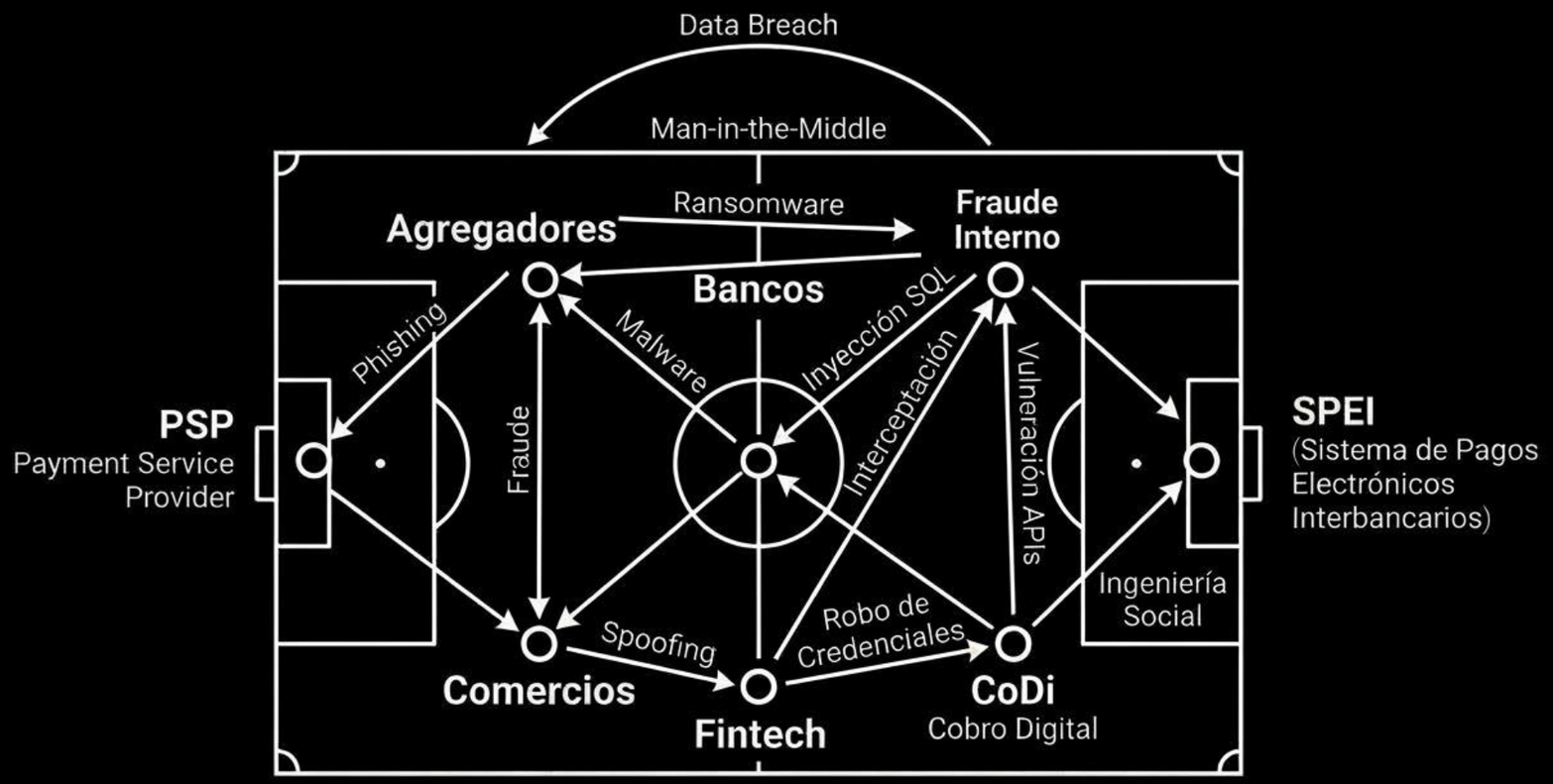


Lo que está en juego cuando la ciberseguridad no es prioridad

ANDRÉS VELÁZQUEZ, CISSP, GCFA, IEM

PRESIDENTE Y FUNDADOR DE MATTICA

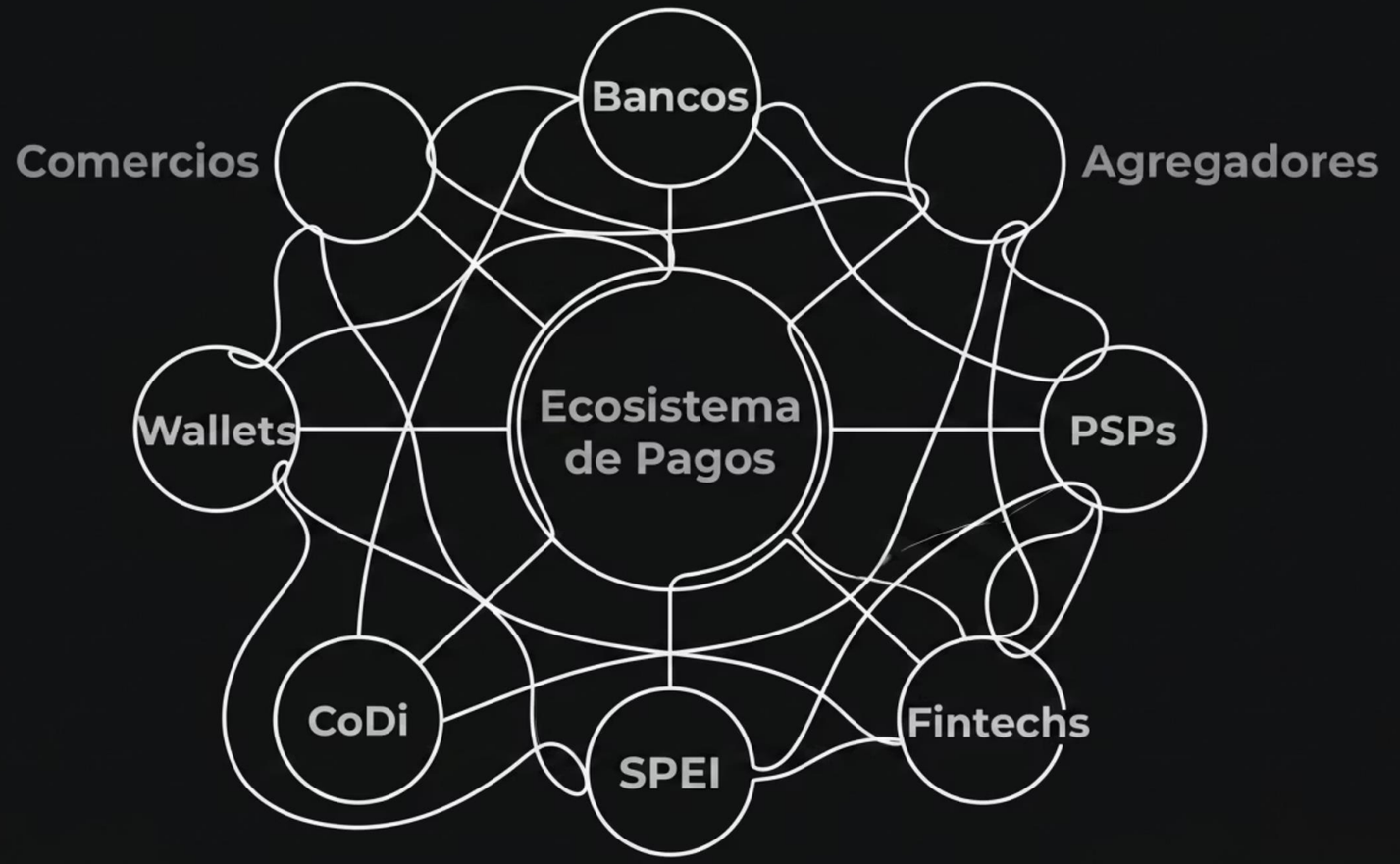
El partido ya empezó.
¿Estás jugando o solo leyendo el reglamento?

MX $483 M

en quebrantos en el sector financiero mexicano por ciberataques en 2024. El monto más alto en 3 años.

Fuente: Banco de México, 2025

El ecosistema de medios de pago en México



Cada conexión es un vector de riesgo. Nadie opera en aislamiento.

El partido no solo ya cambió.

está a punto de cambiar mucho más rápido.

