La Formación en Ciberseguridad desde un enfoque disruptivo

Lic. Aldo González Miranda
Director LATAM de Carrera de Ciberseguridad y Estrategia de Ciberseguridad
Universidad Internacional UNIVERSAE

Lic. Aldo González Miranda
Director LATAM de Carrera de Ciberseguridad y Estrategia de Ciberseguridad

TECCOM 2025

Con una trayectoria de más de 12 años en la industria de la tecnología.

Desarrollando proyectos de ciberseguridad en el rol de consultor, ingeniero y líder técnico por más de 10 años, trabajando para corporaciones internacionales.

Fuí Director Nacional de Gobernanza Digital y Certificadores de Firma Digital, para el MICITT.

Ingeniero en Computación egresado del Tecnológico de Costa Rica, Licenciado en administración de proyectos de TI de la UNED, para la Universidad Internacional UNIVERSAE, actualmente docente para la Universidad Internacional UNIVERSAE y director de trabajo final de graduación para la UNED, además de contar con una amplia gama de certificaciones de la industria de ciberseguridad.

UNIVERSAE
UNIVERSIDAD INTERNACIONAL UIU

EDUCACIÓN CONTINUA CPIC

CPIC
COLEGIO DE PROFESIONALES EN INFORMÁTICA Y COMPUTACIÓN

Agenda

TECCOM 2025

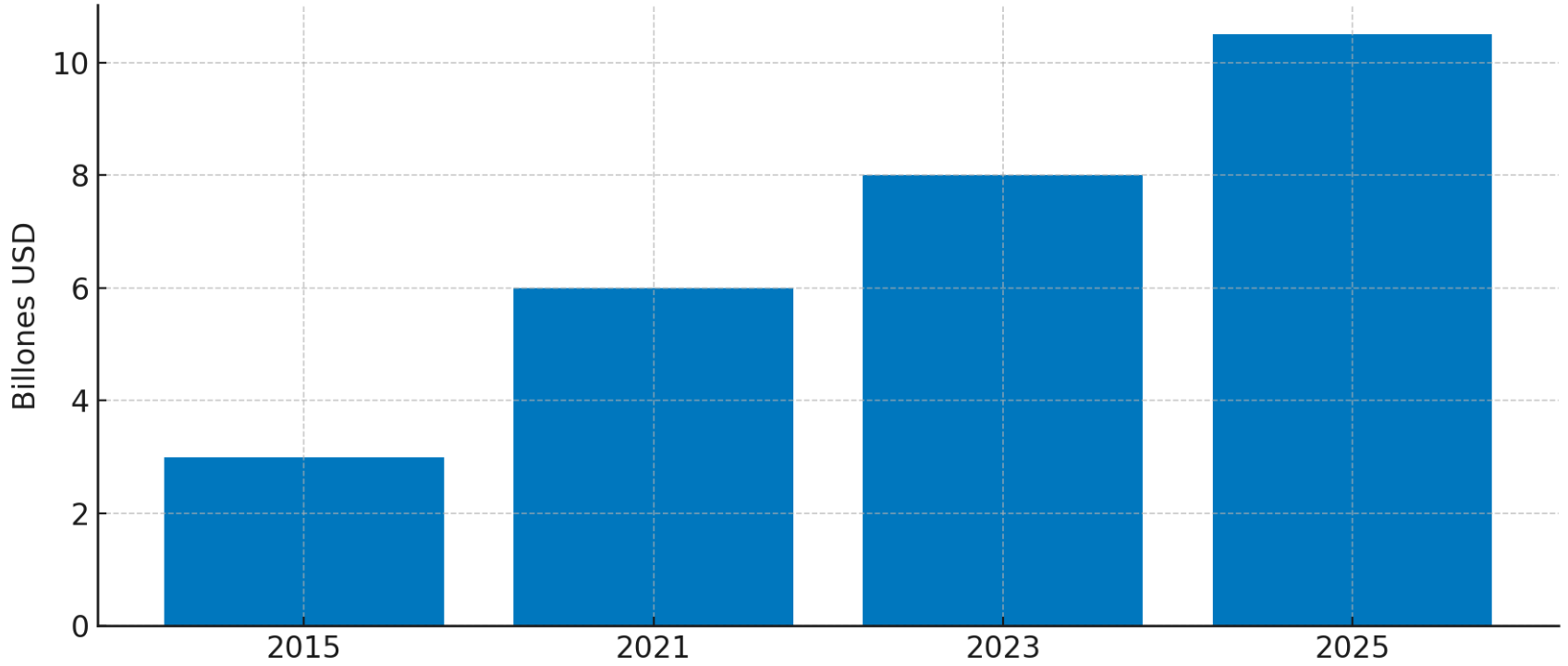
- Nuestra actualidad.
- ¿A qué nos enfrentamos?.
- ¿Nuevas Amenazas?.
- La educación disruptiva en Ciberseguridad.
- Conclusiones.

