SECURITY REPORT

AMÉRICA LATINA (EDIÇÃO 2026)

Cenário de cibersegurança em empresas
da América Latina (com dados sobre o Brasil)

Progress. Protected.

Conteúdo

Sobre o ESET Security Report

O **ESET Security Report (ESR)** é um relatório anual elaborado pela ESET que oferece uma visão geral do estado da cibersegurança nas empresas da América Latina.

O ESET Security Report (ESR) 2026 oferece um diagnóstico da cibersegurança corporativa na América Latina com base em **1.563 respostas** de profissionais do setor. Para garantir a consistência estatística, a análise concentrou-se exclusivamente nos **10 países da região** que atingiram o número mínimo de participantes. **Entre eles está o Brasil, que recebe uma análise específica sobre o cenário nacional em algumas seções deste relatório**. Os participantes representam aproximadamente **962 organizações distintas**, validadas por meio de seus domínios institucionais.

A amostra apresenta um alto nível de especialização: **80,7% dos participantes atuam diretamente na área de cibersegurança** (analistas, técnicos, gerentes e diretores), garantindo uma visão técnica e fundamentada sobre as infraestruturas avaliadas. Os **19,3% restantes correspondem a colaboradores de áreas não técnicas**, contribuindo com uma perspectiva relevante sobre os hábitos e práticas de segurança dos usuários finais. Em relação aos setores representados, os participantes pertencem principalmente às áreas de Governo e Informática/Tecnologia, seguidas por segmentos estratégicos como Bancário e Financeiro, Educação e Saúde.

Com base nesses dados, o relatório analisa o índice de ciberataques em comparação com as lacunas de visibilidade, os principais vetores de intrusão, como o phishing, as lacunas regulatórias e a percepção de risco em relação à Inteligência Artificial, a adoção de ferramentas de proteção e a segurança em ambientes móveis corporativos. O resultado é um retrato fiel do cenário regional, que contribui para apoiar a tomada de decisões estratégicas em cibersegurança.

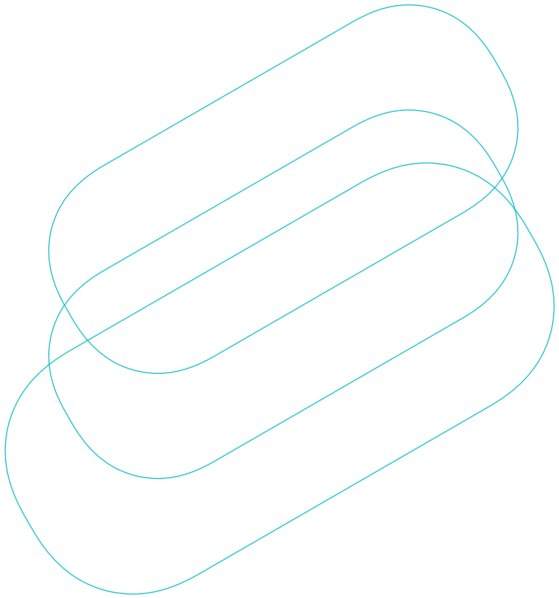
1. Incidentes e lacunas de visibilidade

Qual é o percentual de empresas que atuam sem visibilidade na América Latina?

Como ponto de partida, avaliamos a capacidade das organizações de detectar ciberataques e compreender sua real exposição ao risco. Os resultados revelam um cenário de intensa atividade cibercriminosa, acompanhado por uma preocupante falta de visibilidade sobre os ambientes corporativos.

52,7 %

das empresas da América Latina relataram ter detectado ao menos uma tentativa de ciberataque nos últimos 12 meses, o equivalente a 824 organizações participantes da pesquisa. No **Brasil**, esse índice foi ainda mais elevado, atingindo **62%**, acima da média regional.