El campo de juego está creciendo — ahora mismo.

7,300 millones de transferencias SPEI en 2025 — 16.8 veces el de México.

Para 2026, SPEI superará a tarjetas de débito y crédito en volumen de operaciones.

75% de los adultos en México usa SPEI. En CDMX, 50% de los los pagos ya son electrónicos.

Banxico publicó en marzo 2026 la reforma para estandarizar y simplificar las transferencias en todas las apps.

Banco del Bienestar integrará SPEI, CoDi y DiMo en su app app antes de cierre de 2026 — millones de nuevos usuarios entrando al sistema.

Más volumen. Más simplicidad. Más intermediarios conectados.

¿Alguien está calculando lo que eso significa?

Banco de México, Convención Bancaria 2026 · Reforma Circulares 3/2012 y 14/2017, marzo 2026.

PAIN 1

El ecosistema conectado es la vulnerabilidad

Una brecha en un agregador **es una brecha en todos sus clientes.** La interconexión que hace eficiente al sistema también lo hace frágil.

⚠ En 2025, más del 60% de los incidentes graves involucraron a un tercero en la cadena.

Los intermediarios son el blanco preferido.

No porque sean el equipo más débil.
Porque son el acceso al torneo completo.

74%

de las brechas en el sector financiero tienen origen en un proveedor, intermediario o tercero.

Fuente: IBM Cost of a Data Breach Report.

Artemis II tenía el manual, cumplía, pero...

Cumplir no es lo mismo que estar protegido

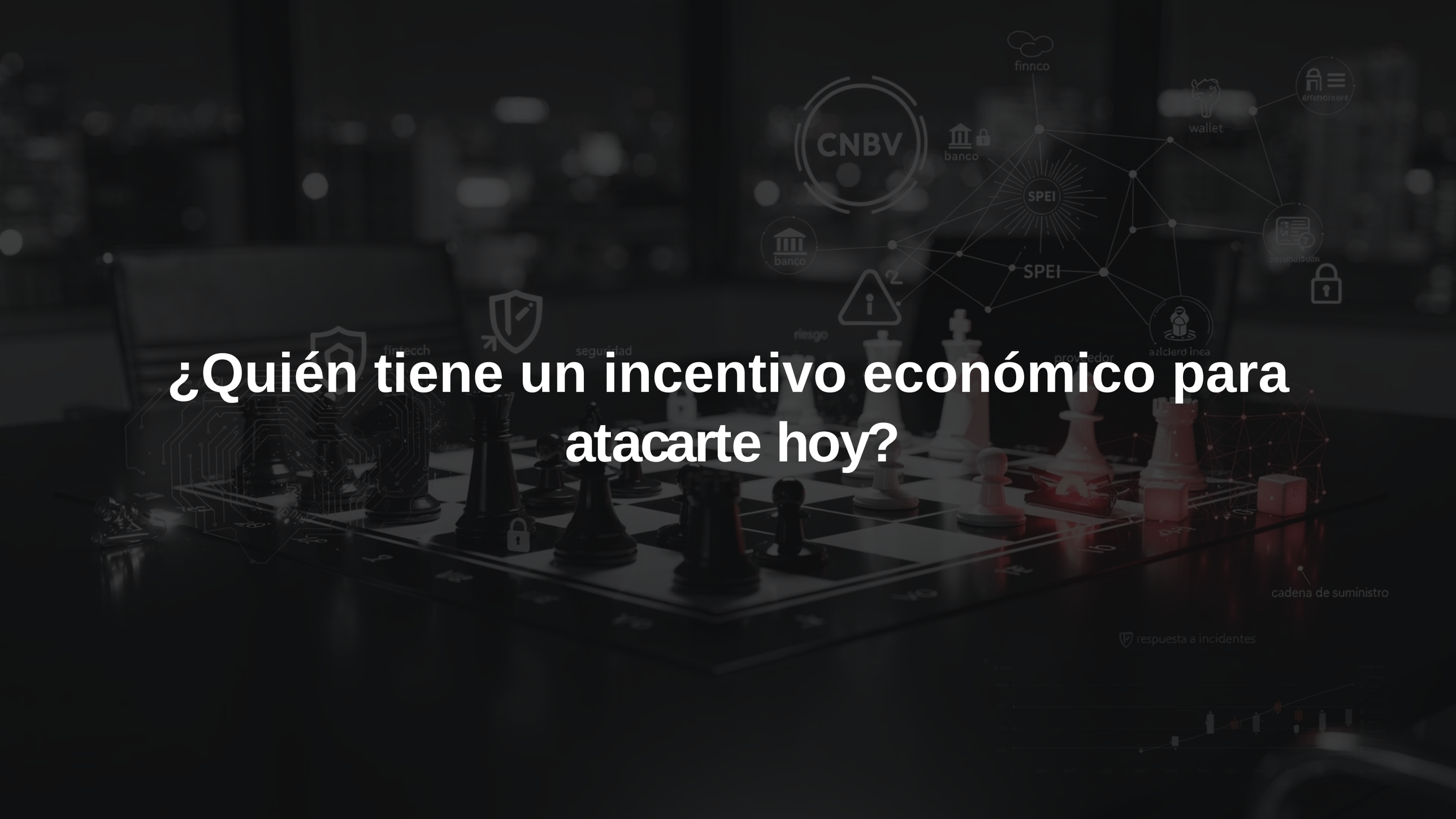
¿Cuántos controles tienen hoy que nacieron de copiar un framework y no entender su riesgo real?

