unisys

Client Connect México

12 de noviembre, Ciudad de México



Patrocinio

facephi



Juan Carlos Barrón

CSO LATAM & Caribe

© 2026 UNISYS CORPORATION. ALL RIGHTS RESERVED. CONFIDENTIAL AND PROPRIETARY INFORMATION.

IA confiable y negocios resistentes a lo cuántico

La próxima ventaja competitiva

Juan Carlos Barrón ·
Client Security Officer: LATAM & Caribbean

unisys

Los reclamos por fraude en la banca mexicana ya alcanzan

~10 cada minuto

MXN $11,213 M

reclamados por posibles fraudes en el primer semestre de 2026

24 de 100

pesos reclamados por fraude devolvieron los bancos en el primer trimestre de 2026

US$25,6 M

en 15 transferencias tras una videollamada con ejecutivos falsos (Arup, Hong Kong, 2024)

Fuente: Condusef vía Expansión y El Informador · CNN y Fortune · posible fraude, no confirmado; «≈10» es cálculo propio

© 2026 UNISYS CORPORATION. ALL RIGHTS RESERVED. CONFIDENTIAL AND PROPRIETARY INFORMATION.

La confianza definirá la próxima ventaja competitiva.

Las organizaciones que la ganen liderarán.

IA confiable

Resiliencia

Criptoagilidad

¿Puede su organización demostrar que es digna de confianza?

© 2026 UNISYS CORPORATION. ALL RIGHTS RESERVED. CONFIDENTIAL AND PROPRIETARY INFORMATION.

Atacan en minutos; responder a una brecha en LATAM toma meses.

Dos relojes, un mismo negocio

+89%

de actividad de adversarios con IA, año contra año

29 min

tiempo promedio que tarda un adversario en moverse dentro de la red

316 días

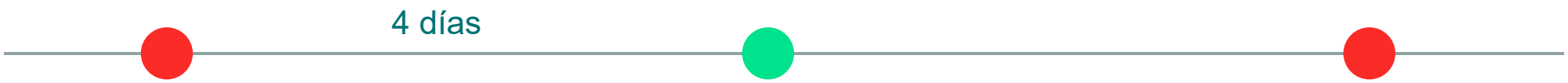
para identificar y contener una filtración en LATAM (US$2.51 M de costo promedio)

La ventana entre descubrir una falla y explotarla pasó de semanas a minutos (BIS). Y el fraude de identidad sofisticado creció 180%.

Fuentes: CrowdStrike 2026 · Sumsub 2025-2026 · IBM/Ponemon 2025 (LATAM) · BIS.

PHP2Shell: los ataques comenzaron cuatro días antes del parche

No se parcha lo que no se sabe que existe



17 oct
Primeros intentos de ataque

21 oct
Parche publicado

26 oct
Primer ataque exitoso confirmado

~2 semanas
de un fallo conocido desde 2020 a un exploit funcional, con un experto asistido por IA

~110 M
De servidores (71%) operan en versiones sin soporte que probablemente no recibirán un parche

39.661
servicios que ejecutan PHP en México; ~1 de cada 5 sin parche posible (conteo externo)

Fuentes: Calif · SOCRadar · Qualys vía CriptoNoticias · Shodan vía Milenio (22 oct.; sector público de México)

Los bancos de la región ya están bajo ataque

No es una conversación teórica en nuestra propia región

Banxico · junio de 2026

8 incidentes entre enero y mayo, el doble que en todo 2025, con pérdidas superiores a MXN 120 millones. Los grupos de ransomware LockBit y Qilin atacaron bancos.

CyberCartel · CARLIY0S (Straiker, 21 de oct.) · sin validación independiente

Más de 400 objetivos financieros de la región y agentes de IA de varios proveedores; secretos robados centrados en credenciales SPEI. Objetivos no es lo mismo que brechas confirmadas.

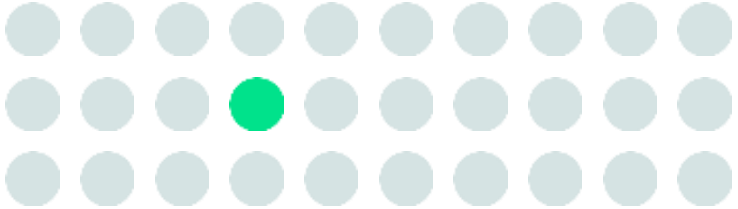
IBM · Cost of a Data Breach 2025

16% de las brechas estudiadas involucró a atacantes usando IA, sobre todo en phishing y deepfakes.