UNIVERSAE
UNIVERSIDAD INTERNACIONAL UIU

EDUCACIÓN CONTINUA CPIC

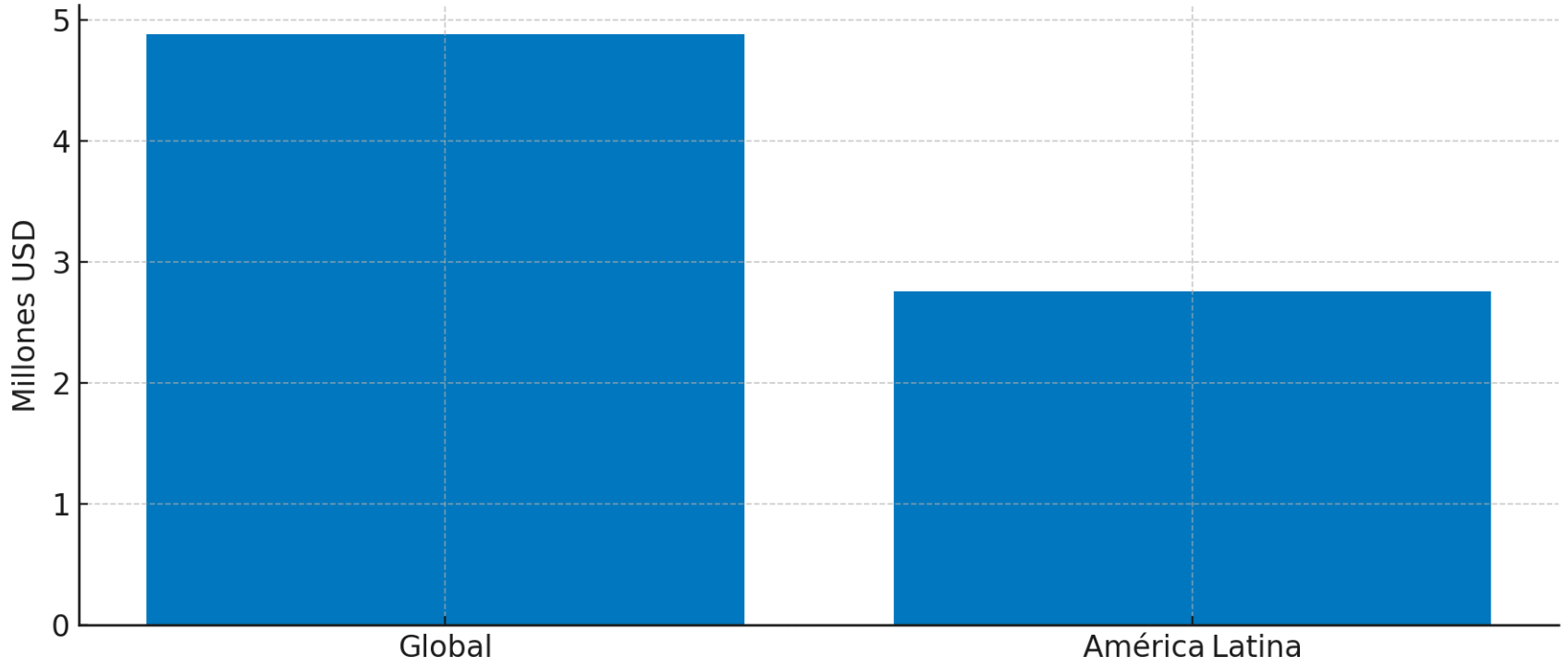
CPIC
COLEGIO DE PROFESIONALES EN INFORMÁTICA Y COMPUTACIÓN

Costo Global del Ciberdelito