Puedes pasar todas las auditorías y aún así ser vulnerable. **El checklist no simula a un adversario real.**

La mayoría de las empresas que sufrieron brechas cumplían con su marco regulatorio en el momento del ataque.

La ventaja no es tener más reglas.

Se trata de entender cómo piensa el rival.



¿Quién tiene un incentivo económico para atacarte hoy?

Esta semana:

¿Cuáles son tus activos más valiosos?

¿Por dónde entraría alguien que te quiere atacar?

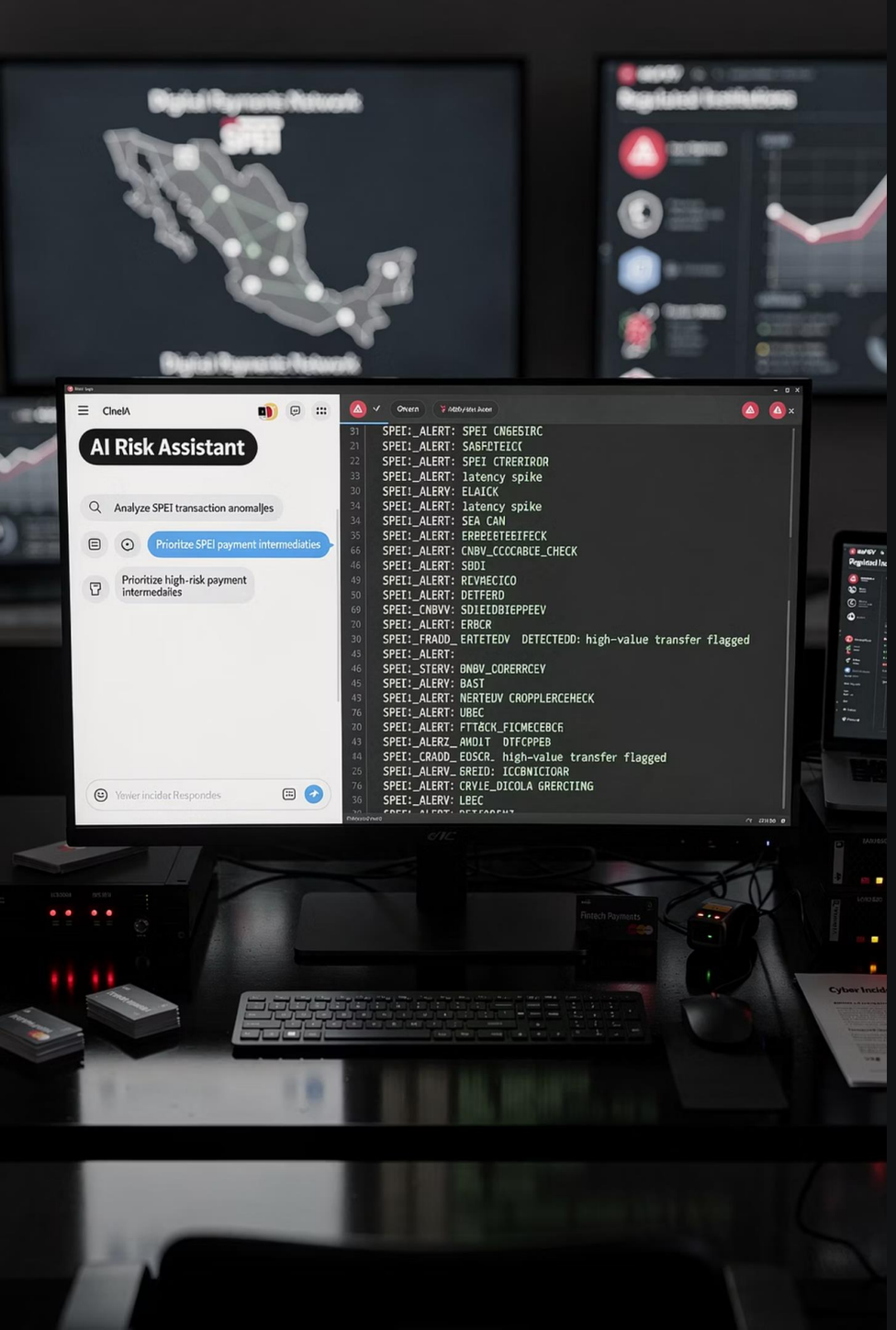
¿Qué se llevaría y cuánto te costaría?

