TENDÊNCIAS DE CIBERSEGURANÇA PARA 2026

Progress. Protected.

TABELA DE CONTEÚDOS

INTRODUÇÃO

O cenário de cibersegurança na América Latina continua apresentando crescente complexidade, com ameaças cada vez mais sofisticadas e direcionadas a setores públicos e privados. O ESET Security Report 2025 revelou que 27% das organizações da América Latina sofreram um ciberataque no ano anterior, enquanto 32% reconheceram não possuir a visibilidade necessária para confirmar se foram atacadas, uma lacuna crítica que limita a capacidade de detecção e resposta.

Além disso, acessos indevidos a sistemas e o roubo de informações sensíveis seguiram entre as principais preocupações das empresas, e o ransomware manteve-se como uma das ameaças centrais, apontado por 95% dos especialistas e com 22% das organizações afetadas nos últimos dois anos.

Nesse contexto, o Laboratório de Pesquisa da ESET América Latina analisou três tendências que devem ditar o ritmo do próximo ano e recomenda que sejam consideradas nas estratégias a serem implementadas pelas organizações em 2026. Ao longo deste relatório, serão abordados os eixos temáticos considerados mais relevantes e que tendem a ganhar protagonismo no próximo período.

Por um lado, o ransomware, um velho conhecido, avançará ou continuará sua aceleração rumo a modelos cada vez mais automatizados e lucrativos, com maior profissionalização e industrialização a partir do surgimento de malware baseado em inteligência artificial.

A tendência predominante, e relativamente recente, indica que o uso ofensivo da IA ampliará em escala a capacidade de gerar conteúdos falsos, campanhas de fraude personalizadas e ataques autônomos. Um cenário que já desafia a velocidade de resposta das organizações, que precisarão lidar com novos vetores de risco, especialmente nas cadeias de suprimentos. Em contrapartida, a IA também se consolidará como ferramenta-chave para a detecção precoce e a automação defensiva.

Tudo isso ocorre em um contexto no qual as regulações sobre o uso de inteligência artificial ainda podem ser consideradas insuficientes na América Latina, onde apenas oito países contam com estratégias formais de IA. Esse panorama impõe o desafio urgente de acelerar marcos de governança, promover a transparência algorítmica e fortalecer a cooperação internacional.

Por meio deste relatório, convidamos as empresas da América Latina a se aprofundarem na análise das principais tendências de cibersegurança para 2026, como forma de estarem mais bem preparadas para fortalecer suas defesas digitais, antecipar ameaças emergentes e proteger seu valioso patrimônio digital em um ambiente cada vez mais desafiador e sofisticado.

1

USO INTENSIVO DE IA E AUTOMAÇÃO OFENSIVA

Mario Micucci
Security Researcher
ESET Latinoamérica

Martina López
Security Researcher
ESET Latinoamérica

A inteligência artificial deixou de ser um tema restrito aos laboratórios dedicados às ciências da computação. Segundo um relatório apresentado em setembro de 2025 pela equipe de pesquisa econômica da OpenAI e publicado como Working Paper do National Bureau of Economic Research (NBER), o número de usuários ativos semanais do ChatGPT equivale a aproximadamente 10% da população adulta mundial.

Essa consolidação se explica por uma multiplicidade de fatores: o aumento de serviços e sistemas que incorporam IA de forma direta ou indireta, a maturidade das ferramentas, alcançada por meio de tentativa e erro, sua capacidade de resolver necessidades ou dores das pessoas e sua fácil acessibilidade para usuários não técnicos.

No ambiente corporativo, a combinação da implementação de ferramentas que utilizam IA com a automação gerou um grande salto de eficiência operacional, que pode, em alguns anos, ser comparado a grandes marcos de desenvolvimento e adoção tecnológica, como a virtualização ou a computação em nuvem. Muitas organizações adotaram essas tecnologias com base em um princípio conhecido como "AI first mindset": automatizar o maior número possível de processos e, depois, estruturar os fluxos de trabalho manuais necessários.

