Microsoft

Microsoft Digital Defense Report 2025
Resumo Executivo para Governos e Legisladores

Iluminando o caminho rumo a um futuro mais seguro

Um relatório Microsoft Threat Intelligence

Declaração introdutória de Amy Hogan-Burney e Igor Tsyganskiy (trecho do relatório completo)

Mobilizando para gerar impacto:

Liderança em cibersegurança em uma era decisiva

Amy Hogan-Burney
Vice-Presidente Corporativa, Customer Security & Trust

Igor Tsyganskiy
Vice-Presidente Corporativo e Chief Information Security Officer (CISO)

Vivemos um momento crucial para a cibersegurança. A transformação digital avança rapidamente, agora potencializada pela inteligência artificial, As ameaças cibernéticas passaram a representar riscos cada vez maiores para a estabilidade econômica e a segurança individual. Elas deixaram de ser questões puramente técnicas que afetavam apenas empresas e passaram a impactar diretamente diversos aspectos da vida em sociedade.

A velocidade com que o cenário de ameaças se transforma exige uma revisão profunda das defesas tradicionais. A adoção da IA, tanto por profissionais de segurança quanto por agentes mal-intencionados, está acelerando essa mudança. As organizações precisam adaptar seus sistemas, entender novas formas de ameaça e preparar suas equipes para acompanhar esse ritmo acelerado.

Além disso, as ameaças cibernéticas desempenham um papel cada vez mais significativo em conflitos geopolíticos e em atividades criminosas, ampliando, tanto em alcance quanto em complexidade, as responsabilidades dos profissionais de segurança. A IA será essencial para ajudar esses profissionais a lidar de forma eficaz com um cenário de riscos em expansão; ainda assim, é preciso avançar com cautela. Em um mundo centrado em IA, as ações, sejam das equipes de segurança, dos criminosos ou de estado-nação, tendem a gerar efeitos secundários cada vez mais rápidos e profundos. Considerar esses impactos em cadeia é fundamental ao implementar novos controles de segurança, compartilhar pesquisas, corrigir vulnerabilidades e fortalecer a colaboração entre organizações.

Os adversários, que incluem estados-nação, grupos criminosos e mercenários digitais, têm usado tecnologias emergentes para lançar ataques em volumes e precisões inéditos, muitas vezes explorando a própria confiança que sustenta nossas interações digitais. Por isso, a colaboração internacional entre os profissionais da segurança será decisiva para definir estratégias coordenadas e estabelecer normas globais que imponham consequências claras a ataques contra infraestrutura crítica e serviços essenciais.

Para os líderes de segurança, a mensagem é clara: a cibersegurança precisa ocupar um lugar central na estratégia organizacional e ser continuamente tratada como parte da gestão de riscos. Parcerias globais, inclusive entre empresas do mesmo setor e até entre concorrentes, devem ser fortalecidas para permitir uma proteção coordenada diante de adversários comuns. As antigas defesas de perímetro já não dão conta do cenário atual. É necessário incorporar resiliência desde o início: em sistemas, cadeias de suprimentos, processos e modelos de governança. Como novas ameaças surgirão em uma frequência cada vez maior, estar bem informado e preparado será determinante.

O que há de novo na edição deste ano

IA como uma necessidade defensiva e também um alvo

Adversários têm recorrido à IA generativa para ampliar a escala de ataques de engenharia social, automatizar movimentos laterais, acelerar a descoberta de vulnerabilidades e até empregar, em tempo real, técnicas de evasão a controles de segurança.

Malwares autônomos e agentes movidos por IA já conseguem ajustar suas táticas no momento da ação, o que exige que profissionais da segurança superem modelos de detecção estática e adotem estratégias baseadas em comportamento e defesa antecipatória.

Paralelamente, os próprios sistemas de IA se tornaram alvos estratégicos. Técnicas como injeção de *prompt* e envenenamento de dados vêm sendo usadas com mais frequência para comprometer modelos e sistemas, aumentando os riscos de ações não autorizadas, vazamentos de dados, roubo de informações e danos reputacionais.

Vetores de acesso inicial cada vez mais diversos

As campanhas de ataque atuais se organizam em cadeias multietapas que combinam engenharia social e exploração técnica. Neste ano, observamos a disseminação acelerada do "ClickFix", uma técnica de engenharia social que leva o próprio usuário a executar código malicioso, driblando proteções tradicionais contra *phishing*.

Também registramos o crescimento de métodos como *device code phishing*, utilizado tanto por grupos cibercriminosos quanto por estados-nação.

A ameaça crescente dos *infostealers*

Cada vez mais, os adversários não precisam "invadir": eles simplesmente entram. No ecossistema altamente especializado do cibercrime, acesso é um ativo central, e os *infostealers* se consolidaram como ferramentas essenciais para capturar credenciais e *tokens* vendidos posteriormente na *dark web*. Quem compra essas credenciais pode conduzir ataques subsequentes, como *ransomware*, exfiltração de dados ou extorsão.

O resultado é claro: organizações que sofrem infecções por *infostealers* ficam muito mais expostas a futuras violações.

Estados-nação ampliam suas operações

Objetivos geopolíticos continuam impulsionando o aumento de operações cibernéticas patrocinadas por Estados, com expansão significativa no direcionamento a setores como comunicações, pesquisa e academia. Essas operações seguem, em grande parte, dentro do escopo e volume esperados, focando no uso de espionagem cibernética contra alvos tradicionais para complementar atividades clássicas de inteligência. Seguindo tendências já observadas no ano passado, estados-nação têm acelerado o uso de IA para evoluir tanto suas operações cibernéticas quanto suas campanhas de influência, tornando-as mais escaláveis, avançadas e precisas.

Convidamos você a ler este relatório com foco prático. Ele não apenas descreve os desafios que enfrentamos e os que estão por vir, mas convoca governos, organizações e profissionais a se mobilizarem, se prepararem e responderem à altura.

Inovação, resiliência e colaboração são os pilares para um futuro digital seguro. Ao adotarmos esses princípios, podemos atravessar a incerteza e construir um mundo no qual a tecnologia nos capacita e nos protege diante da crescente onda de ameaças.