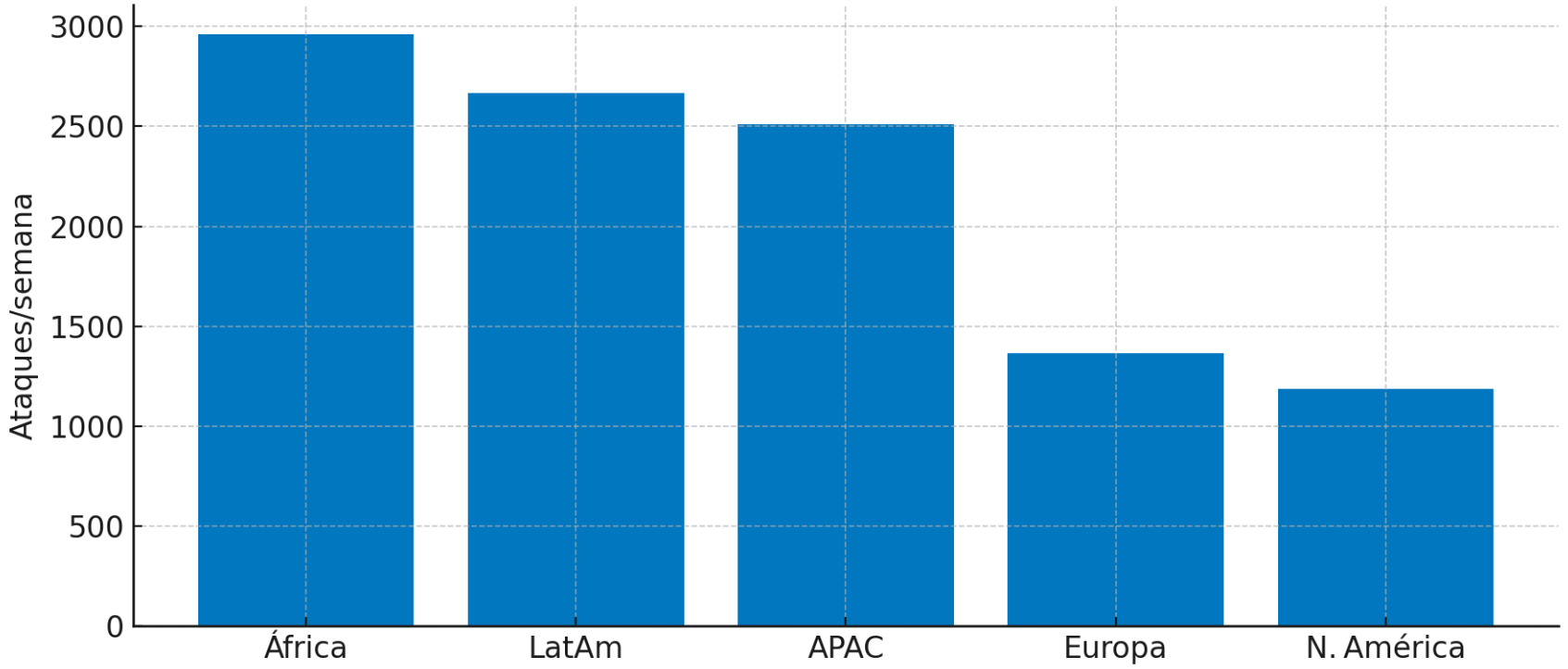
Fuente: Cybersecurity Ventures 2025

Costo por Filtración (2024)



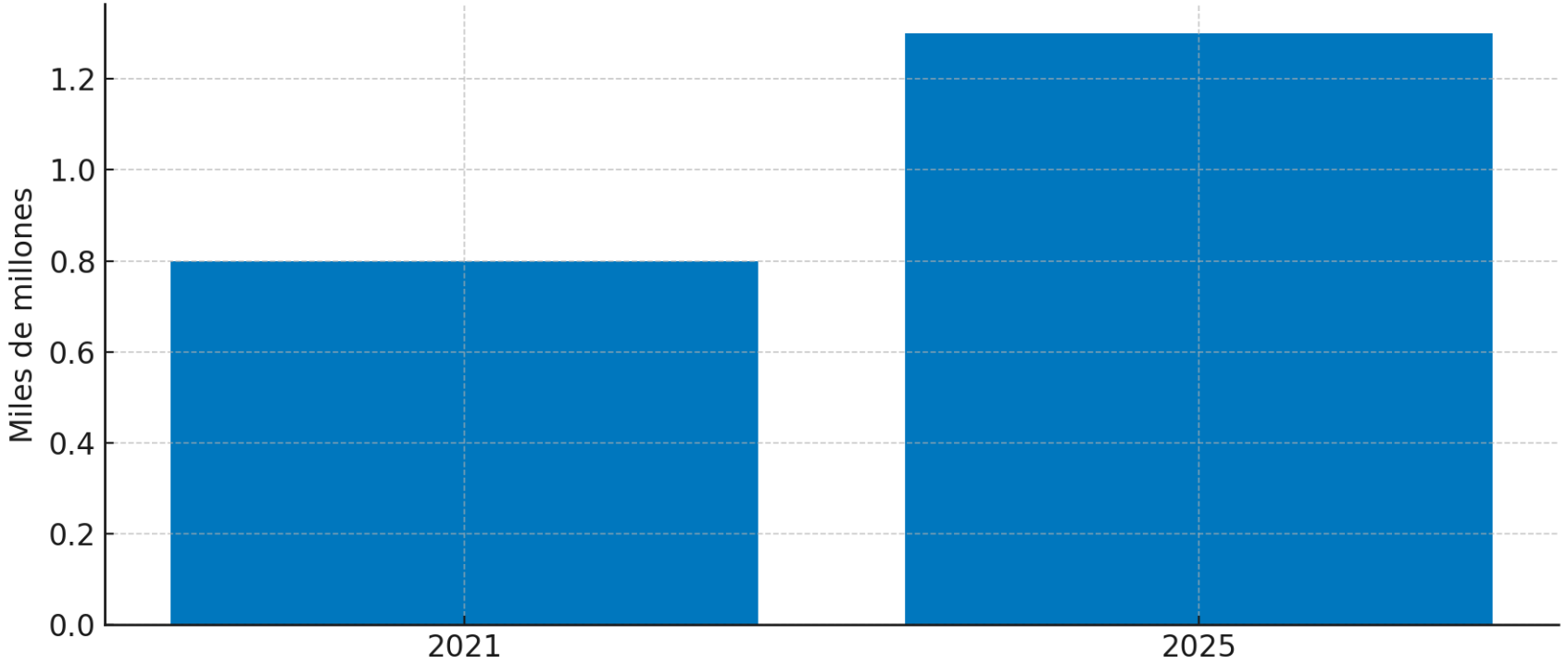
Fuente: IBM Cost of a Data Breach 2024; SecurITIC Latam

