocinados por Estados.

Infraestruturas críticas sob ameaça

Infraestruturas como redes elétricas, transportes e telecomunicações tornaram-se alvos prioritários de ataques cibernéticos patrocinados por governos. Em 2025, espera-se um aumento de incidentes, incluindo:

- Ataques de *ransomware* e DDoS contra redes nacionais.
- Sabotagem digital em setores de energia e transportes.
- Comprometimento de cadeias de suprimento globais, afetando negócios e consumidores.

Desafios na cadeia de suprimentos e restrições tecnológicas

As disputas geopolíticas também impactam o fornecimento de tecnologia, com governos **banindo fornecedores estrangeiros e impondo restrições a chips, IA e telecomunicações**. Empresas precisarão se adaptar a um ambiente onde **sanções e barreiras comerciais podem afetar suas operações digitais**.

Disparidade na resiliência cibernética

Enquanto algumas regiões, como a **União Europeia e os EUA**, reforçam suas capacidades de defesa cibernética, outras — como partes da **América Latina e Ásia** — ainda enfrentam **desafios estruturais e falta de investimento em segurança digital**, tornando-se mais vulneráveis a ataques sofisticados.

03.
Como empresas devem se preparar?

Diante desse cenário de **novas regulamentações e riscos geopolíticos**, organizações precisarão **adotar estratégias mais robustas para garantir resiliência cibernética e compliance global**.

Monitoramento contínuo das regulamentações
Criar uma estrutura ágil para adaptar-se a mudanças legislativas sem comprometer a inovação.

Ciber-resiliência operacional
Investir em defesa contra ataques cibernéticos direcionados a infraestruturas críticas e cadeias de suprimentos.

Gestão estratégica de fornecedores
Evitar dependência de tecnologias restritas por sanções internacionais e diversificar fontes de tecnologia.

Educação e capacitação cibernética
Garantir que colaboradores entendam os riscos emergentes e possam agir rapidamente diante de ameaças.

Governança sobre IA e automação
Adotar boas práticas para proteção de modelos de IA e evitar seu uso em fraudes e manipulações digitais.

Cibersegurança além da tecnologia

As fronteiras digitais estão sendo redesenhadas pela regulamentação e pela geopolítica, tornando o ambiente cibernético mais complexo, regulado e propenso a ataques estratégicos.

Empresas que não investirem em resiliência cibernética e conformidade regulatória enfrentarão riscos crescentes, desde sanções financeiras até paralisação operacional por ataques digitais. Mais do que nunca, cibersegurança precisa ser um pilar estratégico para a sustentabilidade dos negócios no século XXI.

ESTRATÉGIAS PRÁTICAS E RECOMENDAÇÕES

Melhores práticas para CISOs gerirem riscos e defenderem seus orçamentos

A gestão de riscos cibernéticos e a defesa de orçamentos representam desafios complexos para os CISOs (*Chief Information Security Officers*), especialmente em um cenário onde as ameaças evoluem mais rapidamente do que as estratégias de defesa. Como vimos na retrospectiva de 2024, líderes de segurança enfrentaram pressões adicionais devido a incidentes como o vazamento de dados da Snowflake, que expuseram vulnerabilidades sistêmicas em organizações globalmente reconhecidas. Para navegar nesse ambiente, os CISOs precisam adotar abordagens que combinem priorização estratégica, comunicação eficaz e alinhamento com objetivos de negócio.

Construir uma narrativa de valor para a alta administração

Um dos maiores desafios enfrentados pelos CISOs é **demonstrar o retorno sobre o investimento** (ROI) em segurança. Embora o custo de não se proteger seja, muitas vezes, evidente apenas após um incidente grave, é fundamental que o CISO apresente métricas concretas e **estudos de impacto** para justificar gastos. **Exemplos práticos incluem:**

Projeção de prejuízos evitados

Apresentar cenários de riscos baseados em tentativas de ataques passadas, estimando quanto teria sido gasto em possíveis resgates, multas regulatórias ou perda de receita devido à indisponibilidade de sistemas.

Benchmarking setorial

Comparar o nível de investimento em cibersegurança com outras empresas do mesmo segmento de mercado.
Se a média de gastos em segurança representa 10% do orçamento de TI, por exemplo, mostrar a importância de se manter competitivo nesse indicador.