Amy Hogan-Burney
Vice-Presidente Corporativa,
Customer Security & Trust

Igor Tsyganskiy
Vice-Presidente Corporativo
e Diretor de Segurança
da Informação

Para acessar o relatório completo, visite: aka.ms/MDDR2025-PTBR

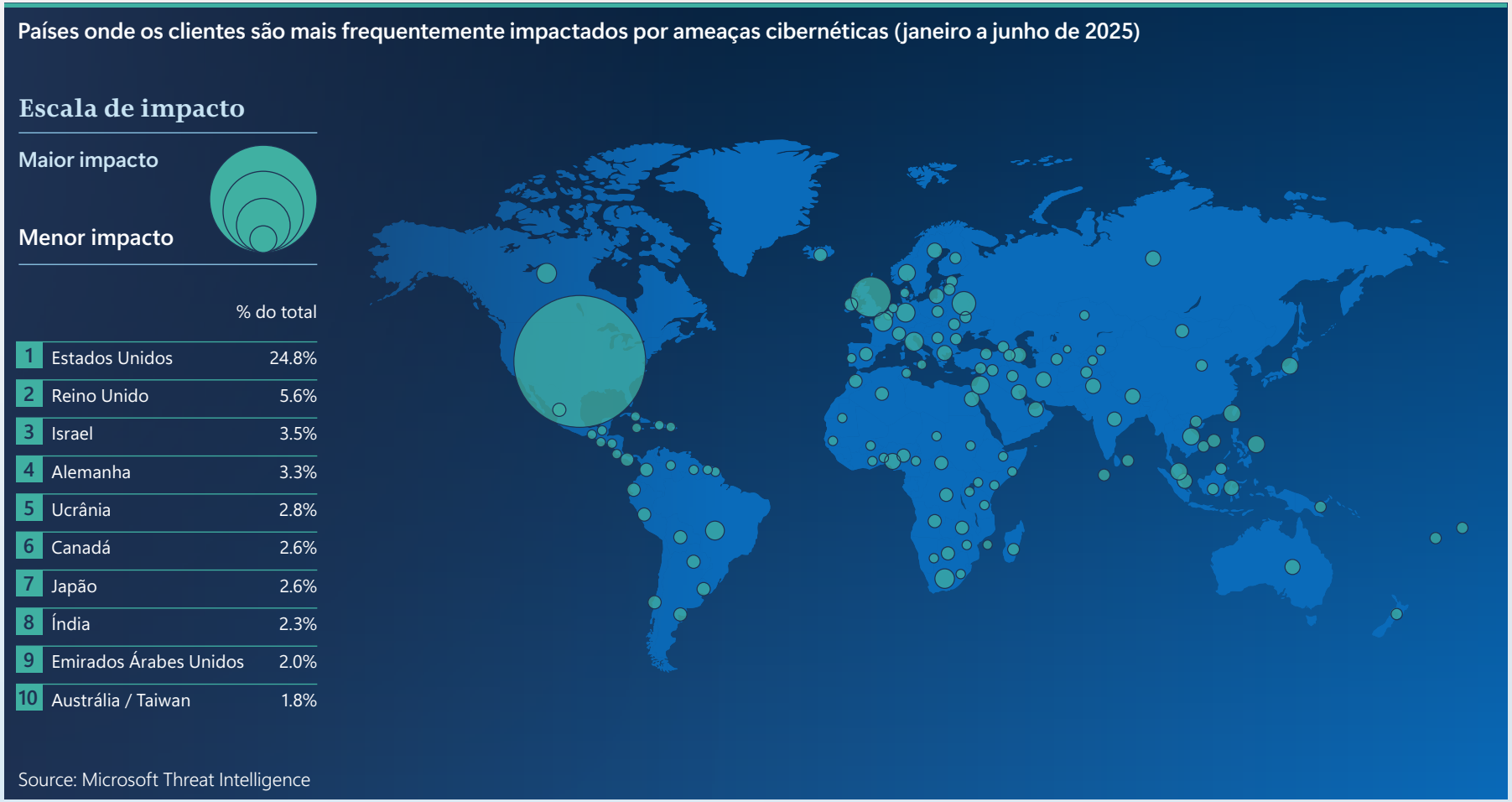
Como os agentes de ameaça estão moldando o ambiente de risco cibernético

O ano de 2025 marca um verdadeiro ponto de inflexão no cenário das ameaças digitais. Os ataques têm se caracterizado cada vez mais por velocidade, escala e sofisticação.

Analisando os últimos meses, fica claro que os agentes de ameaça vêm acelerando o desenvolvimento de técnicas inéditas, capazes de testar os limites das defesas que as organizações implementam para detectar e bloquear investidas maliciosas. Apesar disso, as ameaças que as empresas enfrentam no dia a dia permanecem, em sua maioria, as mesmas: ataques oportunistas conduzidos por agentes que exploram vulnerabilidades já conhecidas. Embora usuários do mundo inteiro estejam expostos, a maior concentração de ataques registrada nos últimos seis meses ocorreu nos Estados Unidos, Reino Unido, Israel e Alemanha.

Para acessar um mapa interativo com mais detalhes, visite: aka.ms/MDDR2025-PTBR

Países onde os clientes são mais frequentemente impactados por ameaças cibernéticas (janeiro a junho de 2025)



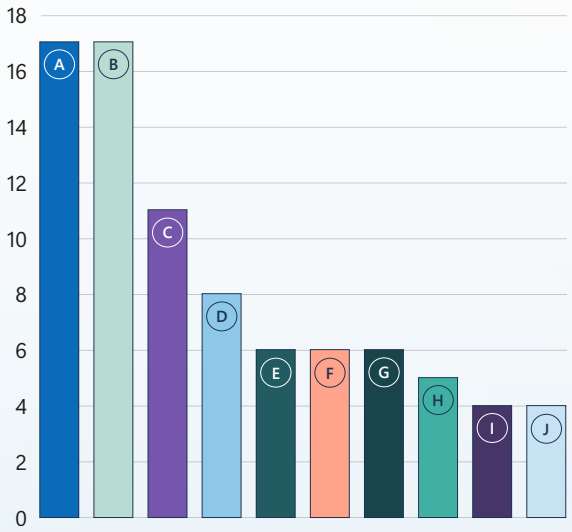
		% do total
1	Estados Unidos	24.8%
2	Reino Unido	5.6%
3	Israel	3.5%
4	Alemanha	3.3%
5	Ucrânia	2.8%
6	Canadá	2.6%
7	Japão	2.6%
8	Índia	2.3%
9	Emirados Árabes Unidos	2.0%
10	Austrália / Taiwan	1.8%