O universo da cibersegurança atravessa uma fase em que a inteligência artificial é, ao mesmo tempo, uma ferramenta de defesa e um amplificador de ataques. A automação pode se tornar tanto um diferencial estratégico quanto um multiplicador do impacto de incidentes. A questão deixou de ser se a IA deve ou não ser utilizada para resolver determinados problemas e passou a ser como garantir que seu uso intensivo não gere mais riscos do que benefícios.

USO EM LARGA ESCALA

A popularização de aplicações baseadas em modelos de inteligência artificial diminuiu significativamente a barreira técnica para a produção de conteúdo. Hoje, é possível gerar desde pequenos trechos de código até documentos complexos e edições audiovisuais sofisticadas com poucos comandos e conhecimento limitado. Por outro lado, a proliferação de conteúdo sintético tende a provocar impactos cognitivos relevantes na forma como as pessoas interpretam e assimilam informações. À medida que textos, imagens, áudios e vídeos artificiais se tornam indistinguíveis dos autênticos, a percepção de realidade passa a ser constantemente tensionada. É razoável antecipar efeitos duradouros sobre a confiança social e a noção de autenticidade. A dúvida deixa de ser exceção e passa a integrar o cotidiano informacional. Perguntar "isso é um deepfake?" tende a se tornar um gesto automático, quase instintivo, diante de qualquer conteúdo que circule.

Por outro lado, dados pessoais, padrões de comportamento e preferências passaram a ser insumos permanentes para os modelos de IA. Isso fará com que o conteúdo gerado seja cada vez mais humanizado e adaptado às expectativas individuais. Em contraste, também se tornarão cada vez mais comuns a criação de possíveis vetores de envenenamento involuntário, o vazamento de informações sensíveis e a propagação de erros e conteúdos arriscados.

No ambiente corporativo, a IA tornou-se um copiloto padrão em diversas profissões, com ou sem autorização formal das organizações. Seu uso indiscriminado, e operacionalmente difícil de controlar, gera riscos que vão além do vazamento de dados. Entre os mais relevantes estão a automação de erros humanos e a tomada de decisões apoiadas em modelos opacos, cujos critérios e vieses nem sempre são compreendidos ou auditáveis.

Para além do uso malicioso, a IA envolve riscos inerentes que exigem o desenvolvimento de uma adoção responsável, em um contexto no qual todos os agentes, inclusive adversários, também fazem uso dessa tecnologia.

O USO MALICIOSO DA IA

A democratização da IA a coloca à disposição de qualquer agente, inclusive daqueles com intenções maliciosas. Até 2026, veremos uma evolução acelerada em três grandes dimensões:

CONTEÚDO FALSIFICADO E MANIPULAÇÃO

A criação de conteúdo falsificado voltado à manipulação, desinformação e fraude tende a se intensificar. A clonagem de voz, hoje possível com poucos segundos de áudio, viabiliza ligações que induzem transferências financeiras, desbloqueios de acesso ou crises emocionais, como as falsas chamadas de sequestro. Também fortalece campanhas de influência cada vez mais segmentadas, corroendo a confiança pública e dificultando a verificação jornalística.

AUTOMATIZAÇÃO CRIMINOSA EM ESCALA

No universo de golpes e fraudes, centros de estelionato, que envolvem recrutamento, coerção e call centers criminosos, passarão a utilizar cada vez mais ferramentas de IA para gerar roteiros, perfis de vítimas e operações automatizadas. Deve crescer o uso de modelos e plugins capazes de executar tarefas completas que antes exigiam maior intervenção humana, reduzindo drasticamente a barreira técnica. Por exemplo, para automatizar ataques de ransomware ou realizar atividades de reconhecimento e exfiltração de dados. Incidentes recentes já indicam campanhas coordenadas integralmente com o uso de IA.