Indicadores de maturidade

Utilizar *frameworks* reconhecidos (por exemplo, NIST, ISO 27001) para evidenciar a posição da companhia em relação a boas práticas e apontar pontos que precisam de reforço.

Essa narrativa de valor tem maior aceitação quando o CISO utiliza linguagem de negócios, traduzindo ameaças cibernéticas em termos de risco financeiro e proteção da marca.

Alinhar a estratégia de segurança aos objetivos de negócio

Os incidentes mais recentes demonstram que as falhas, sejam de origem criminosa ou não, afetam **operações centrais** das organizações. Assim, uma boa governança de cibersegurança deve estar profundamente integrada ao **planejamento estratégico e às prioridades de cada área**. Boas práticas incluem:

Mapeamento de processos críticos
Identificar quais sistemas e fluxos de trabalho são essenciais, definindo prioridades de proteção e metas de disponibilidade para cada um.

Planejamento de contingência
Garantir planos de continuidade de negócios que cubram possíveis interrupções, como as vistas em casos de falhas globais, e que haja testes periódicos desses planos.

Envolvimento de stakeholders
Criar comitês de segurança, incluindo representantes de diferentes setores, para que decisões sobre orçamentos e políticas sejam tomadas de forma conjunta.

Equilibrar orçamento em relação ao cenário de ameaças

A abordagem de **balancear orçamento e riscos** permite que os CISOs alinhem investimentos em cibersegurança aos riscos reais do negócio, evitando subfinanciamento ou gastos excessivos. Em vez de seguir apenas *benchmarks*, essa estratégia prioriza recursos conforme a criticidade dos ativos, impacto financeiro de incidentes e probabilidade de ataques.

Os CISOs devem demonstrar à alta administração que segurança é um fator estratégico para a continuidade dos negócios. Modelos como **FAIR *(Factor Analysis of Information Risk)*** ajudam a quantificar riscos e justificar investimentos, garantindo um orçamento mais eficiente e defensável.

Priorizar investimentos com base no risco real
Alocar recursos para ameaças mais prováveis e com maior impacto operacional e financeiro.

Criar cenários de impacto financeiro
Demonstrar o custo potencial de incidentes versus o investimento necessário para mitigá-los.

Reservar orçamento para ameaças emergentes
Manter flexibilidade para responder a crises inesperadas e mudanças no cenário de ameaças.

Apoiar-se em métricas para ajustes contínuos
Monitorar indicadores para garantir que os investimentos tragam retorno real em segurança.

Ao equilibrar orçamento e risco, os CISOs otimizam recursos e tornam a cibersegurança um **investimento estratégico na resiliência do negócio**, e não apenas uma despesa operacional.

Fortalecer a gestão de riscos de terceiros (Third Party Risk Management – TPRM)

Os ataques à cadeia de suprimentos digital evidenciam que a segurança de uma organização não se limita aos seus próprios controles, mas depende diretamente da postura de seus **fornecedores e parceiros estratégicos**. Em 2024, o vazamento de dados de gigantes como Ticketmaster, ocasionado por conta da plataforma Snowflake, foi um dos destaques do ano, como visto na seção relacionada neste Think Ahead Report.

Essa ocorrência mostrou que ameaças podem se propagar de um fornecedor para toda a sua base de clientes, ampliando os impactos de um ataque. Os CISOs precisam adotar uma **abordagem mais rigorosa para gerenciar riscos de terceiros**, garantindo que vulnerabilidades externas não comprometam a segurança da organização. Para isso, boas práticas incluem:

Ganhar visibilidade sobre a cadeia de fornecedores

Mapear e categorizar os terceiros com acesso a dados e processos, priorizando os que representam maior risco. De acordo com a Gartner, 40% dos líderes de compliance apontam que 11% a 40% de seus provedores são de alto risco.

Implementar framework estruturado

definir um processo claro, com *frameworks* como NIST 800-161, ISO 27036 e CIS Controls ajuda a garantir que fornecedores sigam boas práticas.

Adotar monitoramento contínuo

Modelos tradicionais de avaliação periódica não acompanham a velocidade com que os riscos evoluem. É importante adotar monitoramento contínuo de ameaças.

Reforçar cláusulas contratuais

Estabelecer requisitos claros sobre proteção de dados, notificações de incidentes e responsabilidade em contratos, garante que fornecedores cumpram padrões mínimos.

Criar planos de resposta a incidentes em conjunto

Isso garante que haja uma coordenação eficiente para mitigar os impactos em caso de ataque.