Source: Microsoft Threat Intelligence

Os adversários estão mirando organizaçoes por causa dos dados

Órgãos governamentais, empresas de TI e instituições de pesquisa e acadêmicas continuam entre os setores mais atingidos por ameaças cibernéticas, repetindo a tendência do ano passado. Essas organizações prestam serviços essenciais e concentram grandes volumes de dados sensíveis, incluindo informações pessoais identificáveis (PII) e *tokens* de autenticação, materiais que podem facilitar ataques subsequentes. A situação se agrava porque muitos desses órgãos, ONGs e instituições acadêmicas operam com sistemas legados, difíceis de atualizar e proteger, além de contarem com equipes de TI reduzidas e com capacidade limitada de resposta a incidentes. Essa combinação faz com que elas sejam alvos estratégicos tanto para agentes de estados-nação quanto para cibercriminosos em busca de lucro. Não surpreende, portanto, que o setor de Resposta a Incidentes da Microsoft e sua Equipe DART (Detecção e Resposta) tenham registrado coleta de dados em 79,5% das investigações reativas conduzidas no último ano.

Dez setores mais impactados por agentes de ameaça - nível global (janeiro a junho de 2025)



	%
A. Órgãos e serviços governamentais	17
B. Tecnologia da informação	17
C. Pesquisa e academia	11
D. Organizações não governamentais	8
E. Manufatura crítica	6
F. Sistemas de transporte	6
G. Varejo	6
H. Infraestrutura de comunicações	5
I. Serviços financeiros	4
J. Saúde e saúde pública	4

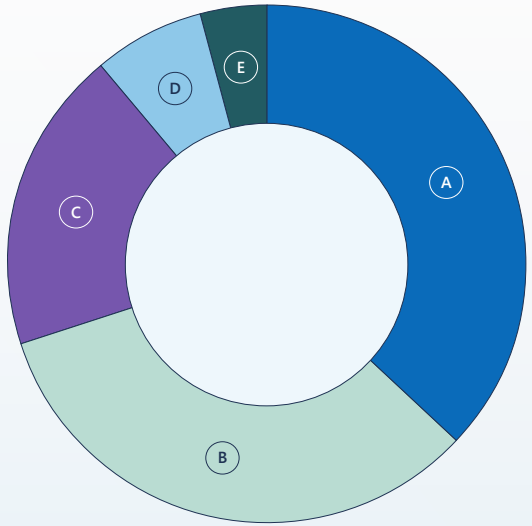
Fonte: Microsoft Threat Intelligence

A maior motivação para os ataques é financeira

A grande maioria dos ataques parte de cibercriminosos, e não de agentes de ameaça vinculados a estados-nação. Entre os incidentes investigados pela DART ao longo do ano, 33% envolveram extorsão, enquanto apenas 4% foram motivados por espionagem.

Casos envolvendo *ransomware* ou outros tipos de atividade destrutiva foram observados em 19% das ocorrências. Outro dado relevante é que 7% das organizações foram impactadas por ações de construção de infraestrutura, quando agentes mal-intencionados se aproveitam de ativos digitais não gerenciados para preparar ataques contra outros alvos ao longo da cadeia.

Motivações identificadas nos atendimentos de resposta a incidentes



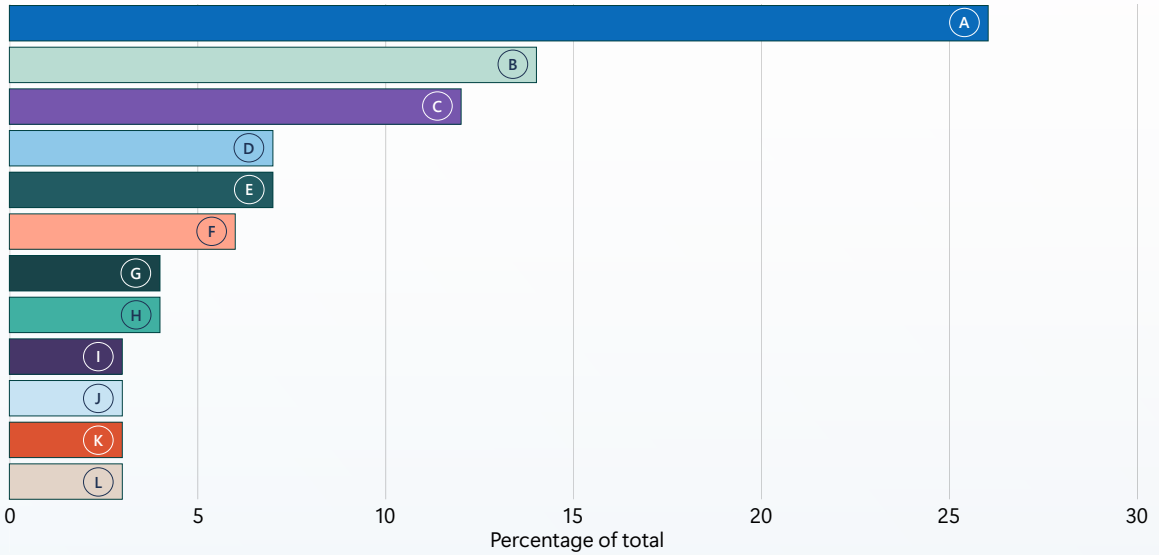
	%
A. Roubo de dados	37
B. Extorsão	33
C. Atividade destrutiva / *ransomware* operado por humanos	19
D. Construção de infraestrutura	7
E. Espionagem	4

Fonte: Equipe de Resposta a Incidentes, Detecção e Resposta da Microsoft

Agentes de estados-nação ampliam suas operaçoes, mas continuam focados em espionagem

Estados-nação vêm expandindo seu escopo de ataque tanto em volume quanto em alcance geográfico, concentrando a maior parte de suas ações no uso de espionagem cibernética para complementar operações tradicionais de inteligência.