Ataques Semanales por Organización – 2024



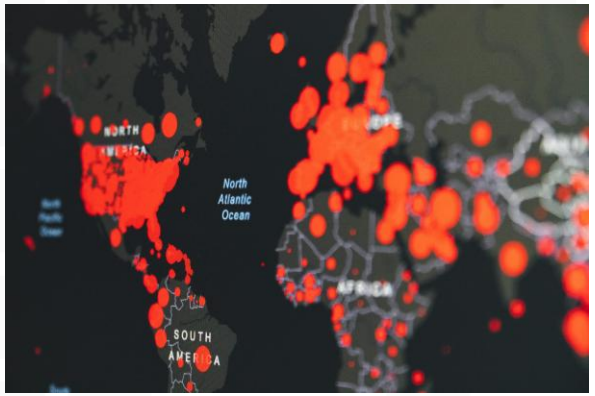
Fuente: Check Point Research Q2 2024

Conexiones IoT – América Latina



Fuente: Inter-American Dialogue IoT 2023

Superficie de Ataque Exponencial

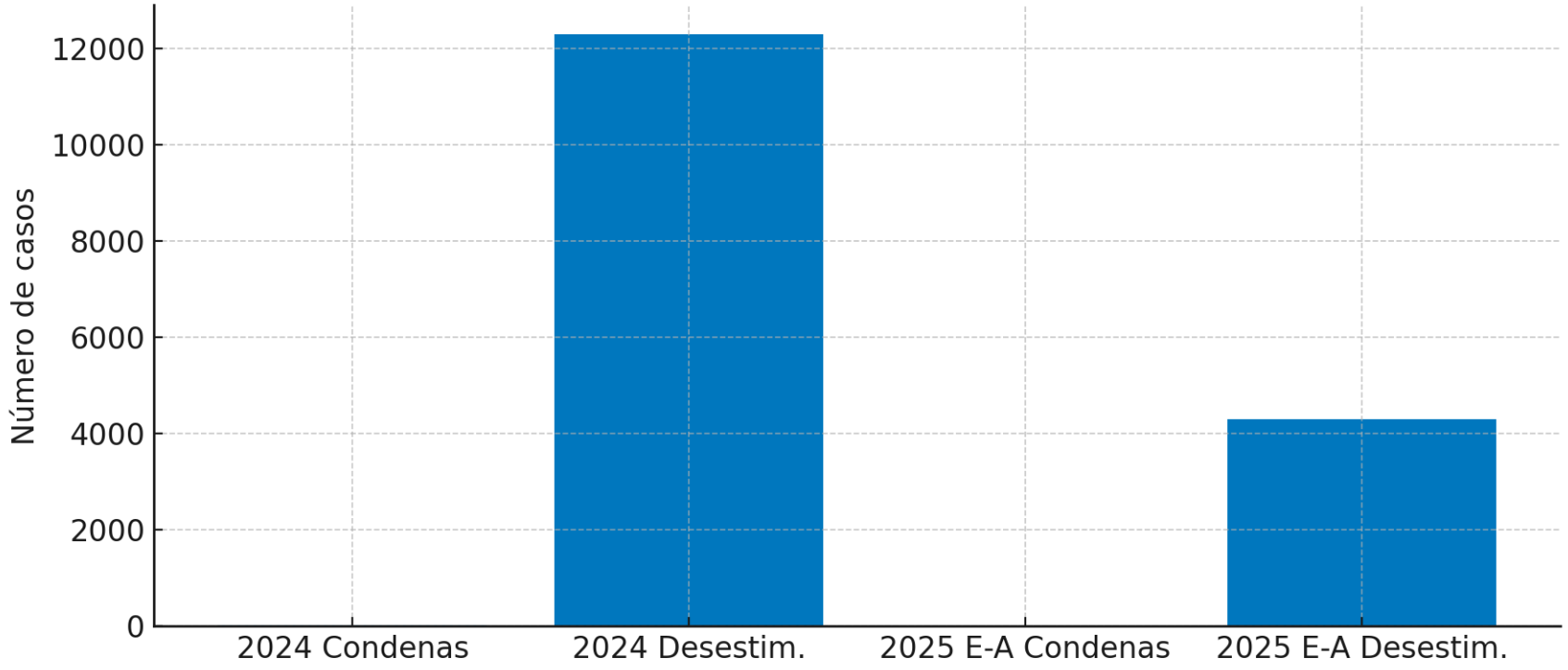