A segurança da cadeia de suprimentos não pode ser um ponto cego na estratégia corporativa. **Fortalecer a gestão de riscos de terceiros proporciona mais maturidade e visão estratégica** para os CISOs e a organização.

Definir métricas e KPIs que demonstrem eficiência

Sem mensuração, é difícil avaliar o sucesso de qualquer iniciativa de segurança. Indicadores de desempenho claros, **periodicamente reportados**, ajudam na defesa do orçamento e no aprimoramento contínuo dos controles. Alguns exemplos:

MTTR (Mean Time to Respond/Recovery)
Indica a rapidez na resposta a incidentes e na recuperação de sistemas afetados.

Número de falhas de auditoria
Avalia quantas não conformidades foram identificadas em auditorias internas ou externas (como ISO 27001).

Taxa de treinamento dos usuários
Mensura quantos funcionários passaram por capacitações de segurança e como isso se reflete na diminuição de incidentes de *phishing* ou engenharia social.

Custo por incidente evitado
Calcula o investimento versus os prejuízos estimados caso o ataque fosse bem-sucedido.

Esses KPIs permitem mostrar, de forma quantitativa, a eficácia dos controles e, sobretudo, a economia potencial para a empresa.

Comunicar riscos em termos de impacto regulatório e reputacional

Como ficou evidente em diversos casos recentes, vazamentos de dados podem gerar efeitos catastróficos, que envolvem desde punições regulatórias até a perda de credibilidade no mercado. Por isso, o CISO deve:

Monitorar legislações e normas do setor em que atua (como LGPD e GDPR) e traduzir essas exigências em custos e riscos para o negócio.

Evidenciar o efeito na reputação ao não investir adequadamente em segurança: perder a confiança de clientes e parceiros muitas vezes pode gerar prejuízos de longo prazo, que superam qualquer gasto imediato.

Desenhar planos de resposta que incluam comunicação de crise, para que investidores e consumidores recebam informações transparentes em caso de incidentes.

Buscar parcerias e alianças estratégicas

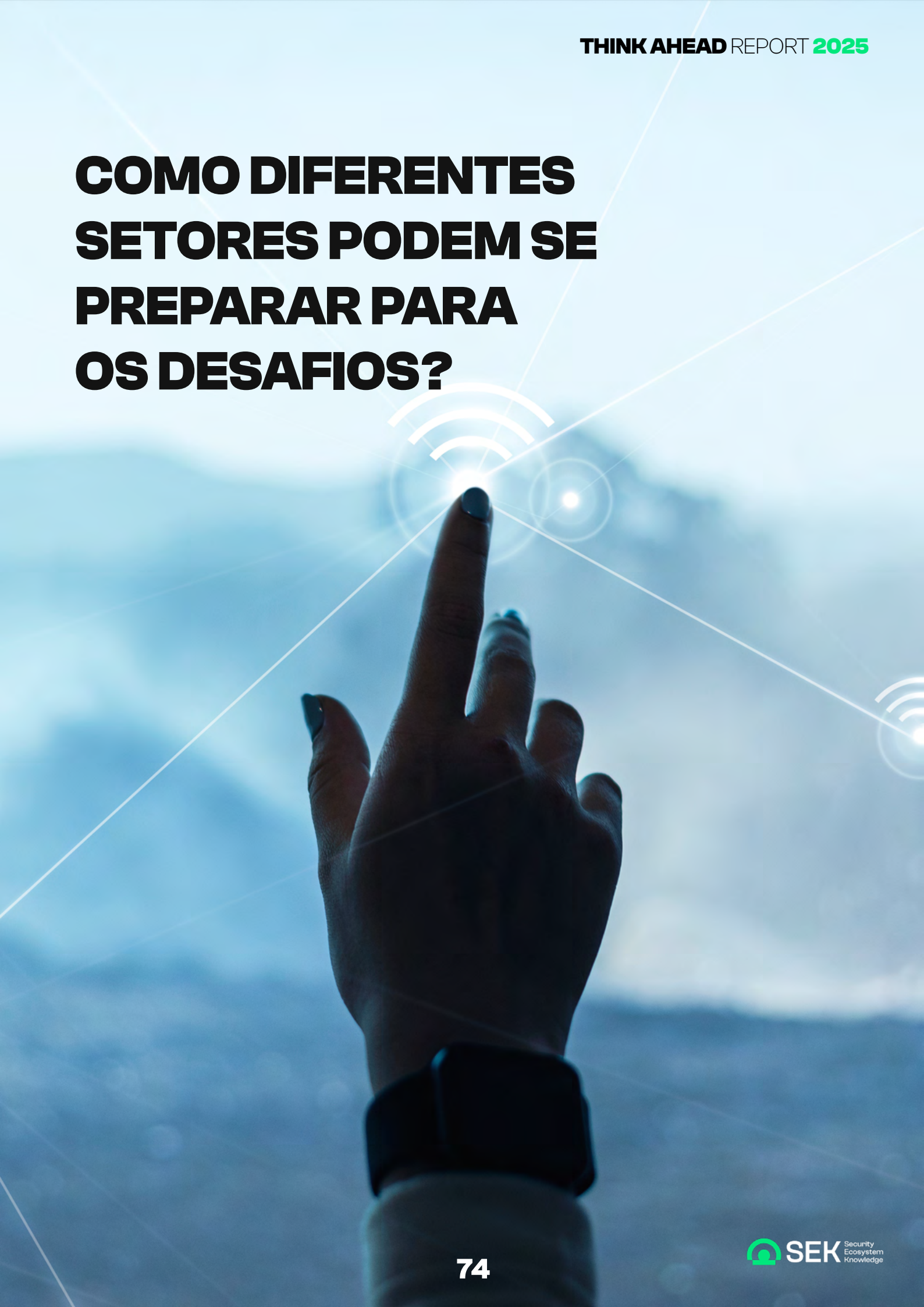
Alguns dos maiores incidentes mundiais em cibersegurança evidenciaram que até mesmo gigantes do setor precisam de **apoio externo**, seja de parceiros do ramo, fornecedores de soluções complementares ou mesmo de entidades governamentais que investigam e coíbem o cibercrime. Para os CISOs, construir alianças significa:

- **Compartilhar inteligência de ameaças** (*Threat Intelligence Sharing*) em fóruns e grupos confiáveis, antecipando tendências criminosas.
- **Negociar contratos de forma coletiva** ou buscar soluções integradas, o que ajuda a otimizar o orçamento e a implementar tecnologias de ponta.
- **Apoiar-se em consultorias e provedores especializados** para auditorias independentes e revisões de segurança.

Essas parcerias podem fortalecer a capacidade de resposta a incidentes e evidenciar uma visão estratégica ao conselho de administração.

No panorama atual, o CISO que deseja **gerir riscos de forma eficaz e defender seus orçamentos** precisa atuar como um **estrategista de negócios**, fazendo a ponte entre aspectos técnicos e resultados tangíveis. Ao alinhar a segurança aos objetivos corporativos, demonstrar ROI por meio de métricas claras e fortalecer a narrativa de valor, os profissionais de cibersegurança podem garantir maior resiliência organizacional diante de incidentes, sejam eles externos ou internos.

COMO DIFERENTES SETORES PODEM SE PREPARAR PARA OS DESAFIOS?



COMO DIFERENTES SETORES PODEM SE PREPARAR PARA OS DESAFIOS?

Nos últimos anos, o **panorama de cibersegurança** deixou claro que nenhuma organização está totalmente protegida contra incidentes capazes de **paralisar operações e comprometer a confiança** de clientes e parceiros. Ao mesmo tempo, notamos que cada setor apresenta riscos e necessidades muito específicos, exigindo **estratégias personalizadas** e ações coordenadas entre diferentes áreas da empresa. Entender como cada segmento pode se estruturar para os desafios de 2025 é fundamental para executivos que **desejam manter suas empresas resilientes**.

A proliferação de tecnologias emergentes, como a inteligência artificial, tem sido uma faca de dois gumes: enquanto oferecem avanços notáveis, também são exploradas por cibercriminosos para aprimorar suas fraudes e golpes.

A interdependência dos sistemas e a rápida evolução tecnológica aumentam o risco de **efeitos cascata** diante de qualquer brecha. Investir apenas em ferramentas não basta: **cibersegurança deve estar integrada à governança e à cultura organizacional**. Além disso, a pressão regulatória e as expectativas do mercado tornam a proteção de dados e a continuidade essenciais para a credibilidade. Embora práticas como treinamento, backups e *firewalls* sejam universais, **cada setor tem desafios próprios**: instituições financeiras enfrentam regulações rigorosas, enquanto organizações de saúde equilibram disponibilidade e proteção de dados. A seguir, apresentamos recomendações práticas para diferentes segmentos.