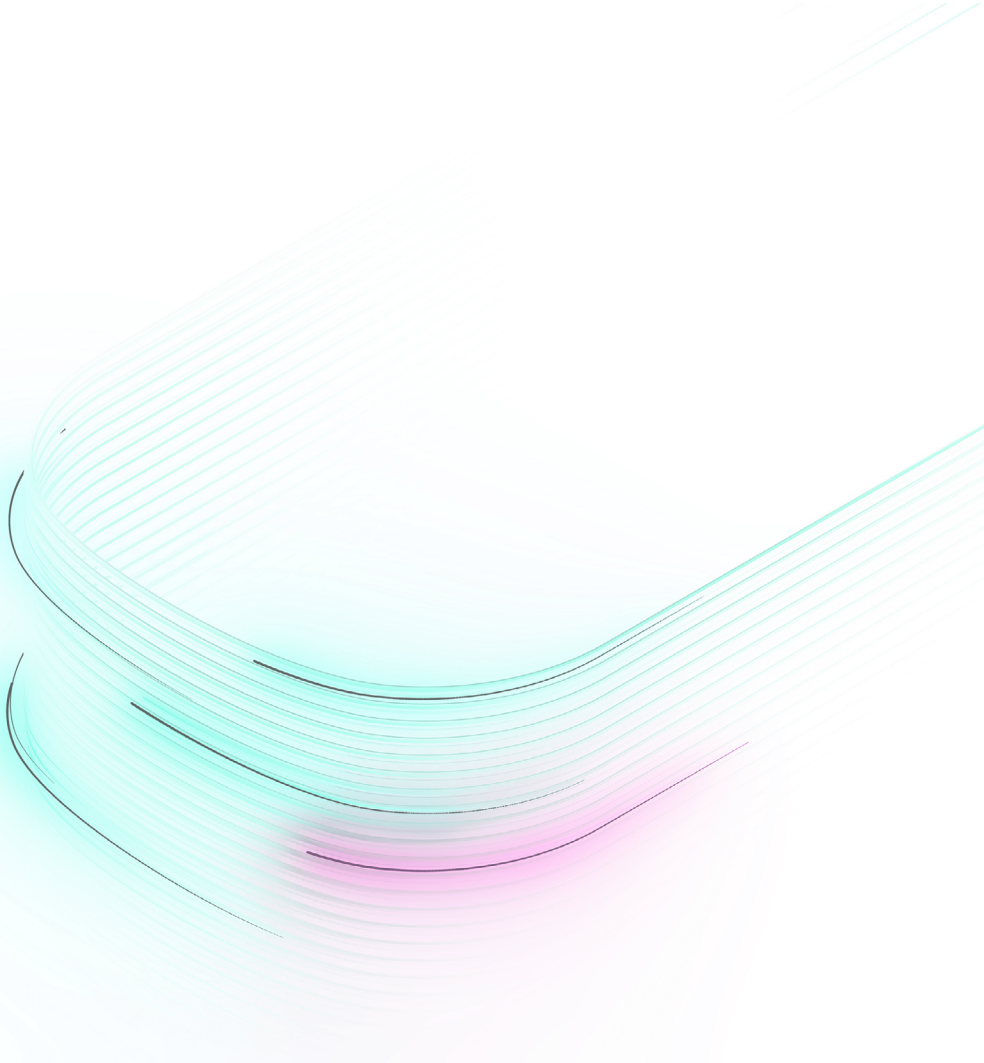


15,4 %

das organizações latino-americanas afirmaram não ser capazes de confirmar se foram ou não alvo de tentativas de ciberataque, o que evidencia uma deficiência crítica na capacidade de monitoramento e detecção de incidentes. No Brasil, esse percentual foi menor, chegando a **14,7%** das empresas entrevistadas.

Invisibilidade tecnológica e panorama regional

Entre as empresas que não detectaram ciberataques, a suspeita de incidentes não identificados e a falta de conhecimento técnico evidenciam uma vulnerabilidade estrutural na capacidade analítica das organizações da América Latina.