98% del tráfico IoT sigue sin cifrar

57% de los dispositivos tiene vulnerabilidades Medias/Altas

80 grupos de ransomware han atacado plantas industriales

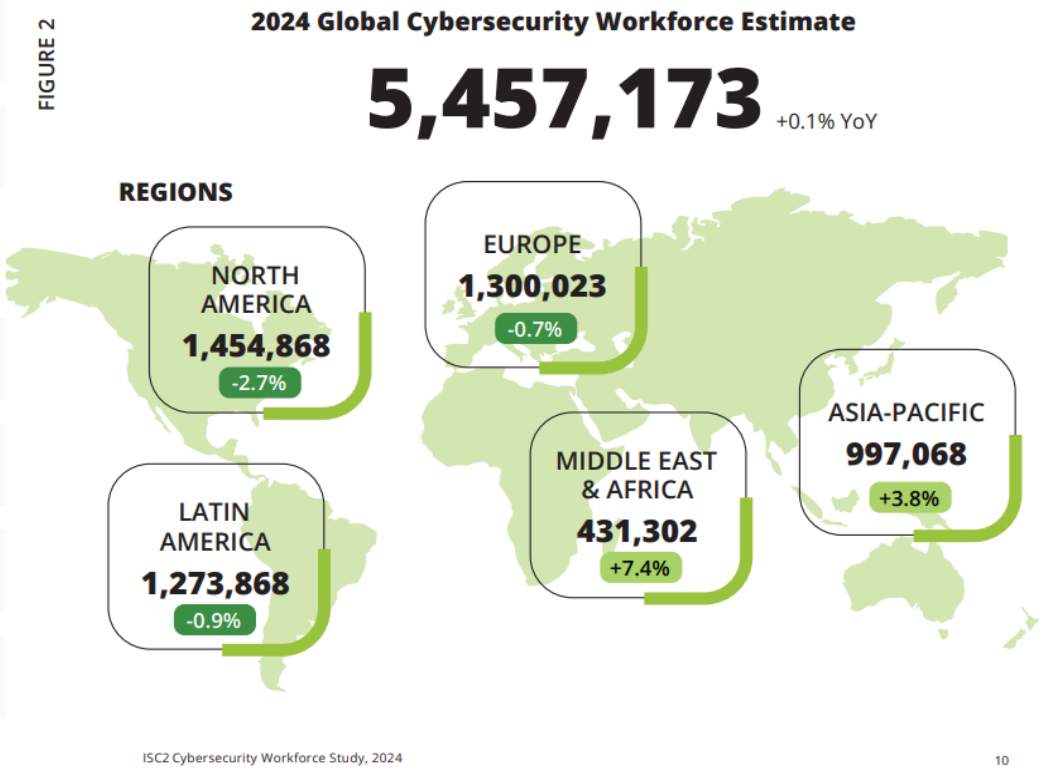
Impunidad en Delitos Informáticos – Costa Rica