CRIMES DE MAIOR GRAVIDADE E USO MILITAR

Por fim, há as questões relacionadas a crimes de maior gravidade e preocupações de Estado. Ferramentas como sistemas de "nudify" e a geração de imagens ou vídeos não consensuais ampliaram o abuso digital, especialmente entre jovens, com impactos psicológicos e jurídicos crescentes. No âmbito geopolítico, avanços em navegação e reconhecimento vêm impulsionando a autonomia de drones e sistemas não tripulados, com riscos associados ao uso malicioso por agentes estatais ou não estatais e ao potencial de danos colaterais.

AUTOMATIZAÇÃO IMPULSIONADA POR IA: A TENDÊNCIA TRANSVERSAL QUE MULTIPLICA O RISCO

Uma das tendências mais disruptivas é a automação integral por meio de IA. Diferentemente da geração isolada de conteúdo, os modelos atuais podem atuar como operadores completos, encadeando tarefas e executando-as de forma autônoma.

Essa automação:

- **Reduz as barreiras de entrada** para cibercriminosos sem conhecimentos técnicos.
- **Multiplica a escala** de campanhas maliciosas, operando 24 horas por dia, 7 dias por semana.
- **Aumenta a velocidade** de teste, adaptação e implementação de ataques.
- **Viabiliza serviços criminosos "as a service"** acessíveis a qualquer cibercriminoso.

O risco central é a criação de ecossistemas criminosos autônomos, nos quais a IA não apenas auxilia o cibercriminoso, mas o substitui.

IMPACTOS ESPERADOS

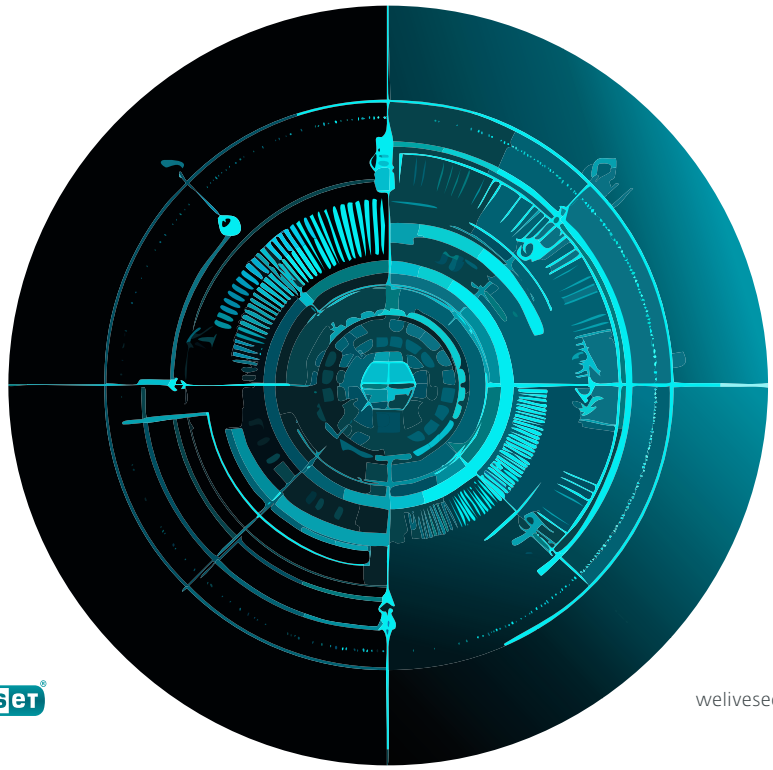
Assim como a IA otimiza processos legítimos, também torna mais eficientes as operações criminosas: geração de código malicioso sem programadores, seleção automatizada de vítimas sem analistas humanos e e-mails de phishing extremamente difíceis de detectar. Isso reduz os custos para os cibercriminosos e amplia as perdas econômicas das vítimas.

Além disso, deve se aprofundar a **erosão da confiança na internet**, especialmente em meios de comunicação e redes sociais. O crescimento de aplicações geradoras de conteúdo sintético dificulta a verificação e afeta não apenas o usuário comum, mas também o jornalismo, o sistema de Justiça e outras instituições que dependem de evidências digitais.