Tu seguridad es tan fuerte como tu proveedor más descuidado.

Esta semana:

¿Cuántos terceros tienen acceso activo a tu infraestructura de pagos en este momento?

No en el contrato. No en el papel. Activo, ahora mismo.



La IA ya juega en el otro equipo.

El mismo modelo que detecta tu fraude, automatiza el ataque.

Reportar un incidente no es admitir derrota.
Es la jugada que protege al equipo completo.

Lo que dice Banxico:

En 2024, el GRI emitió boletines de inteligencia a todas las instituciones reguladas después de cada incidente reportado.

La información de un ataque a una Sofipo protegió a los bancos. Así funciona el sistema cuando se usa.

Fuente: Banco de México, Reporte de Estabilidad Financiera 2024.

Cómo ocurre un ataque a un intermediario de pagos:

1

1. Reconocen tu API pública durante semanas, sin disparar ninguna alerta.

2

2. Detectan que el origen de las llamadas no se valida como debería.

3

3. Sacan fondos en transacciones pequeñas, debajo del umbral de monitoreo.

No fue sofisticación: fue paciencia, y una puerta que nadie estaba vigilando.

Las empresas que responden bien tienen tres cosas en común:

Saben exactamente qué protegen y por qué.

Tienen un protocolo de respuesta que alguien leyó en los últimos seis meses.

Tratan a sus proveedores como parte de su superficie superficie de riesgo.

Lo sé porque he estado en la sala con ellas. En los tabletops, la diferencia entre las que sobreviven y las que no es siempre la misma: una decisión que tomaron antes.

El costo real no es técnico.

Reputación. Regulatorio. Operativo. Al mismo tiempo. Sin aviso.

LO QUE EL SECTOR NECESITA CONSTRUIR EN CONJUNTO.

Compartir alertas de que el golpe te alcance.

Conectar fraude, lavado y ciberataque como una sola amenaza.

Construir inteligencia colectiva que no dependa del regulador.

Eso es exactamente lo que impulsamos los comités en los que participo. Y eso mismo podemos construir para este

