

Ciberseguridad e Inteligencia Artificial en la Economía Digital Desafíos emergentes y desarrollo de capacidades para América Latina

José Luis Solleiro
Instituto de Ciencias Aplicadas y Tecnología
Universidad Nacional Autónoma de México (UNAM)

Julio de 2026

Ciberseguridad e Inteligencia Artificial en la Economía Digital

- Desafíos emergentes y desarrollo de capacidades para América Latina
- Aceleración de la conectividad en América Latina y su consecuente vulnerabilidad sistémica ante la llegada de la Inteligencia Artificial.
- La Inteligencia Artificial representa simultáneamente la mayor oportunidad tecnológica y uno de los mayores riesgos para la seguridad digital del siglo XXI.



La economía digital en crecimiento

- **La transformación digital está modificando:**
- Comercio
- Manufactura
- Salud
- Educación
- Gobierno digital
- Finanzas
- Agricultura
- Logística
- Más del 70 % del PIB mundial depende de procesos digitales.
- Los datos son el nuevo activo estratégico.
- La IA incrementará significativamente la productividad durante la próxima década.

Expansión de la Economía Digital

La economía digital se refiere a una **economía impulsada por las tecnologías digitales**, donde bienes y servicios son producidos, comercializados y consumidos a través de marketplaces, aplicaciones móviles y sistemas conectados.

Crecimiento Acelerado

El comercio electrónico, la banca digital y los servicios públicos en la nube se han expandido masivamente en la región, impulsando la productividad.

Sin embargo, esta transición apresurada incrementa sustancialmente la superficie expuesta a ataques sofisticados de actores maliciosos.

Brechas de Ciberseguridad

El ritmo de la digitalización en América Latina supera con creces la tasa de adopción de infraestructuras críticas de seguridad y marcos legales actualizados.

Esta asimetría estructural genera un ecosistema de alta vulnerabilidad para empresas de todos los tamaños y dependencias gubernamentales.

La inteligencia artificial

- La IA ya no es una tecnología aislada. Hoy impulsa:
  - Sistemas financieros
  - Infraestructura crítica
  - Vehículos inteligentes
  - Cadenas de suministro
  - Defensa
  - Servicios públicos
  - Investigación científica
- Sus características
  - Aprende
  - Predice
  - Automatiza
  - Genera contenido
  - Toma decisiones
- La misma capacidad que permite innovar también amplifica el riesgo



La IA cambia el escenario de las ciberamenazas

- Antes: ataques realizados principalmente por personas.
- Ahora:
- Ataques potenciados por IA capaces de:
  - automatizar campañas masivas
  - personalizar ataques
  - aprender de las defensas
  - adaptarse continuamente
- Automatización de ataques, evasión adaptativa de firewalls y suplantación hiperrealista.
- Ejemplos
  - Phishing generado por IA
  - Deepfakes
  - Malware adaptativo
  - Ingeniería social automatizada
  - Bots inteligentes

Amenaza	Impacto
Deepfakes	Fraude y desinformación
Phishing inteligente	Robo de credenciales
Malware autónomo	Ataques persistentes
IA para reconocimiento	Identificación de vulnerabilidades
Automatización criminal	Escalabilidad del cibercrimen

La IA como defensa: detección temprana de anomalías, correlación masiva de eventos en tiempo real e inmunización automatizada.

