TENDENCIAS DE CIBERSEGURIDAD 2026 EN MÉXICO

BLACKit!

IVAN PEDROZA PAZ

A lo largo de los años he aprendido que la resiliencia no es solo resistir, sino levantarse con más conocimiento. Y que la empatía no es debilidad, sino la herramienta más poderosa para liderar en medio del caos.

Mi meta va más allá de resolver el problema de hoy. Quiero trascender: poner mi experiencia al servicio de otras organizaciones, para que, cuando llegue la tormenta, estén mejor preparadas. Por eso doy lo mejor de mí cada día.

BLACKit!

MALWARE IMPULSADO POR IA:
ATAQUES MÁS AUTÓNOMOS Y EVASIVOS

Los atacantes están usando IA para crear malware que se adapta en tiempo real, cambia su comportamiento y evade controles tradicionales. Esto incluye troyanos bancarios, ransomware y malware para pagos móviles.

Impacto en México:

- Mayor riesgo en banca digital, SPEI, fintechs y pagos móviles.
- Aumento de ataques silenciosos que permanecen más tiempo sin ser detectados.

BLACKit!

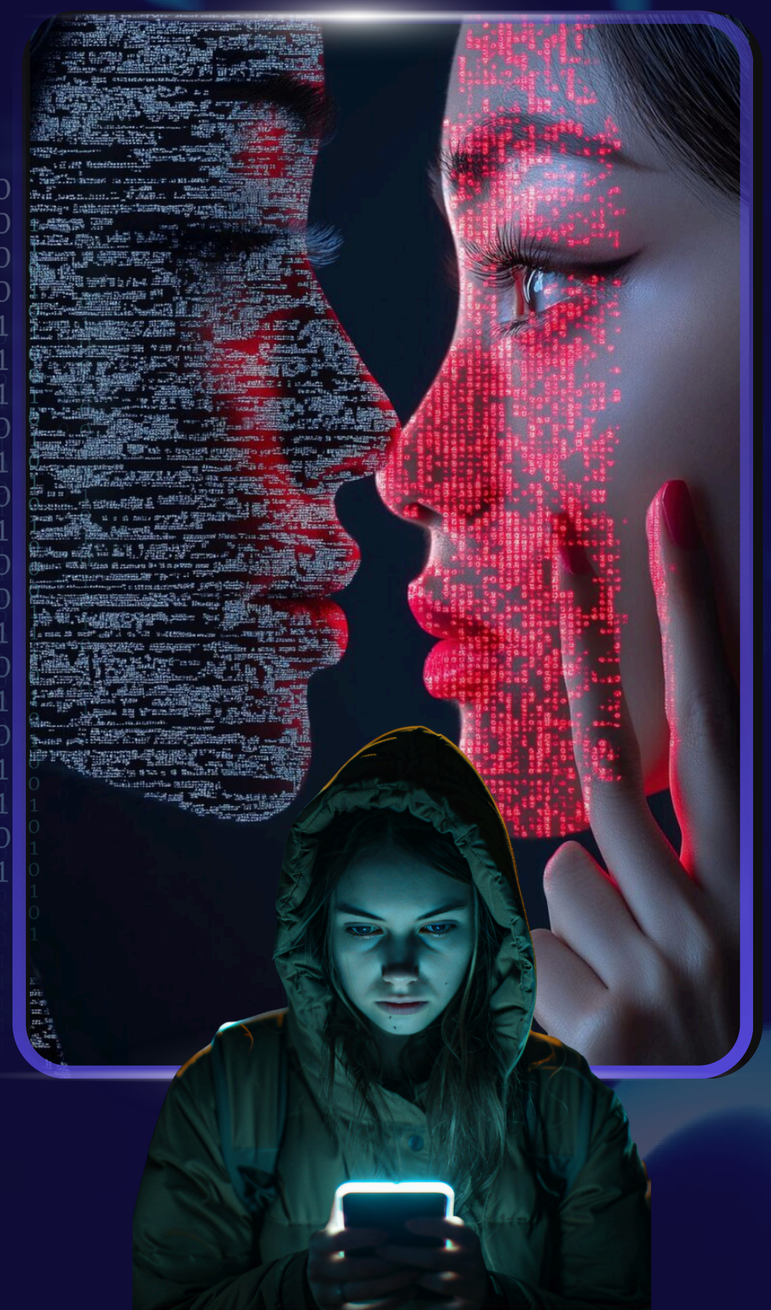
FRAUDE FINANCIERO EN PAGOS MÓVILES
NFC Y BILLETERAS DIGITALES

- El crecimiento de pagos sin contacto y apps financieras está generando un aumento de ataques dirigidos a NFC, wallets y apps bancarias.