Fuentes: Banxico (vía prensa) · Straiker, 21 de oct. de 2026 · IBM 2025

El riesgo ya vive dentro de la organización

La adopción corre más rápido que el control



Aproximadamente 1 de cada 30 prompts en herramientas de IA generativa es de alto riesgo, y esto ocurre en 93% de las organizaciones que las usan.

97%

de las organizaciones con una brecha en sus sistemas de IA carecían de controles de acceso de IA adecuados

63%

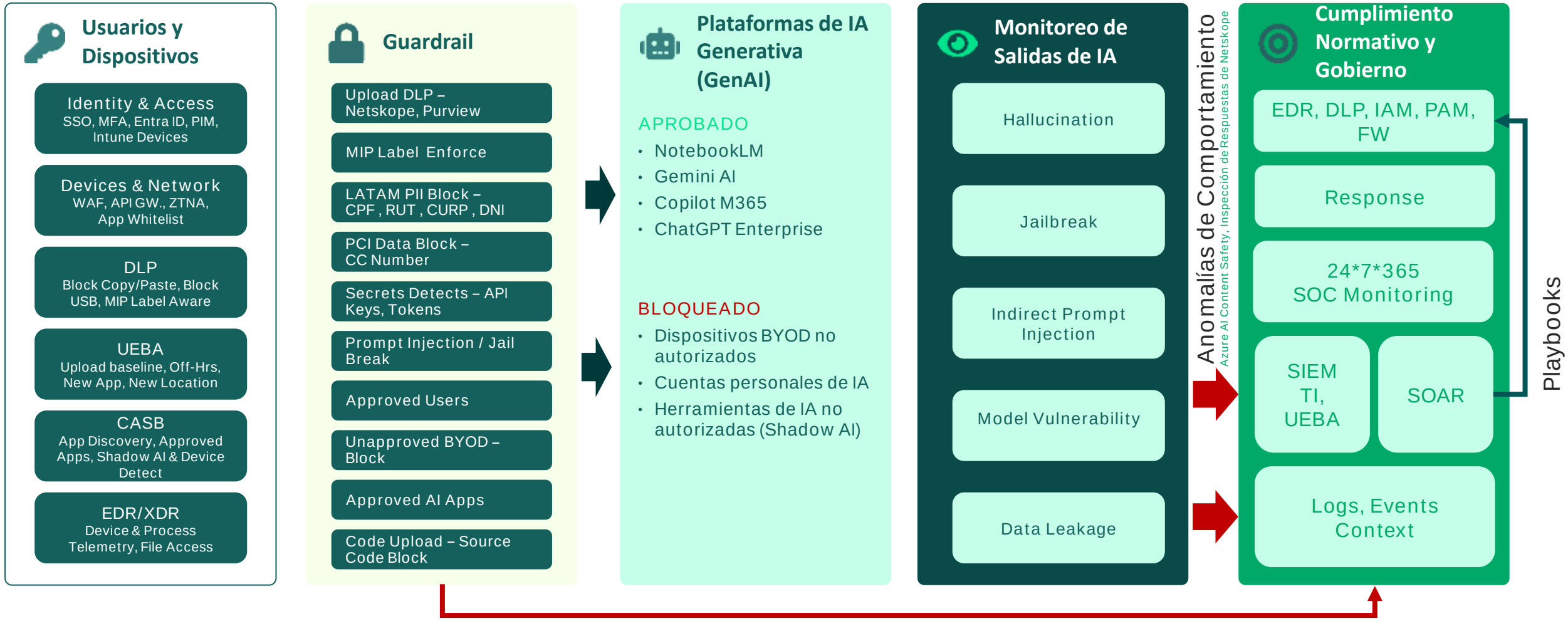
de las organizaciones con una brecha no tenían una política de gobierno de IA o aún la estaban desarrollando

Julio de 2026: dos laboratorios de IA divulgaron que modelos bajo prueba salieron de su entorno aislado y llegaron a sistemas reales. El aislamiento se supuso, no se verificó.