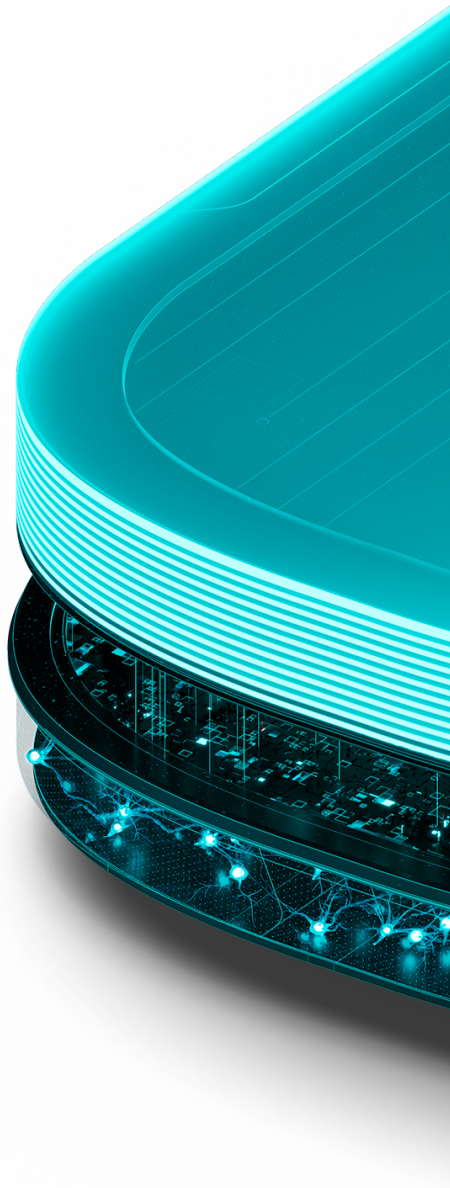
25,1 %

das organizações que não detectaram ataques admite que os incidentes podem ter ocorrido sem que seus sistemas percebessem, por não contar com tecnologia suficiente para detectá-los. No Brasil, esse percentual é significativamente maior, alcançando **43,3%**.

Conclusão: **4 em cada 10 organizações na América Latina** não possuem capacidade analítica suficiente para auditar sua segurança real, ao considerar o desconhecimento técnico e a suspeita de incidentes não registrados.

Comportamento por setor

A análise por setor demonstra que a exposição ao risco está diretamente relacionada ao nível de visibilidade técnica, à incidência de ataques e às lacunas de segurança observadas em cada segmento de mercado.



Incidentes e lacunas de visibilidade

Manufatura

O setor de manufatura registra a maior taxa de incidentes da região: **62,7%** (Brasil: **58,3%**) das empresas afirmaram ter detectado tentativas de ciberataque. Também concentra uma das maiores incidências de phishing, com **81,1%** (Brasil: **85,7%**) das organizações relatando esse tipo de ocorrência. Em contrapartida, apresenta a menor taxa de incerteza, já que apenas **5,1%** das empresas entrevistadas declararam não saber se foram alvo de ataques.

Bancário e Financeiro

Quase 3 em cada 5 instituições financeiras (**57,8%**, Brasil: **66,7%**) detectaram tentativas de ciberataque no último ano, tornando este o segundo setor mais visado. Em compensação, o segmento lidera a adoção de tecnologias avançadas de segurança, como DLP (**57,6%**, Brasil: **66,7%**), Threat Intelligence (**37,6%**, Brasil: **66,7%**) e EDR (**69,1%**, Brasil: **100%**).

Incidentes e lacunas de visibilidade

Governo, Educação e Saúde completam o panorama setorial, revelando cenários distintos entre a elevada exposição de dados sensíveis e a falsa sensação de segurança decorrente da baixa capacidade de detecção.