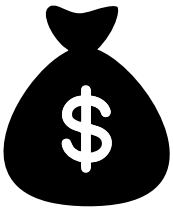
Setor industrial & de infraestrutura

O setor industrial, incluindo infraestruturas críticas, tem enfrentado um aumento significativo nos ciberataques direcionados a sistemas de OT, como visto na seção O fim da segurança por obscuridade em OT. De acordo com o Relatório Global 2024 sobre o Estado da Tecnologia Operacional e Cibersegurança da Fortinet, 73% das organizações sofreram invasões que afetaram sistemas de OT ou ambos. Além disso, o relatório destaca que quase um terço (31%) das empresas relataram mais de seis invasões em 2023, um aumento significativo em relação aos 11% do ano anterior.

Segregar redes de tecnologia operacional (OT) e tecnologia da informação (TI)
Isolar sistemas críticos impede que ataques em redes corporativas afetem operações industriais.

Implementar monitoramento contínuo de sistemas industriais
A detecção precoce de atividades suspeitas permite respostas rápidas a possíveis ameaças.

Atualizar regularmente sistemas e dispositivos industriais
Manter softwares e firmwares atualizados corrige vulnerabilidades conhecidas e fortalece a segurança.



Setor Financeiro

O setor financeiro tem sido um dos principais alvos de ciberataques, especialmente com o **aumento do uso de IA**, que tem potencializado a quantidade e a sofisticação das ameaças cibernéticas. Em 2024, observou-se um aumento significativo no uso de ***trojans* bancários** e fraudes relacionadas a **criptomoedas**, facilitados por técnicas avançadas de ***phishing*** aprimoradas por IA. Além disso, a prática de "***Phishing-as-a-Service***" tornou-se mais comum, permitindo que indivíduos com pouco conhecimento técnico realizem ataques eficazes.

Fortalecer a segurança contra trojans bancários
Relatórios indicam um aumento no uso de trojans bancários, especialmente aqueles que exploram vulnerabilidades em sistemas financeiros. Implementar soluções de detecção avançada e manter os sistemas atualizados são medidas essenciais.

Implementar autenticação multifator (MFA)
A adoção de MFA dificulta o acesso não autorizado, mesmo que credenciais sejam comprometidas, reforçando a segurança das transações financeiras.

Monitorar atividades relacionadas a criptomoedas
Com o aumento de fraudes envolvendo criptomoedas, é importante estabelecer sistemas de monitoramento para identificar transações suspeitas e proteger os investidores.

Utilizar inteligência artificial para detecção de fraudes
A mesma tecnologia que potencializa ataques pode ser empregada para identificar padrões anômalos e prevenir atividades fraudulentas.

Educar clientes sobre phishing e engenharia social
Campanhas de conscientização ajudam a reduzir o sucesso de ataques que visam enganar os usuários para obter informações sensíveis.

Estabelecer parcerias com empresas de cibersegurança
Colaborar com especialistas permite acesso a informações atualizadas sobre ameaças e a implementação de soluções de segurança mais robustas.

Setor Saúde

A transformação digital trouxe **avanços significativos** para o setor de saúde, mas também **expôs vulnerabilidades críticas** em termos de cibersegurança. No Brasil, a situação é particularmente alarmante: o país lidera em ataques cibernéticos na América Latina e está entre os cinco mais visados mundialmente. De acordo com pesquisa da Kaspersky divulgada em maio de 2024, foram registrados mais de 800 bloqueios diários de ataques de *ransomware* no setor de saúde brasileiro, totalizando mais de 106 mil tentativas desde janeiro, posicionando-o como **o terceiro mais atacado no ano**, com 6,5 mil tentativas. Além das **perdas financeiras**, esses ataques resultam em **atrasos em procedimentos** e testes, levando a desfechos adversos e com impacto direto na vida das pessoas.

Proteger dispositivos médicos conectados
A segurança de equipamentos IoT é vital para evitar que vulnerabilidades sejam exploradas, comprometendo dados de pacientes e operações clínicas.