Most-targeted sectors by nation-state actors



	Percentual do total
A. TI	26
B. Instituições de pesquisa e acadêmicas	14
C. Governo	12
D. *Think tanks* / ONGs	7
E. Varejo	7
F. Manufatura	6

	Percentual do total
G. Transporte	4
H. Comunicações	4
I. Serviços financeiros	3
J. Saúde	3
K. Defesa	3
L. Energia	3

Fonte: Dados de notificações relacionadas a estados-nação da Microsoft Threat Intelligence

Um ataque de *ransomware* com impacto global potencial foi interrompido em menos de dois minutos

Em fevereiro de 2025, a economia global esteve à beira de um colapso sistêmico quando uma grande empresa de transporte marítimo sofreu um ataque de *ransomware*. Se seus sistemas tivessem ficado offline por apenas algumas horas, o efeito cascata teria impactado o comércio e a indústria no mundo inteiro. Uma interrupção prolongada poderia ter paralisado o fluxo global de cargas.

Esse ataque ilustra claramente o risco do nosso mundo interconectado: um único ataque de *ransomware* contra uma empresa privada pode gerar consequências globais. Cadeias de suprimentos, físicas e digitais, ampliam a superfície de ataque, e organizações a milhares de quilômetros podem sentir os impactos de uma única intrusão bem-sucedida. Atividades cibernéticas maliciosas não são um problema apenas das vítimas diretas, mas um desafio que envolve toda a sociedade.

Apesar do cenário desafiador, este é um caso de sucesso, uma prova de que investimentos consistentes em cibersegurança funcionam. Graças ao comprometimento da empresa em proteger seus ativos digitais, o ataque foi contido rapidamente. O tempo entre a detecção e a interrupção foi de apenas 14 minutos, e o processo de criptografia foi interrompido um minuto e oito segundos após ter começado.

Com as proteções adequadas habilitadas, ataques de *ransomware* podem ser bloqueados ainda no início, sem que qualquer dado seja criptografado.

A foto é genérica e não representa nenhuma empresa específica, seja do passado ou do presente.

Destaques de estados-nação

China

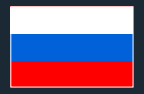
A China continua ampliando sua atuação em múltiplos setores para fins de espionagem e roubo de dados sensíveis. Agentes ligados ao Estado têm recorrido cada vez mais a parcerias com organizações não governamentais (ONGs) para expandir suas capacidades, além de utilizarem redes clandestinas e dispositivos expostos à internet para obter acesso e evitar detecção. Eles também estão mais rápidos em operacionalizar vulnerabilidades recém-divulgadas.

Três setores mais visados por agentes chineses (% do total):

– TI (23%), Governo (10%), *Think tanks* / ONGs (9%), Manufatura (9%)

Três regiões mais visadas por agentes chineses (% do total):

Estados Unidos (35%), Tailândia (14%), Taiwan (12%)



Rússia

A Rússia continua concentrando seus esforços na Ucrânia, mas ampliou seu escopo para atingir pequenas empresas em países que apoiam a Ucrânia, possivelmente utilizando esses alvos menores como pontos de acesso para, depois, alcançar organizações maiores. Além da Ucrânia, os dez países mais afetados são todos membros da OTAN, um aumento de 25% em relação ao ano passado. Os agentes russos também estão recorrendo cada vez mais ao ecossistema do cibercrime.

Três setores mais visados por agentes russos (% do total): Governo (25%), Instituições de pesquisa e acadêmicas (13%), *Think tanks* / ONGs (13%)

Três regiões mais visadas por agentes russos (% do total): Estados Unidos (20%), Reino Unido (12%), Ucrânia (11%)

Irã

O Irã está mirando uma variedade mais ampla de alvos do que nunca, do Oriente Médio à América do Norte, como parte da ampliação de suas operações de espionagem.

Recentemente, três agentes iranianos vinculados ao Estado atacaram empresas de logística e transporte marítimo na Europa e no Golfo Pérsico para obter acesso contínuo a dados comerciais sensíveis, levantando a possibilidade de que o país esteja se preparando para adquirir capacidade de interferir em operações de navegação comercial.

Três setores mais visados por agentes iranianos (% do total): TI (21%), Instituições de pesquisa e acadêmicas (15%), Governo (8%)

Três regiões mais visadas por agentes iranianos (% do total): Israel (64%), Estados Unidos (6%), Emirados Árabes Unidos (5%)

Coreia do Norte

A Coreia do Norte continua centrada em geração de receita e espionagem.

Em um movimento que tem chamado atenção global, milhares de profissionais de TI norte-coreanos trabalhando remotamente têm se candidatado a vagas em empresas ao redor do mundo, enviando seus salários ao governo como remessas.

Quando descobertos, alguns desses trabalhadores passaram a recorrer à extorsão como outra forma de gerar dinheiro para o regime.

Três setores mais visados por agentes norte-coreanos (% do total): TI (33%), Instituições de pesquisa e acadêmicas (15%), *Think tanks* / ONGs (8%)

Três regiões mais visadas por agentes norte-coreanos (% do total): Estados Unidos (50%), Itália (13%), Austrália (5%)

Amostra regional dos níveis de atividade de estados-nação observados

Contagem de eventos observados por país

- Mais de 200 eventos
- 100-200
- 50-100
- 0-50

Américas

Maiores níveis de atividade

Estados Unidos	623
Canadá	51
Brasil	24
Peru	16
Argentina	11
Colômbia	10
México	9
República Dominicana	5
Chile	4
Costa Rica	3

Ásia e Pacífico

Maiores níveis de atividade

Taiwan	143
Coreia	126
Índia	100
Hong Kong (RAE)	95
China	49
Austrália	47
Tailândia	39
Japão	38
Singapura	33
Indonésia	32

Europa

Maiores níveis de atividade

Ucrânia	277
Reino Unido	144
Polônia	97
Alemanha	74
França	72
Espanha	61
Rússia	60
Itália	51
Azerbaijão	35
Bélgica	30

Oriente Médio e África

Maiores níveis de atividade

Israel	603
Emirados Árabes Unidos	166
Arábia Saudita	70
Turquia	70
Iraque	67
Jordânia	44
Líbano	39
Egito	32
Irã	27
Marrocos	26
África do Sul	31
Etiópia	20
Angola	9
Quênia	9
Nigéria	8
Tanzânia	5
Mali	4
Namíbia	4
Botsuana	2

IA: uma solução e vulnerabilidade

À medida que adversários passam a explorar o potencial da IA, os profissionais de segurança também precisam fazer o mesmo. Embora ainda recente, o impacto da IA já é significativo: graças às proteções baseadas nessa tecnologia, provedores relatam neutralizar automaticamente a grande maioria dos ataques baseados em identidade. Com o apoio da IA, as equipes de segurança conseguem agir antes que um ataque cause danos, reduzindo falsos positivos ou falhas de detecção, e tornando as defesas muito mais ágeis e inteligentes.