Fuente: Poder Judicial CR – 2025

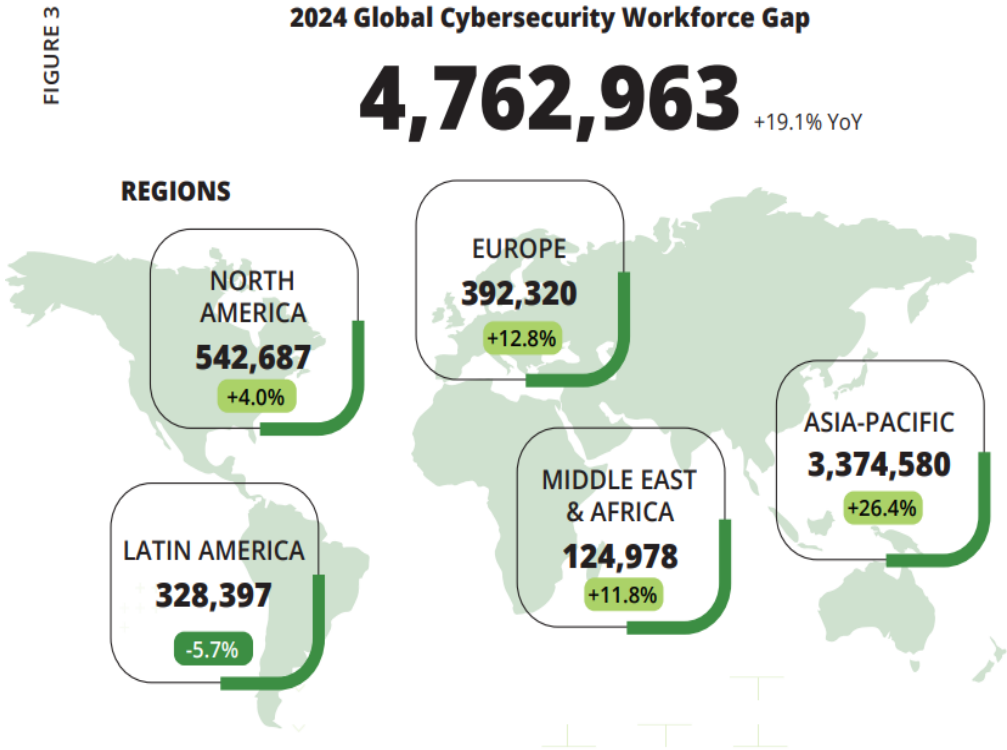
Brecha de Habilidades

FIGURE 2



ISC2 Cybersecurity Workforce Study, 2024

FIGURE 3



La nueva realidad

Desalineación con la industria

Falta de Habilidades Prácticas

Desconexión con sectores estratégicos

Disrupción Académica

Modelo basado en Competencias + Emulación/Simulación

Enseñanza Transdisciplinaria

Aprendizaje Invertido y desafíos abiertos

Vínculo temprano con la industria (Pública / Privada)

Formación Continua y Modular para Profesionales

Disrupción Académica

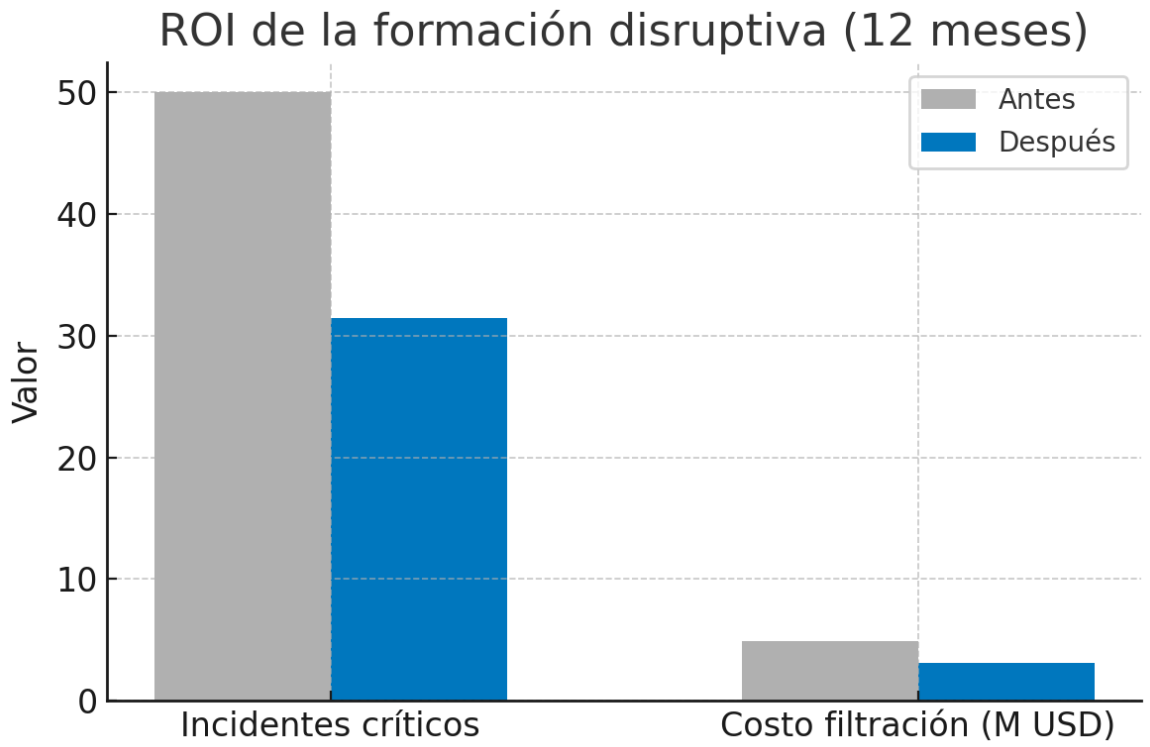
Las universidades deben convertirse en Centros Vivos de Ciberdefensa