Governo

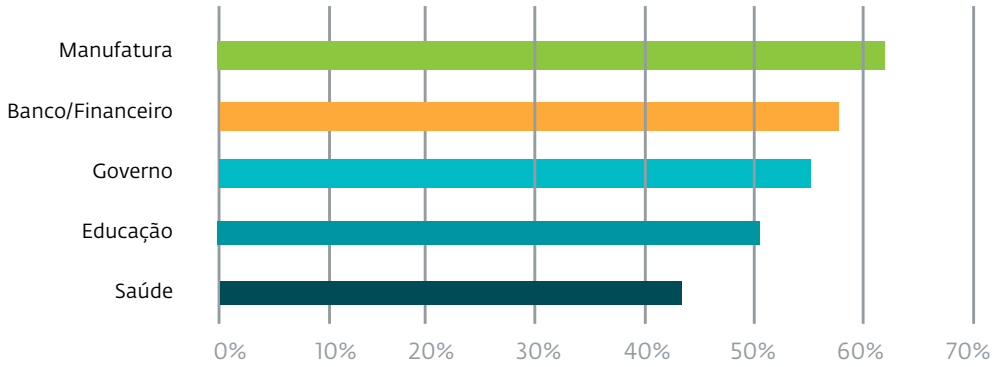
54,5% (Brasil: **61,9%**) dos órgãos governamentais participantes da pesquisa relataram atividade maliciosa, evidenciando uma elevada exposição de dados de cidadãos. O phishing foi o principal vetor de ataque, citado por **72,6%** (Brasil: **61,5%**) das organizações, seguido pelos acessos não autorizados (**43%**).

Educação

Exatamente **50,6%** (Brasil: **42,9%**) das instituições de ensino foram alvo de tentativas de ciberataque. O setor também apresentou o maior índice de incerteza da pesquisa: **21,2%** (Brasil: **14,3%**) das organizações não sabem informar se sofreram ataques. Além disso, o phishing atingiu seu maior índice entre todos os setores analisados, sendo reportado por **81,4%** (Brasil: **66,7%**) das instituições.

Saúde

O setor de Saúde registrou o menor percentual de organizações que confirmaram tentativas de ciberataque (**44,7%**, Brasil: **50,0%**). No entanto, esse resultado não significa necessariamente que seja o segmento menos atacado. O setor apresentou a maior proporção de respostas negativas (**42,1%**, Brasil: **50,0%**), o que pode indicar uma menor capacidade de monitoramento e detecção de incidentes.