Impacto en México:

- Usuarios de CoDi, wallets de bancos y fintechs son objetivo.
- Empresas con apps móviles deben reforzar seguridad en endpoints y APIs.

BLACK it!



Empresas con apps móviles deben reforzar seguridad en endpoints y APIs.

Los atacantes usan IA para crear mensajes, voces y videos falsos extremadamente convincentes.

Impacto en México:

- Suplantación de ejecutivos para autorizar transferencias.
- Fraudes a clientes vía WhatsApp, llamadas y redes sociales.
- Riesgo elevado para áreas de tesorería, finanzas y operaciones.

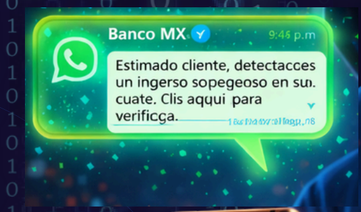
BLACKit!

Troyanos bancarios distribuidos por WhatsApp

Los troyanos bancarios están siendo reescritos para propagarse masivamente por WhatsApp, uno de los canales más usados en México.

Impacto en México:

- Afecta a clientes bancarios y empleados.
- Riesgo para empresas que usan WhatsApp Business sin controles.



BLACKit!

Ataques a SPEI, corresponsales, ATMs y cadena de suministro

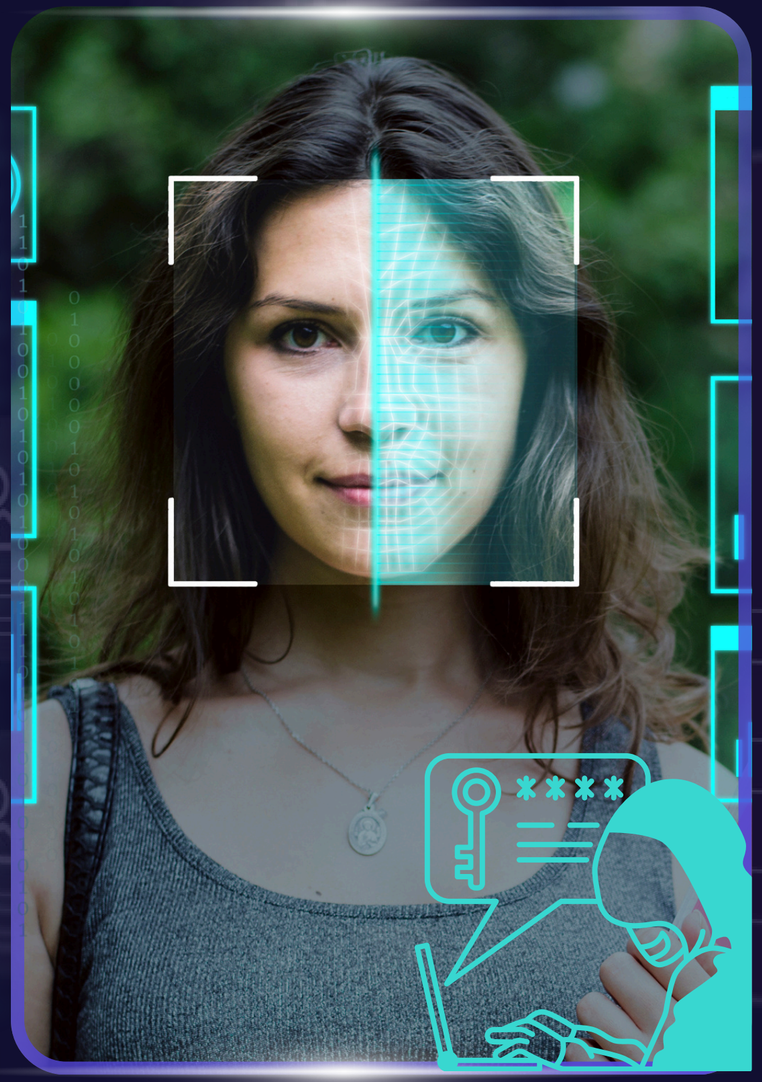
Los atacantes están apuntando a infraestructura crítica financiera, incluyendo:

- SPEI
- ATMs
- POS
- Switches de pago
- Proveedores de nube y software

Impacto en México:

- Riesgo para bancos, SOFIPOs, fintechs y adquirentes.
- Mayor escrutinio regulatorio de CNBV y Banxico.

BLACKit!



Identidad como nuevo perímetro:
credenciales robadas como principal vector

La mayoría de los ataques exitosos comienzan con credenciales comprometidas, no con vulnerabilidades técnicas.

Impacto en México:

- Accesos privilegiados mal gestionados.
- Proveedores externos con permisos excesivos.
- Sesiones secuestradas en banca digital y nube.

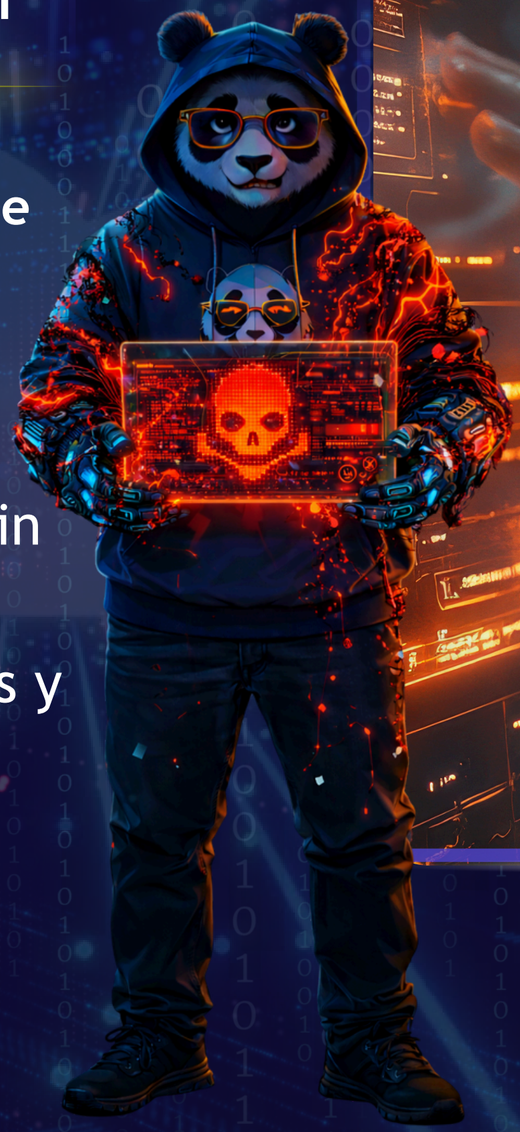
BLACKit!

Abuso de la nube y automatización del cibercrimen

Los atacantes usan infraestructura en la nube para escalar ataques, ocultar origen y automatizar campañas.

Impacto en México:

- Empresas migrando a nube sin controles Zero Trust.
- Riesgo en APIs, contenedores y microservicios.