Transición Académica

"Si el enemigo innova cada semana, nuestra aula no puede actualizarse cada SEMESTRE"

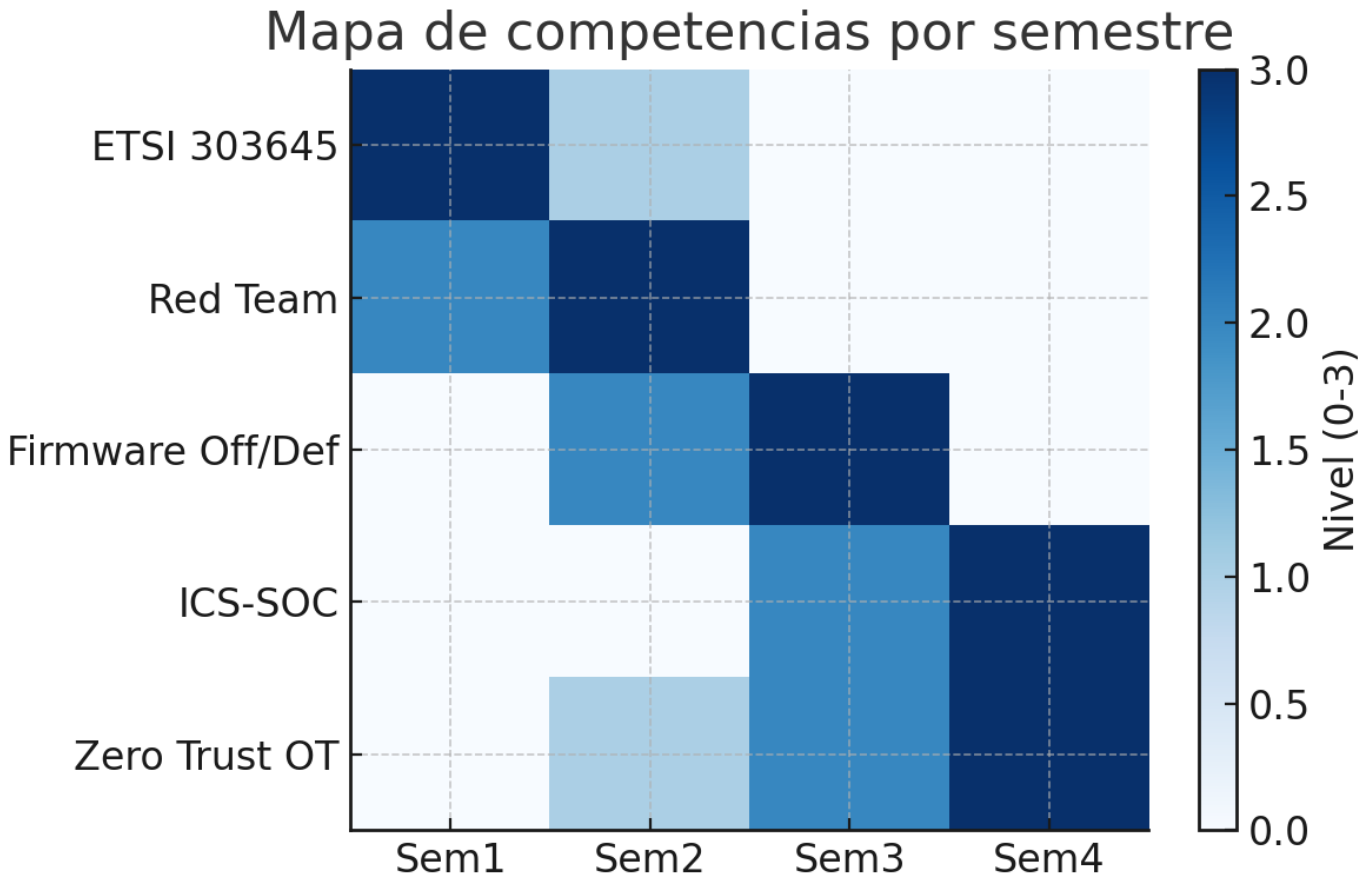
- Normativa y Política Pública
- Psicología del Adversario
- Afectación a la cadena de suministro
- Convergencia en Carreras NO-TI
- IoT Pentest
- Desarrollo de Código Seguro en IoT