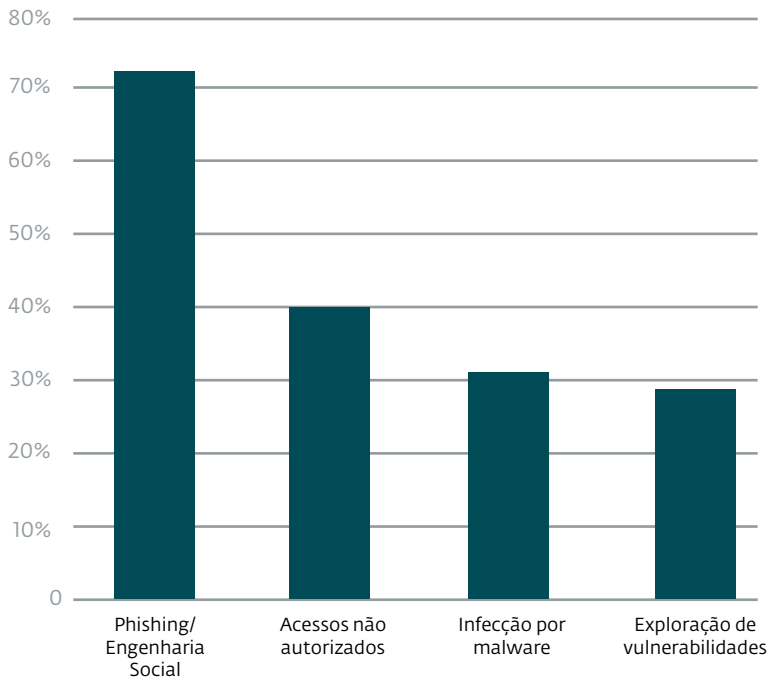
Taxa de ataques detectados por setor

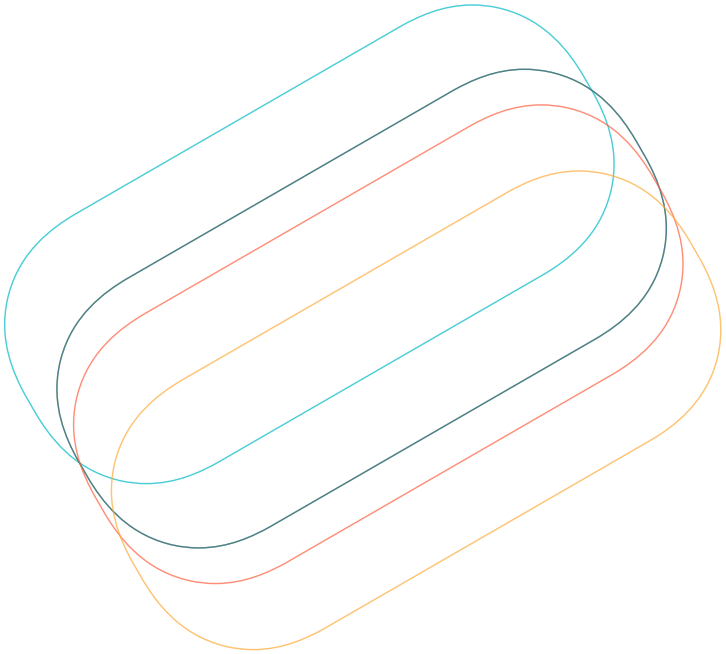
2. Vetores e tipos de ataques registrados

Phishing, acessos não autorizados e malware. Uma análise dos principais vetores de ataque e das portas de entrada mais exploradas pelos cibercriminosos.

Entre as empresas que registraram incidentes, os principais tipos de ataques identificados distribuíram-se da seguinte forma, evidenciando a engenharia social e o comprometimento de identidades como as principais ameaças na América Latina.

Principais vetores e incidentes de ciberataques na América Latina





Vetores e tipos de ataques registrados

73 % (Brasil: 70,9%)

das organizações foram alvo de ataques de phishing ou engenharia social

O phishing consolidou-se como o principal vetor de ataque na América Latina, afetando organizações de todos os setores. Os maiores índices foram registrados em Educação (**81,4%**, Brasil: **66,7%**), Manufatura (**81,1%**, Brasil: **85,7%**) e Bancário e Financeiro (**79,6%**, Brasil: **100%**). O setor de Saúde apresentou a menor incidência desse tipo de ataque, com **67,6%** (Brasil: **100%**).

40 % (Brasil: 44,3%)

das empresas sofreram acessos não autorizados

Os acessos não autorizados representam o segundo vetor de ataque mais frequente, envolvendo técnicas como ataques de força bruta, sequestro de sessões e uso de credenciais comprometidas. O setor mais afetado foi o de Educação (**51,2%**, Brasil: **33,3%**), seguido por Informática e Tecnologia (**43,3%**, Brasil: **40,0%**) e Governo (**43%**, Brasil: **23,1%**).

Intrusões e vulnerabilidades

A falta de higiene básica em sistemas obsoletos e o sequestro de ativos completam o panorama de incidentes, com impactos que variam significativamente de acordo com a infraestrutura de cada setor.

31,6 %

(Brasil: 41,8%)

Infecção por malware

Inclui ransomware, trojans e spyware. O setor de Saúde registra o dobro da média regional, com **52,9%** (Brasil: **66,7%**) dos incidentes relacionados a esse vetor.

