



Ana Lucia Magliano é Vice-Presidente Executiva de Serviços, Mastercard América Latina e Caribe

A digitalização avança a passos largos e, com cada avanço, surgem novos desafios. O risco cibernético e as ameaças digitais evoluem constantemente com novas táticas impulsionadas por inteligência artificial e redes criminosas sofisticadas, colocando em risco a confiança, o crescimento e a segurança do ecossistema digital. Não se trata apenas de proteger transações, mas de assegurar cada interação. Sem confiança, a digitalização não pode prosperar.

Cibersegurança: um desafio global em crescimento

Os cibercriminosos encontraram na IA uma ferramenta poderosa para sofisticar seus ataques. Deepfakes, phishing automatizado e fraudes em grande escala tornam o crime organizado digital não apenas mais eficaz, mas também mais difícil de rastrear. Os números são alarmantes:

- Em 2023, as perdas por fraudes online alcançaram 1 trilhão de dólares em todo o mundo.
- Estima-se que o custo do cibercrime mundial chegue a 14 trilhões de dólares até 2028, o que o tornaria a terceira maior economia do mundo.
- As fraudes continuam sendo uma ameaça significativa e crescente, com quase metade dos consumidores globais sofrendo pelo menos uma tentativa por semana.
- Segundo a empresa de cibersegurança **Cybersecurity Ventures**, o custo global dos ciberataques em 2023 foi de 6 trilhões de dólares, e a previsão é que esse número aumente para 10 trilhões em 2025.
- Na América Latina, vazamentos e violações de dados atingiram um custo médio de 2,46 milhões de dólares – um recorde histórico para a região e um aumento de 76% desde 2020, segundo o estudo Cost of a Data Breach (America Economia – edição especial sobre Cibersegurança – março de 2024).

Esses dados reforçam a necessidade de uma abordagem mais estratégica em cibersegurança, que permita antecipar ameaças em vez de apenas reagir a elas.

Rumo a um ecossistema digital mais seguro

Na Mastercard, por exemplo, a segurança digital é parte integrante da nossa missão. Para nós, garantir a segurança digital envolve três pilares fundamentais:

- 1. Avaliar:** Dar visibilidade aos riscos cibernéticos. Soluções como o **RiskRecon** ajudam empresas e governos a compreender sua exposição ao risco, permitindo o monitoramento constante de vulnerabilidades.
- 2. Proteger:** Implementar tecnologias avançadas para mitigar ameaças. A IA e o monitoramento em tempo real são ferramentas essenciais para prevenir ataques. Com a **Recorded Future**, fortalecemos nossa capacidade de inteligência contra ameaças em tempo real. Além disso, soluções como o **SafetyNet** evitaram perdas de 50 bilhões de dólares por fraudes nos últimos três anos.
- 3. Organizar um ecossistema de confiança:** A luta contra o cibercrime não pode ser feita isoladamente. São necessárias alianças entre empresas, governos e organizações para compartilhar inteligência e criar padrões de segurança mais robustos.

A capacidade de rastrear padrões de ciberataques globalmente é crucial. Hoje, é possível detectar um ataque no Brasil, rastrear sua movimentação até a Indonésia e analisar sua reincidência na Alemanha. Esse nível de conectividade e análise preditiva é fundamental para antecipar ameaças emergentes e fortalecer a resiliência digital.

A IA como aliada na luta contra fraudes

Enquanto os cibercriminosos usam IA para aprimorar seus ataques, a inteligência artificial tornou-se uma aliada poderosa na segurança digital. Nossas soluções de IA generativa permitiram:

- 1. Dobrar a taxa de detecção de cartões comprometidos**
- 2. Reduzir em 200% os falsos positivos na detecção de fraudes**
- 3. Aumentar em 300% a velocidade de identificação de comércios em risco**

Essas inovações fortalecem a segurança e melhoram a experiência do usuário, reduzindo fricções e aumentando a confiança em cada transação.

Um chamado à ação: a segurança é uma responsabilidade compartilhada

Em um mundo cada vez mais interconectado, a confiança é o ativo mais valioso. Sem segurança, as oportunidades da digitalização podem ser comprometidas. Hoje, mais do que nunca, garantir a segurança do ecossistema digital exige inovação, cooperação e uma abordagem preventiva.

(16.05.2025)