O ano de 2026 tende a ser um **ponto de inflexão** para compreender como os deepfakes, a automatização do assédio e a manipulação audiovisual influenciam relações pessoais, reputações e o bem-estar social.

As organizações ficam pressionadas entre a necessidade de automatizar para ganhar eficiência e a realidade de que os cibercriminosos dispõem das mesmas ferramentas. Essa corrida entre a velocidade dos ataques e a capacidade de resposta gera pressão constante sobre as equipes de segurança.

A convergência entre impactos econômicos, sociais e institucionais representará um desafio para todos os personagens do ciberespaço: o prejuízo econômico corrói a confiança social, a desinformação enfraquece instituições e a falta de preparo aprofunda as perdas corporativas.



2

A EVOLUÇÃO DO RANSOMWARE

Daniel Cunha Barbosa
Security Researcher
ESET Latinoamérica

O ransomware propriamente dito é uma ameaça com mais de 30 anos de existência. Embora tenha evoluído ao longo do tempo, os cibercriminosos passaram a demonstrar maior interesse e a utilizá-lo de forma mais intensiva após o surgimento das criptomoedas. Esse foi o principal marco na história dessa ameaça.

Desde então, o ransomware passou a ocupar um papel de destaque entre os diferentes tipos de malware, até chegar ao formato que conhecemos atualmente. Com a adoção de ativos digitais como forma de pagamento, o ransomware se consolidou como o principal método de monetização utilizado por cibercriminosos, registrando mais de 813 milhões de dólares em pagamentos de resgate somente em 2024.

Esse montante, além de permitir que ataques de ransomware e outras ameaças continuem ocorrendo, possibilita que os grupos cibercriminosos evoluam cada vez mais, em um ciclo vicioso que nos levou ao cenário que enfrentamos hoje.

O MODELO DE NEGÓCIO DO RANSOMWARE AS A SERVICE

Os grupos mais experientes de cibercriminosos perceberam que havia uma possibilidade significativa de ganhos com os próprios ataques de ransomware, mas também que poderiam monetizar de outras formas, explorando outros criminosos ou indivíduos mal-intencionados.

Foi assim que passaram a oferecer pacotes de software malicioso com garantia de não detecção, conhecidos como FUD, sigla para Fully Undetectable, além de tutoriais, acesso à infraestrutura de gestão de vítimas, acesso a servidores de comando e controle (C2), e até mesmo suporte técnico.

Esse movimento produziu dois efeitos centrais. De um lado, impulsionou receitas para grandes grupos criminosos em uma escala ainda difícil de mensurar com precisão. De outro, democratizou o acesso a capacidades ofensivas sofisticadas, permitindo que pessoas mal-intencionadas, sejam integrantes de redes cibercriminosas ou indivíduos com pouco ou nenhum conhecimento técnico, executem ataques altamente estruturados. Com modelos e serviços disponíveis no mercado clandestino, tornou-se possível lançar operações complexas investindo apenas algumas centenas de dólares, reduzindo drasticamente a barreira de entrada e ampliando o alcance e a frequência das ameaças.

Essa tendência do RaaS está bastante consolidada e continua em vigor. A grande maioria dos grupos de ransomware em atividade adota esse modelo, e sua eficácia ao longo dos anos incentivou novos cibercriminosos a incorporá-lo desde o início de suas operações.

A IA OFENSIVA COMO ACELERADOR DO RANSOMWARE EM 2026

Diversas análises de cibersegurança indicam que 2026 poderá marcar um ponto de inflexão na evolução do ransomware. Isso está relacionado ao avanço na adoção de modelos de IA projetados, ou manipulados, para executar tarefas ofensivas de forma autônoma. A IA passará a ter capacidade de automatizar desde a fase de reconhecimento até a exploração, em um nível que antes exigia equipes humanas especializadas.