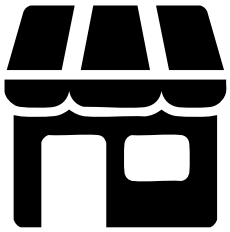
Implementar políticas rigorosas de controle de acesso
Garantir que apenas pessoal autorizado tenha acesso a informações sensíveis reduz o risco de vazamentos e manipulações indevidas.

Realizar auditorias regulares de segurança
Avaliações periódicas ajudam a identificar e corrigir vulnerabilidades antes que sejam exploradas por cibercriminosos.

Treinar funcionários para reconhecer ameaças cibernéticas
A educação contínua da equipe sobre práticas seguras e identificação de possíveis ataques fortalece a postura de segurança da organização.

Estabelecer planos de resposta a incidentes
Preparar-se para possíveis ataques garante uma reação rápida e eficaz, minimizando danos e retomando operações com agilidade.

Assegurar conformidade com regulamentações de proteção de dados:
Manter-se alinhado às leis e diretrizes vigentes evita penalidades e reforça a confiança dos pacientes na instituição.



Setor de Varejo & E-commerce

O varejo e o ***e-commerce*** têm sido alvos frequentes de ciberataques, especialmente com o aumento das transações online. Ataques de ***phishing*** **direcionados a consumidores e a exploração de vulnerabilidades em plataformas de pagamento** são algumas das ameaças enfrentadas.

Implementar sistemas avançados de detecção de fraudes
Utilizar ferramentas que monitoram transações em tempo real ajuda a identificar e prevenir atividades fraudulentas.

Assegurar a conformidade com padrões de segurança de dados de pagamento
Seguir normas como o PCI DSS é mandatório para proteger informações financeiras de clientes e evitar penalidades.

Realizar testes de penetração regularmente
Avaliar a segurança dos sistemas identifica vulnerabilidades que podem ser corrigidas antes de serem exploradas.

Implementar autenticação multifator para clientes e funcionários
Adicionar camadas de segurança dificulta o acesso não autorizado a contas e sistemas sensíveis.

Monitorar e proteger contra ataques de phishing
Estabelecer medidas para detectar e bloquear tentativas de phishing protege a reputação da empresa e a segurança dos clientes.

Educar clientes sobre práticas seguras de compras online
Fornecer orientações claras aumenta a confiança e reduz o risco de fraudes.

Setor de Telecomunicações

O setor de telecomunicações é fundamental para a infraestrutura digital, tornando-se um alvo atraente para cibercriminosos. Em janeiro de 2025, a multinacional espanhola Telefónica enfrentou um ciberataque que resultou no roubo de 2,3 *gigabytes* de dados, incluindo documentos internos e registros relacionados a clientes empresariais. Embora os dados de clientes residenciais não tenham sido comprometidos, o incidente destacou vulnerabilidades nos sistemas internos da empresa.

Para mitigar riscos como esse, é fundamental que as operadoras de telecomunicações implementem medidas robustas de segurança cibernética, incluindo a **segmentação** de redes, **monitoramento contínuo** de sistemas e **atualizações** regulares de software para corrigir vulnerabilidades conhecidas. Além disso, estabelecer **protocolos rigorosos de controle de acesso e promover uma cultura de cibersegurança** entre os funcionários são passos essenciais para fortalecer a resiliência contra ameaças cibernéticas. Outras medidas importantes incluem:

Implementar políticas de segurança cibernética abrangentes
Desenvolver e manter diretrizes claras alinhadas às melhores práticas internacionais, conforme exigido por organismos regulatórios.

Assegurar a conformidade dos equipamentos com requisitos de segurança
Garantir que todos os dispositivos utilizados atendam aos padrões mínimos estabelecidos pelos organismos regulatórios.

Notificar incidentes de segurança relevantes
Estabelecer procedimentos para informar ao órgão competente, outras operadoras e usuários sobre incidentes que afetem significativamente as redes e os dados dos clientes.

Bloquear comunicações fraudulentas
Implementar sistemas para detectar e impedir chamadas e mensagens suspeitas de fraude, incluindo aquelas com numeração não atribuída ou origem internacional falsificada.

Fortalecer a segurança de infraestruturas críticas
Reforçar a proteção de cabos submarinos e outras infraestruturas essenciais contra possíveis ataques, utilizando tecnologias avançadas de monitoramento.

Adotar comunicação criptografada para autoridades e funcionários
Utilizar aplicativos com criptografia de ponta a ponta para proteger comunicações sensíveis contra interceptações.