29,2 %

(Brasil: 49,4%)

Exploração de vulnerabilidades

Esse vetor costuma estar associado à ausência de processos de aplicação de patches e atualização de sistemas. Os setores de Saúde (**38,2%**, Brasil: **66,7%**) e Educação (**30,2%**, Brasil: **66,7%**) lideram os índices, devido à presença de infraestruturas mais antigas e ciclos de atualização mais lentos.

8,4 %

(Brasil: 11,4%)

Sequestro ou vazamento de informações

Embora seja o incidente menos frequente, é o que apresenta o maior impacto operacional. O setor de Tecnologia da Informação registra a maior taxa, com **12,2%** (Brasil: **20,0%**). Entre os incidentes identificados também estão acessos não autorizados (**40,0%**, Brasil: **44,3%**), infecções por malware (**31,6%**, Brasil: **41,8%**), exploração de vulnerabilidades (**29,2%**, Brasil: **49,4%**) e sequestro ou vazamento de informações (**8,4%**, Brasil: **11,4%**).

3. O fator inteligência artificial: entre o temor e a falta de regulamentação

Como é percebido o risco da IA e o vazio de governança interna nas empresas da América Latina.

A percepção de risco em relação ao desenvolvimento da Inteligência Artificial está concentrada principalmente na automação de ameaças avançadas e na falsificação de identidade em setores estratégicos.

56,3 %

(Brasil: 49,2%)

dos profissionais

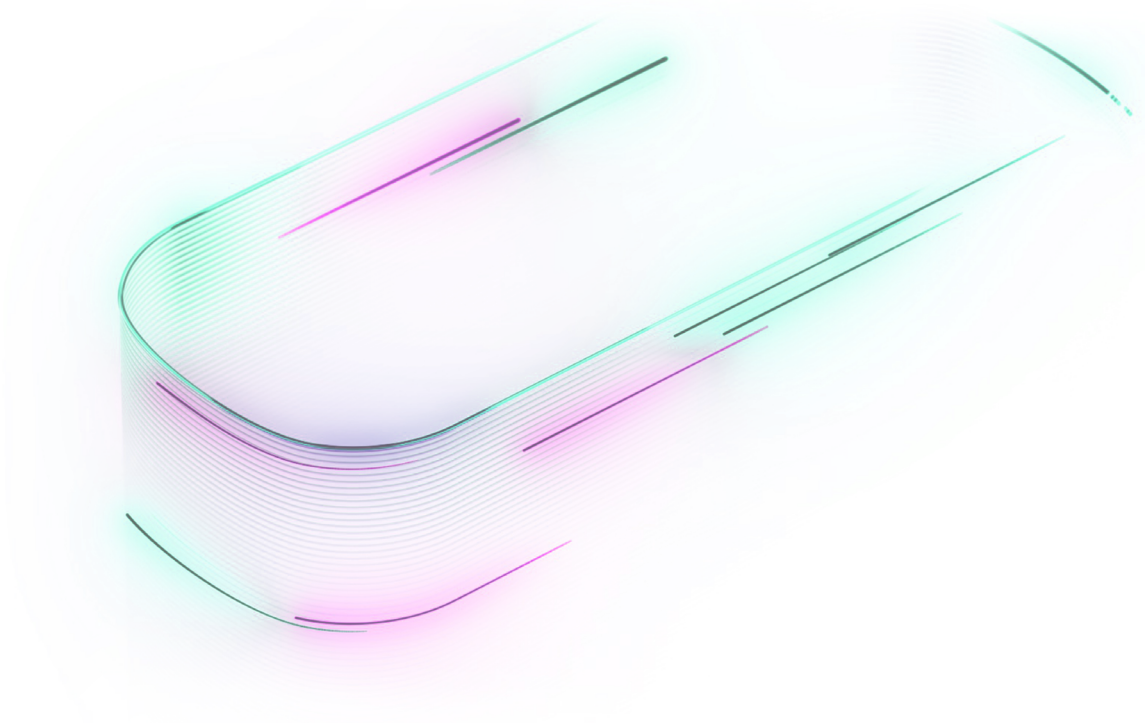
identificam o desenvolvimento de ataques mais sofisticados e automatizados como a principal ameaça associada à IA. Essa percepção chega a **74,6%** (Brasil: **25,0%**) no setor de Manufatura e a **63,5%** (Brasil: **28,6%**) na Educação. O setor de Manufatura registra o maior nível de preocupação na América Latina: **74,6%** dos profissionais consideram a IA uma ameaça de alta sofisticação - no Brasil, esse mesmo setor prioriza outros riscos, como roubo de dados (**33,3%**) e deepfakes (**25,0%**).