Há indícios de que ao menos uma grande organização poderá ser comprometida por um agente de IA capaz de planejar e executar o ciclo completo do ataque, ajustando-se em tempo real e reduzindo a necessidade de operadores experientes por trás das campanhas.

Nesse contexto, agentes de inteligência artificial acessíveis, como o *OpenClaw*, podem ser conduzidos a realizar tarefas maliciosas, tornando-se multiplicadores críticos de ransomwares, não apenas ao gerar variantes polimórficas e contornar defesas, mas também ao automatizar o movimento lateral, a exfiltração estratégica de dados e até a negociação com vítimas.

Essa convergência entre IA e Ransomware as a Service cria um cenário em que até mesmo agentes com baixa capacidade técnica conseguem executar ataques antes restritos a grupos altamente sofisticados, acelerando a industrialização do cibercrime e aumentando a pressão sobre os defensores.

EVOLUÇÃO DO MALWARE: PRIMEIRO RANSOMWARE ESTRUTURALMENTE BASEADO EM IA

No fim de agosto de 2025, nossa equipe de pesquisa descobriu o PromptLock, um ransomware que consideramos um marco por ser estruturalmente baseado em IA. Pelas características apresentadas, o PromptLock foi considerado uma prova de conceito, ainda assim, lança luz sobre uma ameaça em potencial muito real e perigosa.

Diferentemente de operadores de ransomware que já utilizavam IA como apoio para industrializar ataques, o PromptLock seria o primeiro malware capaz de executar um modelo de inteligência artificial para gerar código malicioso, selecionar alvos e decidir quais arquivos criptografar ou exfiltrar de forma autônoma e em tempo real. Para isso, se utiliza scripts em Lua, conhecidos por

sua compatibilidade com diferentes plataformas, como Windows, macOS e Linux.

Durante a análise, foi possível identificar um módulo dedicado à destruição de arquivos, embora ele ainda estivesse inativo na amostra examinada.

Não é novidade que as IAs estão tornando os ataques cada vez mais sofisticados, elaborados e acessíveis. No entanto, seu uso como parte estrutural da ameaça adiciona um nível mais elevado de preocupação ao cenário.

Por meio do uso de APIs, o malware pode acessar modelos de linguagem avançados, permitindo que scripts maliciosos sejam criados e entregues diretamente no dispositivo infectado, além de proporcionar altíssima capacidade de adaptação, mutação e evasão de defesas.

A TRANSFORMAÇÃO DO BIG GAME HUNTING

Para abordar o último ponto previsto nessa tendência, é necessário mencionar o ransomware LunaLock. Para monetizar suas operações, esse grupo adotou uma abordagem diferente das formas de extorsão mais comuns, como a exigência de pagamento para remover a criptografia, a dupla extorsão, que ameaça divulgar ou vender os dados obtidos, ou a tripla extorsão, que pode incluir ataques DDoS a ativos importantes ou até mesmo a empresas parceiras da vítima.

Em vez disso, após atacar a empresa Artists&Clients, o grupo informou que o resgate deveria ser pago para evitar que todo o acervo de arte digital roubado fosse utilizado para treinar modelos de inteligência artificial.

Embora o ataque tenha como alvo uma empresa que seria severamente impactada caso suas obras fossem usadas para alimentar um modelo de IA generativa, o principal ponto de atenção está no precedente que esse tipo de abordagem estabelece. É comum que cibercriminosos compartilhem Táticas, Técnicas e Procedimentos entre si e, embora o ransomware tenha sido a ameaça que abriu caminho para esse método, é provável que outros tipos de malware que possam se beneficiar desse modelo de extorsão também o adotem.

Não deve demorar para que IAs generativas sejam utilizadas para incorporar inovações, mutações, novas funcionalidades ou mecanismos de evasão a todos os tipos de malware conhecidos, o que torna imprescindível que os ambientes também empreguem o máximo possível de avanços tecnológicos para inibir a atuação dessas ameaças.