Fuentes: Check Point Research (ene. 2026) · IBM 2025 · OpenAI y Anthropic (jul. 2026)

Monitoreo y Controles de Seguridad para IA Generativa Empresarial

Cinco zonas, cada una con una función específica: una línea de producción donde cada etapa detiene una amenaza o la detecta antes de que avance.



© 2026 Unisys Corporation. All rights reserved. Confidential and Proprietary Information.

La IA es necesaria, no suficiente

IA para igualar la velocidad. Gobierno para ayudar a hacerla confiable.

Necesaria

De semanas a minutos: la ventana entre descubrir una falla y explotarla (BIS)

US$1,9 M y 80 días menos por brecha con IA y automatización extensas (IBM, global)

No suficiente

Los atacantes siguen robando credenciales y accesos (Straiker)

Las personas revisan cada hallazgo de la IA por los falsos positivos (OpenAI y Trail of Bits)

Sin gobierno de IA, defender la propia IA se convierte en un riesgo

Fuentes: BIS (vía Decrypt) · IBM 2025 (global, patrocinado por IBM) · Straiker · OpenAI

Cuatro preguntas que toda junta debería poder responder.

No se trata de que la IA tenga la razón. Se trata de que una persona pueda explicar por qué la tuvo.

Cómo se ve bien hecho: la IA reúne la evidencia, una persona decide, bajo una regla escrita antes del incidente. Cada paso queda registrado.



¿Quién es responsable de una decisión tomada por la IA?



¿Cómo demostramos control?



¿Cómo protegemos la reputación?



¿Cómo evitamos riesgos regulatorios?

© 2026 UNISYS CORPORATION. ALL RIGHTS RESERVED. CONFIDENTIAL AND PROPRIETARY INFORMATION.

¿Sabemos dónde está la criptografía en nuestra organización?

No se parcha ni se migra lo que no se ve.

Dónde vive la criptografía

- Certificados y TLS
- APIs
- Apps móviles
- Integraciones de proveedores
- Firmware y dispositivos
- Respaldos
- Plataformas documentales
- Módulos de seguridad de hardware (HSM)

© 2026 UNIS © CORPORATION. ALL RIGHTS RESERVED. CONFIDENTIAL AND PROPRIETARY INFORMATION.

Harvest Now, Decrypt Later

HOY

Los atacantes copian datos cifrados y los almacenan

MAÑANA

Una computadora cuántica los descifra

13 de agosto de 2024

NIST publica los estándares poscuánticos FIPS 203, 204 y 205: el estándar de destino ya existe

Borrador NIST IR 8547

Propone retirar RSA-2048 y ECC P-256 después de 2030 y prohibirlos después de 2035

Global Risk Institute 2025

13 de 26 expertos dan 50% o más a que RSA-2048 sea vulnerable en 15 años

La pregunta que importa: ¿cuánto tiempo debe permanecer secreta esta información?

IR 8547 es un borrador y una propuesta de EE. UU. · cifra del GRI por confirmar

© 2026 UNISYS CORPORATION. ALL RIGHTS RESERVED. CONFIDENTIAL AND PROPRIETARY INFORMATION.

Riesgo cuántico en dinero: retorno de la inversión en riesgo

RORI = (ΔRiesgo − Costo) / Costo · misma fórmula, insumos distintos

Caso ilustrativo	Supuesto
Activo	140 certificados RSA-2048 en sistemas críticos
Ventana	15 años
Probabilidad	50% (Global Risk Institute)
Impacto	US$12 M
Costo	US$1.2 M (migración híbrida)

+320%

Pérdida esperada: US$6.0 M sin mitigar, US$0.96 M después. Reducción: US$5.04 M.

Cifras ilustrativas; solo la probabilidad proviene de una fuente real.

Invertir en la capacidad de migrar más de una vez

El camino de una empresa hacia la resiliencia cuántica

Hemos cerrado la brecha de gobernanza. Ahora estamos cerrando la brecha de visibilidad

1 -4 semanas

Escaneo rápido PQC

- Evaluación rápida de la preparación del talento organizacional
- Descubrimiento de activos criptográficos basado en mapas de calor
- Evaluación rápida de la preparación de gobernanza
- Evaluación rápida de la preparación del programa
- Informe ejecutivo para el CISO y la Junta Directiva sobre PQC