O leque de aplicações defensivas da IA é amplo. A tecnologia pode analisar ameaças, identificar vulnerabilidades e lacunas de detecção, validar alertas, reconhecer ataques de *phishing homóglifos*, automatizar processos de remediação e aplicação de patches, além de proteger usuários mais expostos. Agentes de IA, em particular, já ajudam a conter incidentes ao reagirem automaticamente — suspendendo contas suspeitas, iniciando redefinições de senha e limitando um ataque antes que ele evolua. Eles também reforçam políticas internas, monitoram credenciais, permissões e comportamentos de aplicativos e controlam acessos de funcionários.

Ainda assim, seu uso traz riscos: há ameaças que miram diretamente sistemas de IA e seus usuários, e outras que surgem justamente graças às novas capacidades que a tecnologia oferece.

A amplificação dos ataques cibernéticos pela IA

O uso malicioso da IA sempre foi inevitável, mas agora ele ocorre em escala sem precedentes. Adversários vêm usando IA generativa para impulsionar desde ataques de engenharia social até análises de dados e técnicas de evasão de controles de segurança em tempo real. *Malwares* autônomos e agentes movidos por IA já conseguem ajustar suas táticas no calor do momento, exigindo que os defensores abandonem modelos de detecção estática e adotem estratégias baseadas em comportamento e defesa antecipatória.

Nos últimos seis meses, operações de influência impulsionadas por IA cresceram rapidamente. Também surgiram atores *"AI-first"*, inclusive ligados a estados-nação, que priorizam conteúdos e ferramentas gerados por IA, deixando para trás os métodos tradicionais de manipulação.

Os governos precisam assumir a liderança na proteção da IA aplicada à defesa nacional. Isso significa criar e fazer cumprir políticas robustas, incentivar inovações em cibersegurança projetadas para a era da IA e fortalecer parcerias entre o setor público e o privado. Esse esforço inclui regular a IA ao longo de todo o seu ciclo de vida, promover padrões globais, investir na capacitação da força de trabalho e usar a segurança como motor de desenvolvimento econômico — tudo isso enquanto ampliam a cooperação internacional para enfrentar ameaças emergentes.

*

Na era *"AI-first"*, usar IA para defender a IA deixa de ser apenas necessário, torna-se uma vantagem estratégica.

Storm-2139: um caso emblemático de exploração e abuso de IA

Enquanto impulsionam a inovação, a Microsoft e outros provedores globais de IA trabalham para manter princípios de uso responsável. A ação da Digital Crimes Unit (DCU) contra o grupo Storm-2139 mostra como a colaboração entre setor público e privado pode moldar esse caminho e desmantelar os abusos de cibercriminosos.

Em julho de 2024, a Microsoft identificou uma rede global que usava chaves de API roubadas para contornar sistemas de segurança de diferentes serviços populares de IA, incluindo o Azure OpenAI. Os desenvolvedores por trás da operação criavam e vendiam ferramentas maliciosas capazes de gerar milhares de imagens abusivas, como *deepfakes* de celebridades, conteúdo sexualmente explícito e materiais sintéticos violentos, misóginos ou que continham discursos de ódio. Usando tecnologias de proveniência de conteúdo e inteligência de código aberto, a DCU conseguiu rastrear a origem das atividades. A rede incluía criadores que desenvolviam softwares para burlar proteções de IA, distribuidores que personalizavam e revendiam essas ferramentas e usuários finais que geravam o conteúdo sintético abusivo.

Para interromper a operação, a DCU adotou uma estratégia em duas etapas. Em dezembro de 2024, abriu uma ação civil para apreender e redirecionar o domínio usado pelo Storm-2139 para coordenar suas atividades. A medida revelou novas evidências, permitindo uma petição ampliada em fevereiro de 2025, que identificou os principais desenvolvedores e distribuidores.

Em março de 2025, a Microsoft apresentou uma série de denúncias criminais ao Departamento de Justiça dos EUA (DOJ), ao FBI, à Agência Nacional do Crime do Reino Unido (NCA) e ao Centro Europeu de Crimes Cibernéticos da Europol (EC3).

Lições para formuladores de políticas públicas

- O abuso de IA é real e global.
- A IA generativa está sendo usada como arma, e é premente que os governos mundo afora fortaleçam suas regulamentações.
- A interrupção legal funciona.
- Ações civis podem desmontar infraestruturas cibercriminosas de forma eficaz.
- A colaboração internacional é indispensável.
- Encaminhamentos entre países demonstram a necessidade de forças-tarefa conjuntas e inteligência compartilhada.
- Proveniência e inteligência *open-source* são ferramentas-chave.
- Rastrear abusos gerados por IA exige investimento em tecnologias de detecção e atribuição.
- A regulação precisa cobrir toda a cadeia de abuso.
- Da criação ao uso final, é essencial regular o desenvolvimento, a distribuição e a aplicação de ferramentas maliciosas de IA.
- Parcerias público-privadas são essenciais.
- Os esforços coordenados entre governo e indústria permitirão enfrentar as ameaças habilitadas por IA.

O trabalho da DCU ao lado de autoridades internacionais mostra como o conhecimento técnico do setor privado pode fortalecer a capacidade de investigação e punição do setor público. Governos devem institucionalizar e ampliar esse tipo de cooperação, especialmente em áreas emergentes como abuso de IA e mídias sintéticas.

Fortalecendo a resiliência cibernética global por meio de regulação e colaboração

Em um cenário em que violações de segurança deixaram de ser uma possibilidade para se tornarem uma questão de tempo, a resiliência e a capacidade de recuperação ganham importância vital. À medida que sistemas digitais se conectam cada vez mais a estruturas burocráticas, órgãos governamentais e infraestruturas críticas, nos níveis nacional e internacional, ser resiliente significa também garantir que serviços essenciais continuem funcionando, mesmo diante de interrupções. A construção da resiliência exige uma abordagem holística: proteger infraestruturas, gerenciar crises independentemente de sua origem e assegurar continuidade nos âmbitos empresarial, governamental e social.