O RANSOMWARE NA AMÉRICA LATINA: UM CENÁRIO CADA VEZ MAIS COMPLEXO

O impacto do ransomware na América Latina em 2025 deixou evidente que a região continua sendo um dos cenários mais ativos do mundo para esse tipo de ataque. Diversas pesquisas publicadas no WeLiveSecurity mostraram que variantes conhecidas e novos grupos criminosos concentraram esforços em setores sensíveis da América Latina.

A pressão não se limitou a alvos isolados. O ESET Security Report 2025, divulgado em julho, confirmou que organizações do Brasil, da Argentina, do Chile e do México, incluindo universidades, hospitais e órgãos governamentais, foram alvos frequentes de variantes como LockBit, Medusa e RansomHub.

O relatório também revelou que 22% das organizações da região sofreram um ataque de ransomware nos últimos dois anos e que 95% dos especialistas em segurança consideram essa uma de suas principais ameaças. No entanto, menos da metade dessas instituições implementava controles de segurança maduros, o que evidencia uma lacuna preocupante entre percepção e capacidade de resposta.

Por fim, o relatório apontou um problema estrutural: embora 27% das organizações declararem ter sofrido um ciberataque, 32% reconheceram que poderiam não ter visibilidade suficiente de seus ambientes para determinar se foram atacadas ou não. Essa falta de monitoramento cria um ambiente especialmente

favorável para que grupos de ransomware permaneçam por longos períodos dentro das redes corporativas.

A AUSÊNCIA DE CONTROLES BÁSICOS É UM DESAFIO

O cenário regional deixa claro que, para além do avanço tecnológico das ameaças e do fato de que a IA continuará fazendo parte de sua evolução, a ausência de controles básicos seguirá sendo um fator determinante para viabilizar a expansão do ransomware na América Latina ao longo de 2026.

3

REGULAÇÃO E POLÍTICAS DE CIBERSEGURANÇA NA ERA DA INTELIGÊNCIA ARTIFICIAL

David González
Security Researcher
ESET Latinoamérica

Nos últimos anos, a inteligência artificial tornou-se um elemento central da vida digital e da cibersegurança. Hoje, ela potencializa a detecção precoce de ameaças, a análise de grandes volumes de ações e a antecipação de comportamentos maliciosos com maior precisão.

Esse mesmo avanço, no entanto, abriu espaço para novos riscos, como campanhas de phishing e BEC mais reais, deepfakes de voz utilizadas em fraudes, automação de ataques e malwares capazes de aprender e se modificar.

A IA consolida-se como um vetor estratégico duplo: fortalece a defesa digital, mas também amplia as capacidades ofensivas. Por isso, a regulação já não pode ser vista como um debate teórico, e sim como um componente estrutural da gestão de riscos e da resiliência organizacional.

Qualquer discussão séria sobre regulação em cibersegurança estará inevitavelmente atravessada pela evolução da IA e por sua incidência direta na segurança das organizações.

UM DEBATE REGULATÓRIO QUE DEIXA DE SER TEÓRICO

A discussão regulatória deixou de ser abstrata e tornou-se operacional. Ao longo de 2026, a avaliação da IA não estará voltada apenas à sua capacidade de inovação, mas também ao seu impacto sobre direitos, segurança e governança.

A Artificial Intelligence Act introduziu uma abordagem baseada em risco que estabelece:

- Obrigações de transparência e rotulagem de conteúdo sintético.
- Restrições a usos de alto risco, como biometria, manipulação comportamental e infraestrutura crítica.
- Deveres específicos para modelos de propósito geral, conhecidos como GPAI.
- Implementação escalonada até 2026.

A transição é clara: já não basta desenhar marcos legais; agora é imprescindível implementá-los, supervisioná-los e auditar seu cumprimento efetivo.