ROI de la formación disruptiva



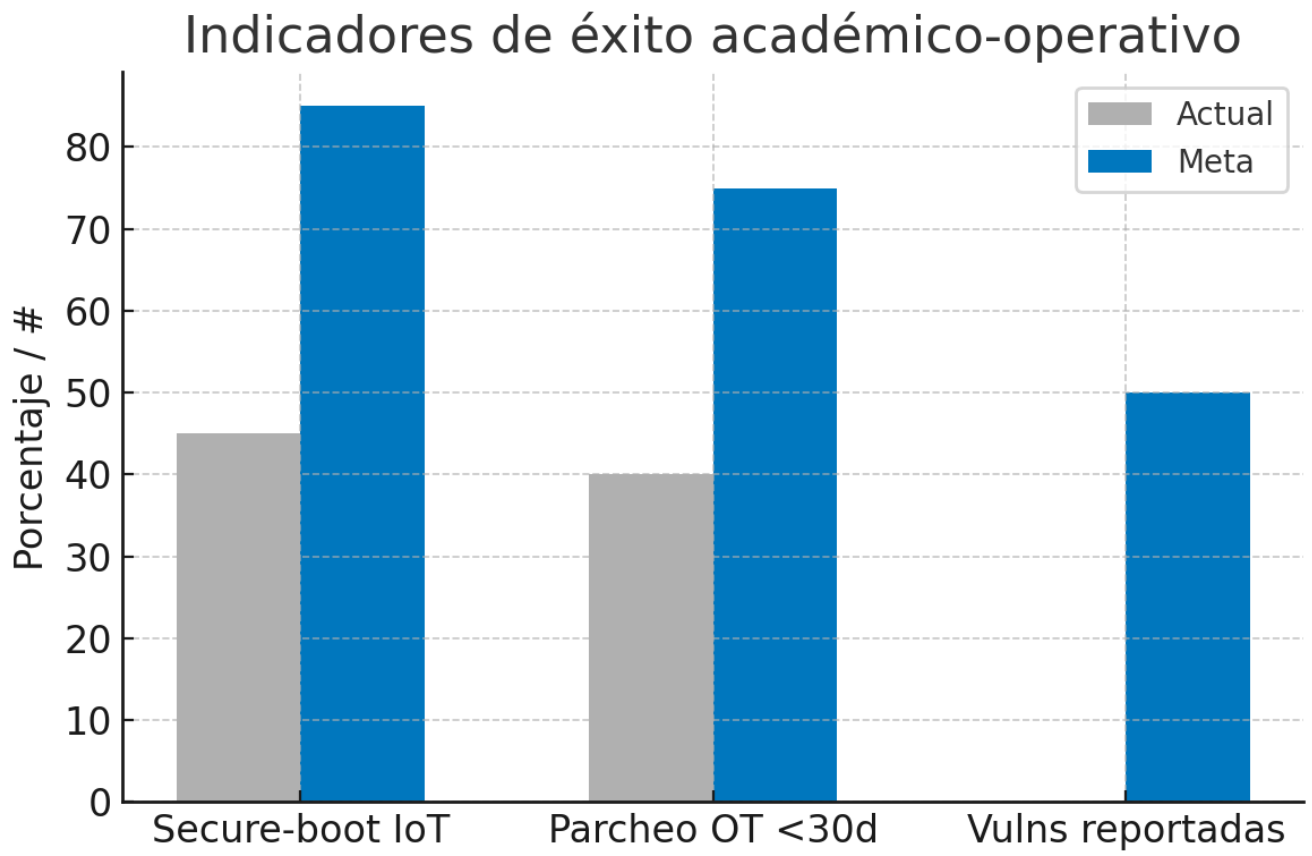
Fuentes: SANS Cyber Range ROI Survey 2024; IBM Cost of a Data Breach 2024

Mapa de competencias por semestre



Fuentes: NICE Framework 2024; ENISA Skills Matrix 2023; Diseño curricular interno

Indicadores de éxito académico-operativo



Fuentes: Dragos ICS Year-in-Review 2024; Eclipse IoT Developer Survey 2025

Conclusiones

- La Ciberseguridad, especialmente en IoT exige un salto cualitativo, no incremental.
- La frontera entre ingeniería, ética y política pública ya NO existe.
- La experiencia práctica es la nueva moneda de la empleabilidad.
- El ciclo de aprendizaje debe ser reducido.
- La métrica definitiva es reducir la superficie de ataque y la exposición real.

“La brecha no es solo de talento; si enseñamos igual que ayer, defenderemos el mañana con herramientas del pasado.”