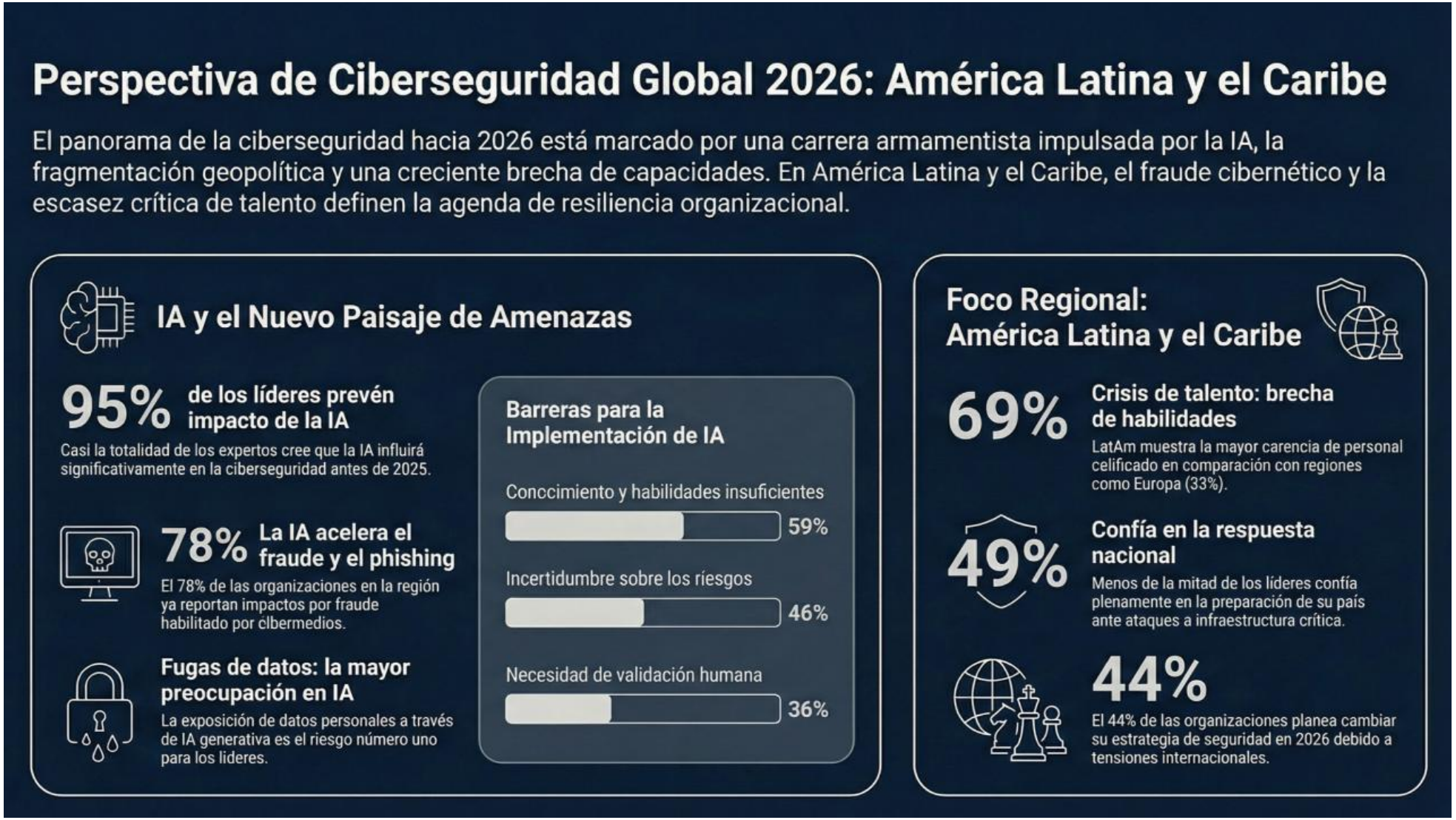
- La IA es una herramienta defensiva que permite:
  - detección temprana
  - análisis de millones de eventos
  - respuesta automática
  - análisis predictivo
  - inteligencia de amenazas
- Ejemplos
  - SOC inteligentes
  - SIEM con IA
  - EDR inteligentes
  - Threat Intelligence
  - Análisis de comportamiento



https://www.innovaciondigital360.com/cio/tendencias-tecnologicas-2026-america-latina/

América Latina

- rápida digitalización
- baja inversión en ciberseguridad
- escasez de especialistas
- incremento del ransomware
- crecimiento del fraude digital
- infraestructura crítica vulnerable
- Sectores más afectados
  - Gobierno
  - Banca
  - Salud
  - Educación
  - Energía
  - Telecomunicaciones



https://www.linkedin.com/pulse/el-panorama-de-la-ciberseguridad-en-am%C3%A9rica-latina-hacia-2026-desaf%C3%ADos-ynq3e/

¿Qué capacidades requiere América Latina?

- **Capital humano**
- especialistas en IA
  - analistas SOC
  - investigadores
  - expertos legales
  - científicos de datos
- **Infraestructura**
  - centros SOC
  - CSIRT nacionales
  - nube segura
  - laboratorios
  - centros de datos
- **Instituciones**
  - agencias nacionales
  - coordinación público-privada
  - CERT sectoriales
  - Marcos jurídicos homologados y adaptados al ritmo de la innovación

Ruta Estratégica 2026-2036

Fase I: Normativa

Actualización legislativa integral alineando leyes de protección de datos personales con el uso ético y ciberseguridad en IA.

Fase II: Talento

Capacitación y creación de posgrados nacionales en ciber-IA y retención de ingenieros de datos mediante incentivos locales.

Fase III: Alianzas

Intercambio transfronterizo ágil de experiencias y buenas prácticas

Fase IV: Autonomía

Desarrollo de centros locales de datos y supercómputo ; avance en autodeterminación tecnológica

Gobernanza de la IA y la ciberseguridad

- Elementos esenciales
- Marco regulatorio
- Ética
- Protección de datos
- Responsabilidad algorítmica
- Transparencia
- Gestión del riesgo
- Normas internacionales

¡Muchas gracias!

solleiro@unam.mx