Para as organizações, esse cenário implica:

- Controles de integridade sobre informações geradas ou processadas por IA.
- Maior escrutínio da cadeia de fornecedores de tecnologia.
- Políticas de resposta a incidentes relacionados à IA.
- Intervenção humana em decisões críticas, o chamado "human in the loop", para mitigar riscos de automação opaca.

Nesse contexto, a regulação não freia a inovação. Ela redefine os padrões mínimos de confiança digital.

AMÉRICA LATINA: AVANÇOS ESTRATÉGICOS E LACUNAS ESTRUTURAIS

Na América Latina, o nível de preparação é heterogêneo. A Comissão Econômica para a América Latina e o Caribe (CEPAL), em conjunto com o Centro Nacional de Inteligência Artificial (CENIA), desenvolveu o Índice Latino-Americano de Inteligência Artificial (ILIA), que mede o nível de preparação e adoção da IA em 19 países, integrando dimensões como fatores habilitadores, P&D e governança.

Seu objetivo é oferecer um diagnóstico estratégico que permita a governos e empresas compreender onde estão e para onde avançar, fomentando competitividade e investimento responsável no ecossistema regional de IA. Busca ser uma ferramenta para o desenho de regulações, estratégias e políticas nacionais de IA, alinhadas a padrões internacionais e adaptadas às necessidades locais.

De acordo com o ILIA 2025, apenas 8 dos 19 países analisados contam com estratégias ou políticas públicas formais de IA: Brasil, Argentina, Chile, Colômbia, Costa Rica, Peru, República Dominicana e Uruguai.

Esse avanço convive, ainda assim, com lacunas críticas em privacidade, governança de dados e responsabilidade legal, que afetam a resiliência de infraestruturas críticas e a confiança pública em sistemas baseados em IA.

A ausência de marcos robustos pode resultar em uso indevido de dados, vieses algorítmicos e vulnerabilidades em sistemas críticos, impactando tanto a resiliência das infraestruturas quanto a confiança da sociedade.

As estratégias nacionais permitem estabelecer princípios éticos, definir responsabilidades legais e garantir que a IA seja utilizada para impulsionar o desenvolvimento econômico sem comprometer a segurança. Além disso, facilitam a cooperação internacional e a atração de investimentos em tecnologia, fatores-chave para reduzir a lacuna digital na região.

Apesar de muitos países já contarem com algum plano, estratégia ou política, ainda é necessário avançar em temas como cibersegurança, privacidade dos dados inseridos em modelos locais de IA, responsabilidade na definição e no uso de modelos e algoritmos, além de governança e soberania de dados.

É nesse ponto que questões centrais sobre regulação precisam ser enfrentadas para oferecer maior segurança aos cidadãos, evitar vieses e discriminações por parte dos modelos de IA, principalmente:

- **Responsabilidade:** quem responde quando um

sistema de IA causa prejuízos? Há competência técnica para revisar e auditar modelos de IA?

- **Tratamento de dados**: existe consentimento do usuário? Ele é informado, com transparência e clareza, sobre como seus dados serão utilizados?

- **Clareza sobre armazenamento:** Londe os dados serão guardados? Em servidores próprios ou externos?

- **Transparência dos resultados:** a IA deve ser rastreável e compreensível para diferentes públicos, promovendo o conceito de IA Explicável (XAI).

- **Mitigação de vieses:** modelos de IA podem perpetuar preconceitos presentes nos dados de treinamento, levando a decisões injustas ou discriminatórias.

- **Proteção contra usos indevidos:** é fundamental implementar mecanismos de detecção de anomalias no treinamento, além de monitoramento e avaliação contínua dos algoritmos.

POR QUE A REGULAÇÃO IMPORTA: O "TRIÂNGULO" DO IMPACTO DA IA NA CIBERSEGURANÇA

O Fórum Econômico Mundial identifica três vetores que compõem o novo equilíbrio da cibersegurança impulsionado pela IA. Esse "triângulo" permite compreender de forma abrangente como as capacidades ofensivas e defensivas estão sendo redistribuídas, bem como os riscos emergentes para as organizações:

- **Expansão da superfície de ataque e maior impacto operacional**

A adoção de IA em processos e cadeias de suprimentos introduz componentes altamente interdependentes, como modelos, dados, prompts, agentes e pipelines de MLOps, que viabilizam novos vetores de ataque. Entre eles estão o envenenamento de dados, a manipulação de inferências, a evasão de modelos e o comprometimento de fornecedores de tecnologia.