BLACKit!

Ransomware más agresivo y orientado a extorsión múltiple

El ransomware sigue creciendo, afectando al 12.8% de organizaciones financieras globales en 2025.

Impacto en México:

- Robo de datos + cifrado + extorsión pública.
- Ataques a bancos, aseguradoras, fintechs, retail y energía.

BLACKit!


PRINCIPALES ATAQUES
QUE ENFRENTARÁN
LAS EMPRESAS MEXICANAS EN 2026
CYBER SECURITY
BLACKit!

1. Fraude financiero automatizado con IA

- Transferencias no autorizadas
- Manipulación de apps móviles
- Suplantación de identidad con deepfakes

2. Ataques a pagos móviles y NFC

- Interceptación
- Clonación
- Malware en dispositivos

3. Troyanos bancarios por WhatsApp

- Robo de credenciales
- Secuestro de sesiones
- Vaciamiento de cuentas

BLACKit!

4. Ransomware dirigido a infraestructura crítica

- Bancos
- Fintechs
- Retail con POS
- Energía y gasolineras

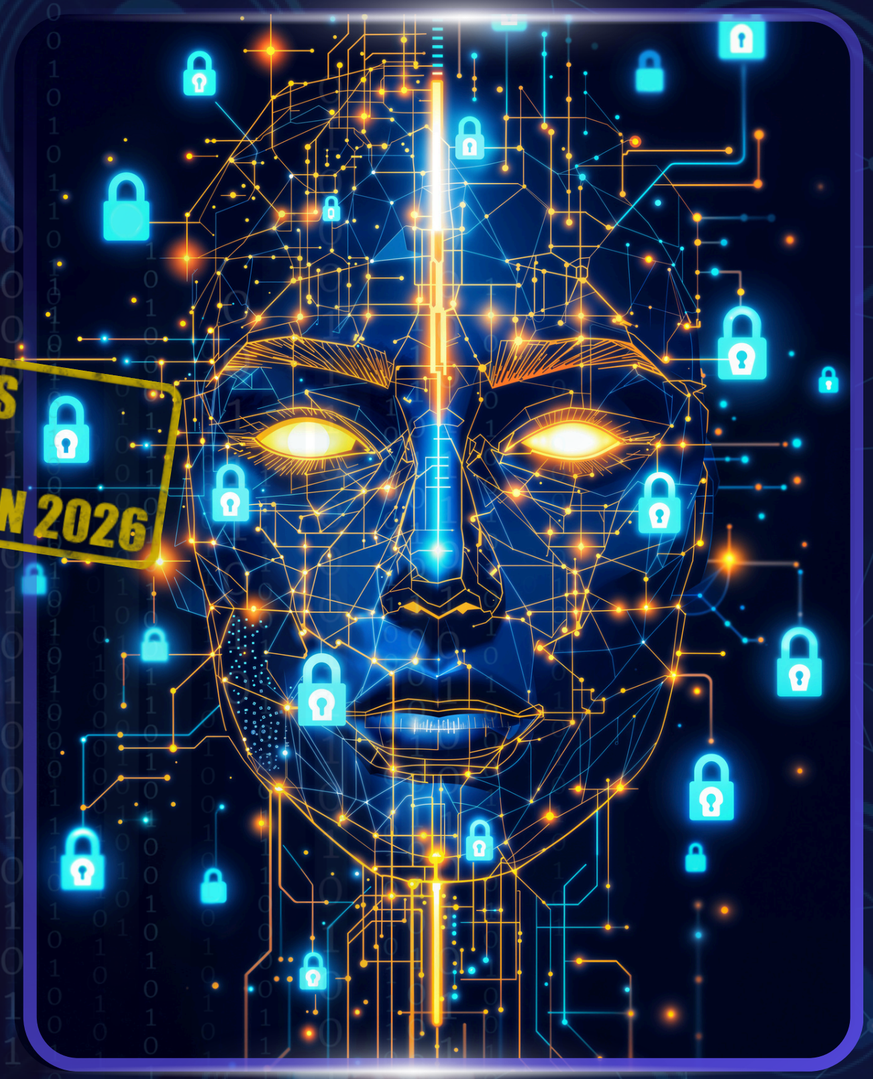
5. Ataques a la cadena de suministro

- Proveedores de software
- Nube
- Integradores
- Switches de pago

6. Compromiso de identidad y accesos privilegiados

- Secuestro de tokens
- Abuso de sesiones
- Accesos excesivos

PRINCIPALES ATAQUES QUE ENFRENTARÁN LAS EMPRESAS MEXICANAS EN 2026



BLACKit!

Qué deben hacer las empresas mexicanas en 2026

Prioridades estratégicas

- Zero Trust real (no solo MFA).
- Protección de identidad y accesos privilegiados.
- Seguridad en apps móviles y APIs.
- SOC con IA defensiva y XDR.
- Simulacros de respuesta a incidentes.
- Evaluación continua de proveedores.
- Políticas claras y visuales para toda la organización.

Ciberseguridad Después del Ataque

1. Situación Inicial

- Tipo de ataque detectado
- Sistemas afectados
- Impacto preliminar (operación, clientes, reputación)
- Riesgos inmediatos

2. Contención Inmediata

- Aislamiento de sistemas comprometidos
- Activación de BCP/DRP
- Revocación de accesos críticos
- Monitoreo de movimientos laterales
- Comunicación interna de emergencia

BLACKit!

Ciberseguridad Después del Ataque