A resiliência precisa ocorrer em múltiplos níveis, do nacional ao internacional, alinhando capacidades, compartilhando inteligência e coordenando respostas. Só por meio de colaboração integrada e proativa é possível criar sistemas não apenas seguros, mas também capazes de se adaptar, absorver impactos e manter serviços essenciais em operação.

Governos ao redor do mundo têm avançado rapidamente na criação de políticas, leis e regulações voltadas a mitigar riscos cibernéticos e fortalecer a resiliência. No último ano, três tendências se destacaram nas prioridades governamentais:

1. **Expansão regulatória e execução**
   Diversos países implementaram ou aprimoraram regulações abrangentes de segurança cibernética baseadas em responsabilidade, gestão de risco e comunicação rápida de incidentes. Essas normas incluem medidas obrigatórias de conformidade, exigências de governança e mecanismos de supervisão, consolidando a migração de diretrizes voluntárias para padrões obrigatórios.
2. **Reforço da segurança na cadeia digital de suprimentos**
   Governos também passaram a impulsionar requisitos destinados a proteger toda a cadeia de suprimentos das tecnologias digitais. Novas regulações determinam princípios de *secure by design*, exigem transparência via *Software Bills of Materials* (SBOMs) e estabelecem monitoramento pós-comercialização mais robusto.
3. **Evolução da cooperação internacional das regulamentações**
   Onde antes os países dependiam sobretudo de parcerias pontuais e do compartilhamento informal de informações, o último ano marcou o primeiro caso de reconhecimento mútuo formal de requisitos de segurança cibernética entre nações. Esse avanço reflete a percepção crescente de que ameaças digitais ignoram fronteiras e exigem respostas harmonizadas.

Apesar dos benefícios, essas iniciativas também podem gerar inconsistências entre jurisdições, aumentando complexidade e custos e, ao mesmo tempo, diminuindo o nível geral de segurança. Por isso, governos que desejam reduzir riscos e fortalecer a resiliência devem priorizar normas e padrões que promovam aprendizado contínuo, interoperabilidade global e responsabilização. Além disso, regulações devem seguir abordagens iterativas, orientadas por risco e focadas em processos e resultados.

Avançando esforços multissetoriais para paz e segurança no ambiente digital

O aumento de conflitos cibernéticos estimulou um movimento global de cooperação, com países atuando na ONU e em outros fóruns para construir e sustentar um conjunto comum de regras que orientem o comportamento responsável no espaço digital. Para que esses debates avancem, é fundamental a participação de atores não governamentais, especialmente a indústria e a sociedade civil, capazes de oferecer expertise tecnológica e destacar o impacto humano das operações ofensivas conduzidas por Estados-nação. Como resultado, as instituições multilaterais precisam evoluir para garantir uma participação multissetorial adequada, inclusive nos diálogos sobre cibersegurança conduzidos pela ONU.

Diferentemente de domínios tradicionais de conflito e cooperação entre países, como controle de armamentos ou leis marítimas, o ciberespaço é majoritariamente criado, operado e transformado pelo setor privado. E está evoluindo rapidamente. Qualquer arcabouço internacional voltado à paz e estabilidade online precisa levar isso em conta, garantindo que aqueles que constroem e sustentam o ambiente digital participem das discussões sobre comportamento estatal responsável. O encerramento recente do mandato do Grupo de Trabalho Aberto da ONU sobre Segurança Cibernética (OEWG) abre uma oportunidade crucial para repensar como os próximos diálogos internacionais serão estruturados, modelos tão dinâmicos quanto o próprio ambiente digital que pretendem regular. Nesse sentido, a Microsoft reforça a importância de:

- **Criar um mecanismo permanente e mais orientado à ação dentro da ONU:** Por mais de duas décadas, diferentes grupos de trabalho forneceram espaços para debater comportamento estatal responsável no ciberespaço. Mas o avanço futuro exige uma estrutura mais ágil e contínua dentro da ONU, baseada em normas claras, expertise técnica e participação significativa de atores não governamentais, sem depender do consenso absoluto entre todos os Estados-membros para emitir orientações.
- **Aprimorar regras existentes e expandi-las quando necessário:** Iniciativas como o projeto político do Tribunal Penal Internacional sobre crimes digitais e o Emblema Digital da Cruz Vermelha demonstram que princípios do direito internacional já podem ser aplicados ao ambiente digital, desde que haja vontade política, clareza institucional e capacidade operacional. Da mesma forma, as 11 Normas Voluntárias para o Comportamento Estatal Responsável no Ciberespaço constituem salvaguardas essenciais que precisam ser aplicadas e protegidas. Mas novas normas também devem ser continuamente desenvolvidas para acompanhar o ritmo da evolução digital. Serviços comerciais de nuvem, por exemplo, tornaram-se tão fundamentais ao cotidiano que deveriam ser reconhecidos como infraestrutura crítica internacional e, portanto, imunes a ataques cibernéticos por parte de Estados-nação.
- **Institucionalizar o diálogo multissetorial sobre IA, segurança e ética:** A *Roundtable for AI Security and Ethics* (RAISE), liderada pelo UNIDIR com apoio da Microsoft e outras organizações, é um exemplo de iniciativa contínua que evidencia o valor de um diálogo sustentado entre setores sobre riscos de IA em contextos de segurança. Órgãos da ONU poderiam replicar e fortalecer iniciativas semelhantes, alinhando capacidade técnica e desenvolvimento de políticas públicas e promovendo inovação responsável por meio da colaboração inclusiva.

Dissuasão em prática: criando consequências para agentes estatais

À medida que infraestruturas essenciais, água, alimentos, saúde, comunicações, transporte, se tornam cada vez mais dependentes de sistemas digitais, operações cibernéticas conduzidas por estados-nação contra esses recursos deixam de ser toleráveis. Isso é ainda mais grave quando envolve o pré-posicionamento para futuros ataques disruptivos ou destrutivos.