O impacto vai além do aspecto técnico: pode interromper processos essenciais, degradar indicadores críticos do negócio e comprometer a confiança do cliente.

- **Defesas potencializadas por IA**

A IA eleva as capacidades do ecossistema defensivo ao permitir detecção baseada em comportamento, análise massiva de telemetria e automação coordenada de respostas.

Em ambientes XDR e em nuvens de segurança, isso se traduz em menor tempo de detecção, maior precisão e redução de falsos positivos.

- **Escalonamento de ameaças impulsionado por IA**

A IA também amplia as capacidades ofensivas, desde spear phishing gerado automaticamente até deepfakes de voz altamente verossímeis, além de ferramentas que automatizam a descoberta de vulnerabilidades e a criação de malware adaptativo.

O resultado é um cibercrime mais rápido, mais preciso e acessível até mesmo para cibercriminosos com pouca experiência.

UM EQUILÍBRIO URGENTE ENTRE INOVAÇÃO E SEGURANÇA

A IA consolida-se como uma aliada fundamental para a defesa digital e, ao mesmo tempo, como um vetor de risco que exige governança e regulação eficazes.

Embora a América Latina apresente avanços, com oito países contando com estratégias formais de IA, ainda persistem lacunas em privacidade, governança de dados e responsabilidade legal, que precisam ser tratadas com prioridade para proteger a população e fortalecer a resiliência de sistemas críticos.

A ausência de marcos regulatórios sólidos abre espaço para riscos como vieses algorítmicos, uso indevido de informações e vulnerabilidades em infraestruturas críticas. Por isso, é essencial que os governos acelerem a criação de normas claras, promovam a transparência e incentivem a cooperação regional. Somente assim será possível equilibrar os benefícios da IA com a proteção dos cidadãos e a resiliência digital.

CONCLUSÃO

A construção de um ecossistema digital mais seguro na América Latina depende de uma compreensão aprofundada das ameaças que impactam a região e do fortalecimento das capacidades que as organizações precisam desenvolver para preveni-las, detectá-las e responder a elas de forma eficaz. Os desafios destacados ao longo deste relatório demonstram que a cibersegurança já não pode ser tratada apenas como resposta a incidentes, mas sim a partir de uma visão estratégica que considere a evolução tecnológica, os novos modelos de ataque e a crescente dependência digital dos setores público e privado.

As tendências analisadas revelam um cenário em que a automação e a inteligência artificial desempenharão um papel determinante, tanto ao potencializar táticas ofensivas quanto ao viabilizar defesas mais robustas. No entanto, essa dualidade exige redobrar esforços em governança, capacitação e adoção de práticas preventivas que reforcem a resiliência organizacional. A falta de visibilidade, a implementação limitada de controles essenciais e a insuficiência regulatória são fatores que precisam ser enfrentados de forma urgente e contínua.

Fica claro que o fortalecimento das capacidades de cibersegurança é um processo permanente, que demanda investimento, planejamento e colaboração multissetorial.

As organizações que conseguirem integrar esses elementos à sua estratégia estarão mais bem posicionadas para antecipar riscos, proteger seus ativos mais críticos e se adaptar a um ambiente em que as ameaças evoluem em velocidade sem precedentes.

Convidamos, assim, as empresas da América, incluindo o Brasil, a utilizarem esta análise como ponto de partida para refletir sobre seu próprio nível de preparação e avançar rumo a uma cultura de segurança mais madura, proativa e alinhada aos desafios que marcarão os próximos anos.

CYBERSECURITY
EXPERTS ON YOUR SIDE