3. Investigación Forense

- Vector de entrada identificado
- Alcance del compromiso
- Datos o procesos afectados
- Línea de tiempo del ataque
- Participación de terceros o proveedores

4. Comunicación Estratégica

Audiencias clave:

- Reguladores (CNBV, Banxico, UIF)
- Clientes
- Proveedores
- Empleados
- Consejo / Comité de Riesgos

Mensajes:

- Qué ocurrió
- Qué se está haciendo
- Qué deben hacer ellos
- Cómo se protegerán a futuro

BLACKit!

Ciberseguridad Después del Ataque

5. Remediación Técnica

- Parcheo y corrección de vulnerabilidades
- Reconfiguración de accesos y privilegios
- Revisión de integridad de sistemas críticos
- Sustitución de hardware comprometido (ATMs, kioscos, POS, IoT)
- Validación de proveedores y terceros

6. Revisión de Gobernanza

- Evaluación del modelo de riesgos
- Roles y responsabilidades durante la crisis
- Cumplimiento de políticas
- Efectividad del SOC / monitoreo
- Lecciones organizacionales

7. Cultura y Capacitación

- Entrenamiento post-incidente
- Simulacros de respuesta
- Campañas de phishing y concientización
- Protocolos visuales y simples para toda la organización

BLACKit!

Ciberseguridad Después del Ataque

8. Fortalecimiento Estratégico

- Zero Trust
- MFA universal
- XDR/EDR/SIEM modernizado
- Automatización de respuesta
- Red teaming periódico
- Integración de ciberseguridad en ESG

9. Roadmap de Resiliencia

Corto plazo (0–30 días)

- Contención, remediación, comunicación, cumplimiento regulatorio

Mediano plazo (30–120 días)

- Reforzamiento técnico, rediseño de políticas, capacitación

Largo plazo (120+ días)

- Evolución del modelo de seguridad, SOC avanzado, cultura resilient

BLACKit!

Ciberseguridad Después del Ataque

10. Métricas de Recuperación

- Tiempo de contención
- Tiempo de recuperación
- Sistemas restaurados
- Incidentes recurrentes
- Cumplimiento regulatorio
- Percepción de clientes y empleados

BLACKit!

BLACKit!

LO S1MPL3 TE L1BER4

Gracias

GUADALAJARA • CDMX • LEÓN • BAJA CALIFORNIA