Apenas reforçar a defesa dessas infraestruturas dificilmente basta para conter estados-nação adversários. Como essas ações têm motivação política, exigem respostas políticas. Proteger infraestruturas críticas, instituições democráticas e sistemas civis significa criar mecanismos claros que mostrem que atividades maliciosas que violem normas internacionais terão consequências equivalentes.

No último ano, cresceu de forma notável o reconhecimento da importância dessa dissuasão cibernética. Governos e setor privado têm se alinhado cada vez mais para responder a incidentes maliciosos. Entre os avanços recentes:

- A **OTAN** desenvolveu arcabouços de atribuição baseados em coalizões e passou a explorar contramedidas coletivas. Em julho, divulgou uma declaração conjunta reconhecendo e condenando atividades maliciosas atribuídas à Rússia pelos países membros.
- Os **EUA** publicaram declarações contundentes, denúncias criminais e atribuições de ataques feitas em coordenação com aliados.
- A **União Europeia** tem recorrido com mais frequência à sua Cyber Diplomacy Toolbox e ao regime de sanções para responsabilizar agentes mal-intencionados, embora a aplicação ainda varie entre os estados-membros.
- Esses passos criam uma base importante para avançar. Para consolidar um arcabouço mais robusto de dissuasão cibernética, governos com visões convergentes deveriam trabalhar para:
- **Tornar as atribuições públicas mais regulares.** Estados precisam emitir declarações de atribuição de forma consistente, aproveitando informações compartilhadas por parceiros e pelo setor privado, sempre indicando se normas ou leis internacionais foram violadas em um incidente cibernético.
- **Estabelecer limites.** É fundamental deixar explícito que diferentes tipos de atividade maliciosa, da espionagem ao pré-posicionamento e a operações disruptivas ou destrutivas, acarretarão respostas progressivamente mais severas.
- **Aplicar consequências variadas.** As respostas não devem ficar restritas ao ciberespaço nem seguir um único modelo. Atores distintos são sensíveis a diferentes tipos de pressão: sanções econômicas, medidas diplomáticas, exposição pública, demonstrações de postura estratégica ou desclassificação seletiva de informações.
- **Proibir retaliações pelo setor privado.** Empresas privadas não têm legitimidade nem condições para conduzir contra-ataques a estados-nação, e fazer isso pode aumentar o risco de escalada. O setor privado deve contribuir com processos de atribuição e cooperar com governos, mas apenas o Estado pode impor consequências por condutas ilícitas no plano internacional.

Construir um modelo eficaz de dissuasão cibernética é essencial para preservar a estabilidade do ambiente digital e exigirá novas soluções diplomáticas e de governança nos próximos anos. É por isso que a Microsoft apoia pesquisas conduzidas pelo Royal United Services Institute (RUSI), que buscam caminhos inovadores para conter e desestimular atividades maliciosas online.

Lidando com facilitadores geopolíticos das operaçoes de *ransomware*

Muitos dos grupos de *ransomware* mais ativos conseguem operar sem enfrentar consequências, atacando vítimas em outros países enquanto seus próprios governos simplesmente ignoram suas ações. Seja por manterem vínculos diretos com o Estado ou porque autoridades permitem que atuem livremente. O efeito é o mesmo: a criação de "Estados de abrigo seguro", que toleram ataques no exterior e violam normas internacionais de *due diligence*, segundo as quais governos devem impedir atividades cibernéticas ilegais dentro de seus territórios.

Diante desse cenário, combater operações de *ransomware* exige não apenas medidas técnicas, mas também um esforço internacional mais coordenado e uma pressão política que responsabilize governos pelo apoio direto ou indireto a esses grupos. Uma das estratégias possíveis é classificar certos Estados como patrocinadores de *ransomware*, assim como acontece com Estados que patrocinam o terrorismo, com os estigmas e penalidades correspondentes. Isso criaria incentivos claros para que esses governos enfrentem os grupos que operam dentro de suas fronteiras.

Outras ações podem reforçar essa resposta global:

- **Ações legais:** *Ransomware* é uma forma de extorsão que, na maioria dos países, já viola leis existentes. Aplicá-las de forma rigorosa é fundamental. Ao reconhecer Estados como patrocinadores de *ransomware*, civis também poderiam buscar reparação em tribunais contra esses governos após um eventual ataque.
- **Parcerias público-privadas:** É essencial fortalecer a cooperação entre o setor privado e as forças de segurança para ampliar a capacidade de resposta ao cibercrime. Iniciativas como a *International Counter Ransomware Initiative* (CRI) e a *Ransomware Task Force* do Institute for Security and Technology (IST) são bons exemplos desse modelo.
- **Consequências impeditivas:** Governos precisam definir com clareza o que constitui um comportamento responsável no ambiente digital, e reforçar essa definição com consequências progressivas, em diferentes frentes, capazes de desestimular ataques patrocinados ou tolerados por Estados.

Combatendo cibermercenários: fechando as brechas na regulação global

Os cibermercenários, empresas privadas que vendem capacidades ofensivas no ciberespaço, operam em áreas cinzentas da lei, muitas vezes além das suas fronteiras. Seu alcance transnacional e a ausência de supervisão efetiva dificultam o rastreamento e a responsabilização, permitindo que atuem com quase total impunidade. Muitos ainda recorrem a *rebranding* constante, mudanças de jurisdição e redes financeiras complexas para escapar da regulação.

Para enfrentar essa ameaça crescente, governos e setor privado precisam trabalhar juntos de maneira mais estruturada para desmantelar o mercado que sustenta essas atividades. Isso inclui ampliar o compartilhamento de inteligência, coordenar respostas e criar regulações mais robustas. Normas internacionais também devem proibir o uso de cibermercenários e acabar com as brechas legais que permitem sua atuação. Em muitos casos, será necessário impor limitações rigorosas, ou até proibições completas, a esse mercado, assegurando que seus produtos, incluindo *spyware*, não sejam usados em violação à lei, a direitos humanos ou à segurança de produtos tecnológicos.

Alguns países já vêm adotando medidas efetivas nesse sentido. Os Estados Unidos restringiram o uso de serviços de cibermercenários por agências federais e proibiram empresas que atuam de forma irresponsável, impactando diretamente o faturamento desses fornecedores. No Reino Unido e na França, houve avanços importantes na condução do Pall Mall Process, um fórum internacional com mais de 20 governos membros que busca regular as Capacidades Comerciais de Intrusão Cibernética (CCIC) por meio de estruturas compartilhadas. Em abril de 2025, o processo resultou na criação de um Código de Conduta inédito para orientar governos a limitar os danos associados às CCICs.