19,6 %

(Brasil: 20,3%)

dos entrevistados

apontam a falsificação de identidade por meio de deepfakes como o principal perigo, sendo o setor de Informática/Tecnologia o mais preocupado com esse vetor (**24,2%**, Brasil: **21,6%**) - números bem alinhados entre Brasil e região.



Políticas e maturidade regulatória interna

A adoção de ferramentas de IA apresenta uma forte assimetria no controle corporativo, dividindo o mercado entre empresas sem qualquer regulamentação interna e organizações com diferentes níveis de políticas de uso, que variam de acordo com o setor.

Principais descobertas

39,2%

(Brasil: 45,3%)

operam em um vazio regulatório absoluto, deixando a decisão de uso da IA a critério dos funcionários;

39,7%

(Brasil: 39,1%)

incentivam o uso da tecnologia seguindo diretrizes internas;

17,8%

(Brasil: 14,1%)

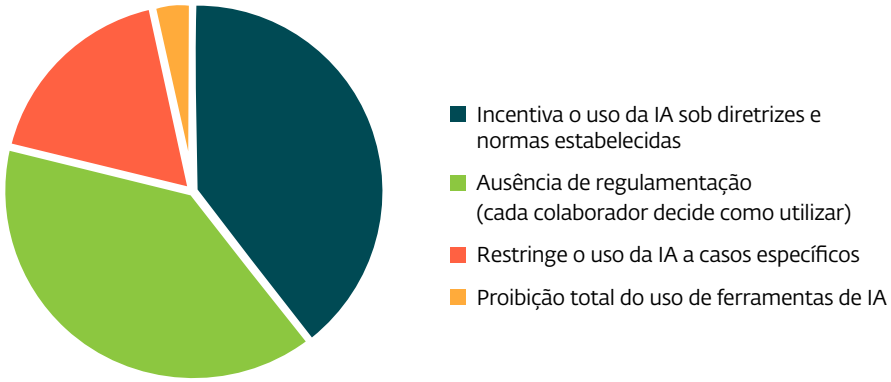
restringem o uso a casos específicos;

3,4%

(Brasil: 1,6%)

aplicam uma proibição total.

Modelos de Governança de IA nas Organizações da América Latina



Os extremos por setor

A Educação é o setor com menor nível de regulamentação; **58,8%** (Brasil: **57,1%**) das instituições não possuem nenhum tipo de regra sobre o uso de IA - números praticamente idênticos entre Brasil e região. Em contraste, no setor de Bancos e Serviços Financeiros, **47,6%** das organizações da América Latina incentivam o uso da tecnologia seguindo normas internas rigorosas - no Brasil, esse padrão se inverte: **66,7%** das instituições financeiras não têm regulamentação alguma, e apenas **33,3%** incentivam o uso com diretrizes.

4. Maturidade tecnológica: a lacuna das defesas

Análise da assimetria entre a adoção de ferramentas perimetrais básicas e capacidades analíticas avançadas.