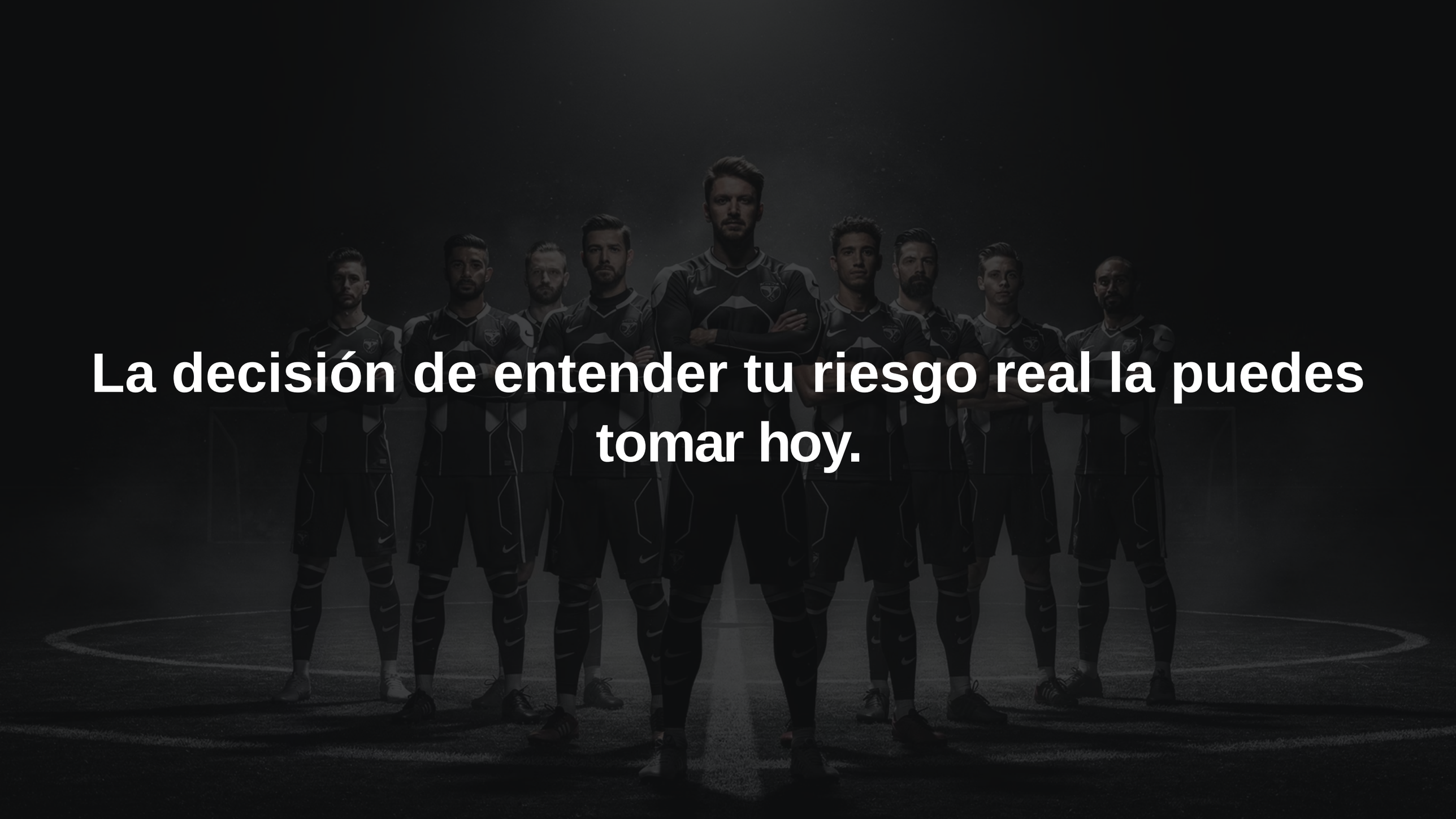
ANTES DE SALIR DE AQUÍ:

¿Sabes exactamente qué terceros tienen acceso activo a tu infraestructura hoy?

Si mañana hay un incidente, ¿tienes un protocolo escrito o vas a improvisar?

¿Tu ciberseguridad está diseñada para tu riesgo real o para pasar la siguiente auditoría?

Si alguna respuesta es 'no sé' — alguien más ya lo sabe.


La decisión de entender tu riesgo real la puedes tomar hoy.

Andrés Velázquez *CISSP,GCFA,*

IEM

Founder / President - MaTTic

Más de 20 años liderando respuesta a incidentes e investigaciones digitales en México y América Latina.

Andrés Velázquez

Columna:
https://www.forbes.com.mx/author/andres-velazquez/

Andrés Velázquez

Más de 20 años liderando respuesta a incidentes e investigaciones digitales en México y América Latina.

CISSP · GCFA · IEM

Stanford GSB · MIT Crisis Management

FIRST LATAM · EU CyberNet

Forbes México · Tecnológico de Monterrey