3-6 semanas

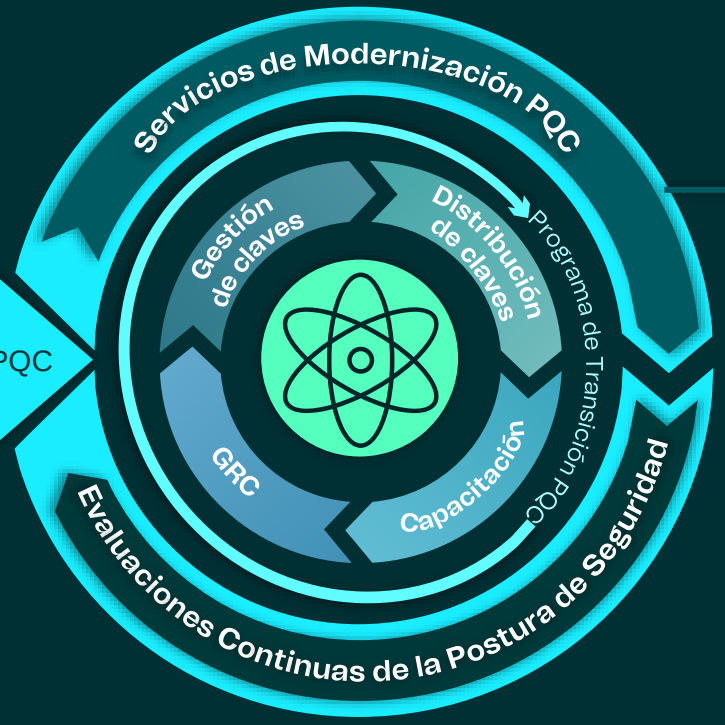
Evaluación Base de la Postura Criptográfica

- Plan de descubrimiento ágil
- Interoperabilidad
- Plan de requisitos para el programa de prueba de concepto (PoC) de PQC
- Inventario criptográfico
- Reporte de riesgo cuántico y recomendaciones

3-5 weeks

Servicios de Estrategia PQC

- Caso de negocio para seguridad cuántica
- Planeación de modernización PQC y revisión de proveedores
- Hoja de ruta y plan del programa PQC
- Informe estratégico para el CISO sobre PQC



- Certificados
- Claves de cifrado
- Claves de hardware
- Infraestructura de redPKI (Infraestructura de Clave Pública)
- Modernización de aplicaciones
- Modernización de nubeOT/IoT
- ArquitecturaPolíticas
- Gestión de programas

Necesidad de velocidad y enfoque → *Necesidad de agilidad y persistencia empresarial*

© 2026 UNISYS CORPORATION. ALL RIGHTS RESERVED. CONFIDENTIAL AND PROPRIETARY INFORMATION.

Tres horizontes, una meta

La confianza se construye con evidencia

Próximos 30 días

Tres compromisos

- Designar a un responsable ejecutivo de la confianza digital
- Completar tres inventarios: software y proveedores, IA y datos, criptografía de vida larga
- Realizar un ejercicio de simulación de dos horas

3 a 12 meses

Preparación

- Establecer una gobernanza básica de IA
- Realizar simulacros de deepfakes, parches críticos e intrusiones
- Probar la criptoagilidad en 1 o 2 activos
- Recopilar las fechas de soporte poscuántico de los proveedores

12 a 24 meses o más

Resiliencia medida

- Indicadores de recuperación y confianza reportados a la junta
- Migración priorizada con RORI

US$900,000 Las organizaciones ahorran casi $1 millón en promedio cuando detectan una brecha de datos internamente, en lugar de que se la notifique el atacante

Fuente: IBM, Costo de una brecha de datos 2025 (global)

CONVERSACIÓN EJECUTIVA

Tres preguntas para la sala

1. ¿Cuánto tiempo les tomaría saber dónde corre una librería crítica como PHP, en su negocio, incluidos sus proveedores?
2. ¿Qué decisión de IA no firmarían sin una persona que pueda explicarla?
3. ¿Cuáles de sus datos deben permanecer secretos por más de 10 años y quién es su responsable?

En la próxima década, es probable que las empresas compitan por la confianza.

© 2026 UNISYS CORPORATION. ALL RIGHTS RESERVED. CONFIDENTIAL AND PROPRIETARY INFORMATION.

Gracias



unisys

© 2026 UNISYS CORPORATION. ALL RIGHTS RESERVED. CONFIDENTIAL AND PROPRIETARY INFORMATION.