A transparência é um pilar essencial. Governos devem expor fornecedores e intermediários, aplicar sanções e dar o exemplo ao não recorrer a cibermercenários. O setor privado, por sua vez, precisa reforçar a segurança das plataformas, monitorar abusos e agir rapidamente para desarticular operações desse tipo. Com *due diligence* e colaboração, é possível reduzir significativamente o espaço de atuação dos cibermercenários, protegendo a segurança nacional, os direitos humanos e a estabilidade digital global.

Tecnologias quânticas: uma prioridade estratégica na nova era da competição

As tecnologias quânticas, que abrangem computação, comunicações e sensoriamento, estão se tornando pilares essenciais para a segurança econômica e nacional do futuro.

Seu potencial para acelerar descobertas científicas, permitir novos marcos em comunicações seguras e transformar profundamente a criptografia colocou esse campo entre as maiores prioridades globais. Não por acaso, governos de todo o mundo já tratam a tecnologia quântica como um imperativo nacional. Tanto aliados quanto adversários estão investindo em programas de pesquisa e desenvolvimento (P&D) e fortalecendo seus ecossistemas acadêmicos e empresariais para disputar essa liderança.

Hoje, empresas privadas já conduzem grande parte do P&D quântico e estão no centro da corrida global por essas tecnologias. Esse protagonismo também atrai a atenção de atores hostis, que podem direcionar esforços para atingir programas corporativos de P&D, startups e *spin-offs* acadêmicos. Por isso, é fundamental estabelecer salvaguardas sólidas e uma preparação estratégica desde agora, antes que as tecnologias quânticas se tornem amplamente operacionais. Os riscos e as oportunidades são enormes: liderar o campo quântico pode definir não só vantagens competitivas, mas também o futuro da integridade das comunicações seguras e da economia digital global.

As implicações da corrida pela vantagem quântica são vastas:

- **Liderança científica e industrial:** Tecnologias quânticas podem impulsionar uma nova onda de inovação em química e ciência de materiais.
- **Impacto na criptografia:** Um computador quântico suficientemente avançado pode quebrar algoritmos de chave pública amplamente utilizados, comprometendo a segurança de comunicações e dados.
- **Superioridade em sensoriamento:** Sensores quânticos podem detectar ativos furtivos aéreos ou navais, enfraquecendo estruturas de dissuasão estratégica.
- Os governos têm um papel decisivo na construção de um futuro *quantum-safe*, em estreita colaboração com o setor privado e por meio de políticas eficazes. Para acelerar essa preparação, recomenda-se que os governos:
- **Estabeleçam a segurança quântica como prioridade nacional de cibersegurança.** A criptografia resistente a ataques quânticos deve ser tratada como um imperativo estratégico e incorporada aos marcos nacionais de cibersegurança.
- **Alinhem estratégias de segurança quântica entre jurisdições.** Políticas públicas, normas e cronogramas de transição devem ser harmonizados. O G7 pode liderar esse alinhamento, ampliando seu trabalho em criptografia pós-quântica no setor financeiro para abranger estratégias mais amplas de segurança quântica.
- **Adotem padrões internacionais.** É essencial apoiar o desenvolvimento de padrões globais e evitar abordagens regionais fragmentadas que prejudiquem interoperabilidade, inovação e segurança.
- **Definam cronogramas antecipados e graduais.** A ação deve começar antes de 2030. Nos EUA, por exemplo, a política CNSSP-15 exige que todos os novos produtos e serviços destinados a sistemas de segurança nacional utilizem algoritmos resistentes a ataques quânticos a partir de janeiro de 2027.
- **Liderem pelo exemplo com planos de transição transparentes.** Governos devem publicar e atualizar periodicamente seus roteiros de transição, com cronogramas, marcos e orçamentos, para facilitar o compartilhamento de conhecimento e boas práticas.
- **Ampliem a conscientização e a capacitação profissional.** É necessário informar o público e setores críticos sobre riscos e preparação quântica, além de investir em formação profissional para apoiar a transição para um ecossistema *quantum-safe*.
- **Modernizem pela adoção da nuvem.** A migração para a nuvem deve ser vista como um habilitador estratégico. Plataformas em nuvem podem acelerar a transição ao incorporar capacidades de segurança quântica, reduzindo o esforço individual de cada organização.

Conclusão

À medida que marcos regulatórios globais evoluem e novas tendências legislativas redefinem o cenário da cibersegurança, uma verdade permanece inalterada: a segurança é uma responsabilidade compartilhada.

Governos, líderes do setor privado, sociedade civil e usuários individuais desempenham papéis essenciais na construção de um ecossistema digital resiliente. As análises e dados apresentados ao longo deste relatório reforçam a urgência da colaboração, não apenas entre países, mas também entre os setores e disciplinas.

Nosso compromisso em iluminar o caminho para um futuro mais seguro vai além de um tema de campanha, trata-se de um apelo à ação. Acreditamos que transparência, interoperabilidade e padrões harmonizados são pilares fundamentais do progresso. Seja por meio de nossa inteligência contra ameaças, atuação em políticas públicas ou inovações de engenharia, buscamos fortalecer tanto quem defende quanto quem toma decisões.

Obrigado por ler o Microsoft Digital Defense Report deste ano. Convidamos você a explorar nossos materiais complementares, compartilhar seu feedback e se juntar a nós na construção de um mundo digital mais seguro e confiável.

Microsoft

Microsoft Digital Defense Report 2025

Iluminando o caminho para um futuro mais seguro

Para mais notícias sobre cibersegurança, acesse:
microsoft.com/corporate-responsibility/cybersecurity

Para mais informaçoes sobre o relatório, visite:
aka.ms/MDDR2025-PTBR

Para acompanhar novidades em políticas de cibersegurança, siga o nosso LinkedIn:
aka.ms/MOILinkedin

Para insights e tendências voltados a líderes de segurança, acesse:
www.microsoft.com/security/security-insider

Um relatório Microsoft Threat Intelligence
Outubro de 2025