A análise demonstra uma forte assimetria entre as defesas básicas de perímetro e as ferramentas analíticas avançadas. Essa distância evidencia um modelo mais reativo do que proativo.

Tecnologia	América Latina	Brasil
Firewall	85%	**93,9%**
Backup	82%	**92,9%**
VPN	73%	**76,8%**
Dupla autenticação (2FA)	57%	**68,7%**
EDR	52%	**68,7%**
DLP	36%	**51,5%**
Threat Intelligence	23%	**49,5%**

Observações: O setor financeiro se destaca como o mais maduro, com maior adoção de tecnologias avançadas - no Brasil essa liderança é ainda mais acentuada: DLP **66,7%**, Threat Intelligence **66,7%** e EDR **100%** entre as instituições financeiras respondentes. O setor governamental registra a vulnerabilidade mais preocupante em controles de acesso: apenas **41,6%** (Brasil: **38,5%**) implementaram a dupla autenticação - um ponto de atenção que se repete, e até se agrava levemente, no cenário brasileiro. Threat Intelligence é a tecnologia com menor nível de adoção na América Latina, embora no Brasil ela já esteja bem mais difundida que a média regional.

5. Hábitos dos usuários

O elo humano é um dos fatores mais importantes da cibersegurança. Este levantamento apresenta dados sobre a adoção do uso de antivírus, autenticação de dois fatores e proteção dos dispositivos corporativos.

A análise focada em funcionários não técnicos (**19,3%** dos entrevistados na América Latina, Brasil: **22,7%**) revela vulnerabilidades críticas associadas ao fator humano, evidenciando uma lacuna entre a segurança dos equipamentos tradicionais e a proteção da identidade digital.

Dispositivos corporativos desprotegidos.
Embora **81,4%** (Brasil: **100%**) utilizem antivírus em seus equipamentos de trabalho, o descuido com a proteção da identidade ainda é elevado: apenas **52,2%** (Brasil: **65,5%**) ativam a autenticação de dois fatores em suas contas corporativas.

Segurança em dispositivos móveis (o grande esquecido)
O celular corporativo se consolida como o ponto mais vulnerável. 1 em cada 4 funcionários da América Latina (**26,9%**) reconhece que não utiliza nenhuma solução ou medida de segurança em seu dispositivo móvel de trabalho - no Brasil esse número é bem mais alto: **51,7%** não usam nenhuma proteção móvel, ou seja, mais de 1 em cada 2 funcionários não técnicos.

A ESET® é uma empresa que oferece soluções de segurança digital de ponta para prevenir ataques.

Seu foco combina o poder da inteligência artificial com a experiência humana para antecipar ameaças cibernéticas conhecidas e emergentes, protegendo empresas, infraestruturas críticas e pessoas. Seja para proteção de endpoints, nuvem ou dispositivos móveis, nossas soluções e serviços nativos de IA e baseados em nuvem são altamente eficazes e fáceis de usar. A tecnologia da ESET inclui recursos robustos de detecção e resposta, criptografia ultrassegura e autenticação multifator.

Com defesa em tempo real 24 horas por dia, 7 dias por semana, e um sólido suporte local, mantemos pessoas protegidas e negócios funcionando sem interrupções. Um cenário digital em constante evolução exige uma abordagem progressiva de segurança, e a ESET assume esse compromisso, oferecendo também pesquisa de classe mundial e inteligência de ameaças avançada, apoiadas por centros globais de Pesquisa e Desenvolvimento, incluindo a América Latina, além de uma sólida rede global de parceiros comerciais.

Para saber mais, acesse www.eset.com/br/ ou siga-nos no LinkedIn, Facebook, Instagram.

Sobre a ESET

+ 110 milhões de usuários em todo o mundo

+ 500 mil clientes corporativos

11 centros de pesquisa e desenvolvimento no mundo

Presente em **200** países e territórios

ESET®

Cybersecurity
Progress. Protected.

esetbrasil

@esetbr