Conclusão

A segurança cibernética em 2025

Se os últimos anos foram uma escalada de ataques cada vez mais sofisticados, 2025 será um ano decisivo para a **construção de uma cibersegurança verdadeiramente resiliente**. Não se trata só de responder a ameaças conhecidas, o que já é importante, mas de **fortalecer a capacidade das empresas de resistirem**, se adaptarem e se recuperarem rapidamente diante de um cenário em que IA, *infostealers* e novas superfícies de ataque remodelam a dinâmica da segurança.

Este **Think Ahead Report 2025**, criado pela SEK, tem o propósito de oferecer uma **visão estratégica** para profissionais de TI, CISOs, empresas e toda a comunidade de cibersegurança, preparando-os para os desafios e oportunidades do próximo ano. O relatório é bem mais do que um levantamento de tendências.

A mensagem central é evidenciar a ciber-resiliência como uma necessidade para garantir a continuidade dos negócios e a proteção dos ativos digitais.

A **ascensão dos ataques impulsionados por IA** é um divisor de águas. O que antes exigia esforços humanos, agora pode ser automatizado, escalado e personalizado em um nível sem precedentes. Os atores de ameaça estão explorando a capacidade dessa tecnologia para otimizar seus vetores de ataque. E se 2024 foi o ano da experimentação, 2025 será o ano da consolidação de todas essas estratégias.

A **adoção da IA no setor de cibersegurança** passará a ser um ponto importante na defesa. O ataque sempre teve a vantagem da surpresa e da assimetria de custos. Mas se os defensores souberem explorar a IA para aumentar sua capacidade de resposta, essa balança pode finalmente começar a se equilibrar. A capacidade de resposta e continuidade operacional será a chave para transformar ameaças em oportunidades e fortalecer a postura de segurança a cada incidente superado.

No campo da segurança OT, o conceito de **"segurança por obscuridade" finalmente termina**. A dependência de métodos obsoletos e de segurança em sistemas legados coloca empresas em risco, especialmente quando falamos de infraestrutura crítica e dispositivos conectados. Além disso, à medida que **novas regulamentações** surgem e a **geopolítica cibernética** fica mais complexa, as empresas vão ter que se manter atentas e em **conformidade com as leis**, colocando-se também no papel de **líderes confiáveis** no mercado.

Para os **CISOs**, isso representa um novo desafio. Não basta mais implementar boas práticas técnicas. Será necessário justificar investimentos, provar ROI da segurança e garantir que a alta liderança compreenda que **cibersegurança não é uma despesa, e sim um diferencial competitivo**. Nesse sentido, a preparação contínua precisa ser vista como um pilar estratégico, integrando-se à **cultura organizacional** e garantindo que a empresa esteja sempre preparada para enfrentar o inesperado.

Se há uma lição que 2024 nos deixou, é que ninguém está imune, mas é possível estar preparado. **Em 2025, a cibersegurança será sobre quem tem a melhor estratégia**, a melhor capacidade de adaptação e os parceiros certos, não sobre quem tem a melhor tecnologia isolada.

SEK

O Think Ahead Report 2025 é apenas o começo.

As empresas que saírem na frente serão aquelas que transformarem essas previsões em ações concretas. Resiliência não é um destino, mas um processo contínuo de adaptação, fortalecimento e inovação.

E a SEK está aqui para ajudar.

Referências

Gartner - Top Trends in Cybersecurity for 2025

Gartner – Third-Party Risk Management Best Practices

World Economic Forum - Global Risks Report 2025

World Economic Forum – Global Cybersecurity Outlook 2025

Microsoft Digital Defense Report 2024

Fortinet – Cyberthreat Predictions for 2025

Fortinet - Estado da tecnologia operacional e cibersegurança de 2024

Google Cloud Cybersecurity Forecast 2025

Cloud Security Alliance - The 12 Most Critical Risks for Serverless Applications

IBM X-Force Threat Intelligence Index 2024

IBM – Cost of a Data Breach Report 2024

Kaspersky – State of ransomware in 2024

KnowBe4 - How a North Korean Fake IT Worker Tried to Infiltrate Us

Cloudflare – Cloudflare's Q3 DDoS report

Check Point – The State of Cyber Security 2025

Data Breaches Digest

Radware – Report: 69% of orgs report multicloud security configurations led to data breaches or exposures

THINK AHEAD REPORT 2025