INDU DAS

Varma

Fundador · Hyperwise LLC

Technology, Consulting & Audit

35 años en banca institucional

Citi · Temasek · Fintech Asia/México/EE.UU

India · EUA · Vietnam · Singapur
Malasia · Indonesia · Pakistán · China · Dubai · Georgia

México · 18 años construyendo

Lo que construyo

PRUDENZE	Plataformas de Gobernanza / cumplimiento – pre-ejecución para automatizacion financiera
VIGIL	Ciberseguridad agentica para cajas y cooperativas – SIEM+SOC
COMPLY	Gestión de los ciclos de vida de los procesos financieros para la automatización
CLAVIS	Core agentico de credito y arrendamiento para SOFOM
LAYER3X	Firewall de ejecución para pagos con IA
GUARDIAN	MFA + SSO + Autenticación, autorización, monitorización
PORTFOLIO	Gestión automatizada de carteras de crédito
RECON	Conciliación de 1.000 millones de registros en 15 minutos

hyperwise.io · indu@hyperwise.io

LA REALIDAD HOY

La nueva generación no va a ir a su sucursal. Ya no.

LA REALIDAD HOY

CAJAs.

Presupuesto

Poco o ningún presupuesto para tecnología

Regulación

Regulaciones confusas o sin claridad operativa

Mentalidad

"Nuestros socios no necesitan eso"

Talento

Difícil encontrar personas que entiendan ambos mundos

Estas cuatro barreras son reales. Y todas tienen solución.

LA DECISIÓN

Transformarse o desaparecer.

No hay una tercera opción.

Si eligen desaparecer

Salir ahora y cerrar operaciones.

Ir con el gobierno, pedir subsidios, recibir un no, y convencerse de que hicieron lo posible.

Las cajas que no ofrezcan experiencia digital en los próximos 3 años no existirán en 5.

Si eligen transformarse

Comprar software caro diseñado para grandes bancos — creado en Dinamarca, vendido en México.

O buscar proveedores que entiendan lo que realmente hacen, a costos accesibles, construidos para resolver problemas mexicanos.

Esa segunda opción existe.

LA COMPETENCIA

Están sentados sobre una mina de oro.Los demás lo saben.

Nu Bank · Plata · Klar

Polanco · Zapopan · Monterrey

Diseñados para personas con historial crediticio, en ciudades grandes, con smartphone de última generación.

No entienden a Totatiche, Río Verde, ni Pico de Oro.

Revolut · Wise

Londres · Berlín · CDMX expats

Diseñados para personas que ya tienen cuenta bancaria y viajan al exterior.

Irrelevantes para el 75% de los mexicanos que no tienen cuenta formal.

El futuro: Instagram · TikTok

Todas partes · Todo el tiempo

La generación Z no quiere una app de banco. Quiere hacer transacciones donde ya está.

WhatsApp ya es viejo y riesgoso. El siguiente canal ya existe.

Ninguno de ellos entiende lo que ustedes hacen. Eso es su ventaja — si la usan.

NUESTRO ENFOQUE

Tomamos las regulaciones como nuestro mejor aliado.

Mientras otros ven la regulación como obstáculo, nosotros la usamos para innovar dentro de sus límites — a costos que las cajas pueden pagar.

01

Regulación como ventaja

Conocemos la CUB, la LFPDPPP 2025, FOCOOP, CONDUSEF y CNBV. Construimos dentro de esos límites — no a pesar de ellos.

02

Costo accesible

No vendemos software de banco grande a presupuesto de caja. Cada solución tiene un modelo de precio diseñado para la realidad de su institución.

03

Construido para México

No para Dinamarca. No para Silicon Valley. Para Totatiche, Río Verde y Pico de Oro — donde realmente viven sus socios.

ANUNCIO

Diagnóstico gratuito para las 150+ cajas de México.

En alianza con Milito Technology Group — sin costo para ninguna caja.

¿Qué cubre el diagnóstico?

→ Postura de cumplimiento regulatorio

→ Postura de seguridad IT

→ Brechas frente a examen CNBV

→ Nivel de madurez digital

→ Recomendaciones priorizadas

Las cajas que no participen

Las que crean que sobrevivirán los próximos 5 años sin cambiar — le pido a sus empleados que empiecen a buscar trabajo.

No es una predicción.
Es lo que ya está pasando.

INTELIGENCIA ARTIFICIAL

La IA no es para despedir personas. Es para crecer 10X sin perder a nadie.

Donde la IA ayuda

✓ Procesar 1 millón de eventos en el tiempo que un analista procesa uno

✓ Detectar patrones de fraude invisibles al ojo humano

✓ Automatizar cumplimiento regulatorio en tiempo real

✓ Atender a socios 24/7 sin contratar personal adicional

Donde la IA falla sin gobernanza

✗ No tiene memoria de cumplimiento regulatorio

✗ Ejecuta 1 millón de veces más rápido de lo que puede ser auditada

✗ Una caja fue atacada 2.5 millones de veces en 5 horas — 250K registros perdidos

✗ CNBV audita a la caja. No al proveedor de IA.

Por eso invertimos más de $7 millones de dólares en plataformas que gobiernan la IA antes de que ejecute.

EL FUTURO ES HOY

El futuro de su caja está en sus manos.

A menos que no amen lo que hacen y dónde trabajan.

1

Ofrezcan experiencia móvil

Si aún no tienen banca móvil — este es el momento. No el año que viene. Hoy. Sus socios jóvenes ya tienen cuenta en Nu Bank. Los que no la tienen aún, la tendrán mañana.

2

Hablen con los jóvenes de sus socios

No con el socio. Con su hijo de 22 años. Él decide dónde va el dinero familiar. Si su caja no tiene app, para él no existe.

3

Gobiernen su IA antes de que llegue

La IA ya está en sus proveedores de tecnología. Ya está en su core bancario. La pregunta no es si usarán IA — es si tendrán gobernanza cuando llegue el examinador de la CNBV.

Hoy no vine a venderles nada. Vine a trabajar con ustedes.

Antes de que vean una sola diapositiva,

quiero que piensen en una sola pregunta.

¿Si alguien atacara tu entidad esta noche, cuánto tiempo tardarían en enterarse?

No el tiempo de recuperación.
El tiempo en que alguien en tu institución se da cuenta de que algo pasó.

30 años en Citi, Temasek y fintech mexicano. Construyo infraestructura de gobernanza para instituciones financieras financieras reguladas.

HYPERWISE

Ciberseguridad para el Sector Financiero Mexicano

Casos ~~representativos~~ basados en incidentes reales del sector mexicano mexicano

AGENDA

Contenido del taller

01 Realidad SOCAP: el panorama que nos compete

02 Contexto: Amenazas en México 2024–2025

03 Caso 1 – Ransomware Akira en una SOFIPO

04 Caso 2 – Fraude en transferencias electrónicas

05 Caso 3 – Troyano Grandoreiro adaptado a México

06 Metodología Hyperwise · Resultados · Diagnóstico

LA REALIDAD SOCAP

Tu institución no es un banco. Tus riesgos sí lo son.

Presupuesto IT

MXN 50–300K al año.
Los atacantes saben esto.

Equipo técnico

1 a 3 personas cubren
todo: redes, usuarios, CNBV.

Presión regulatoria

Examen CNBV, FOCOOP,
requerimientos en escalada.

Superficie SPEI

Cada transferencia SPEI
es un vector de ataque activo.

Socios expuestos

Tus terceros son tu backdoor.

Confianza del socio

Un incidente destruye
décadas de reputación local.

C O N T E X T O

El Panorama de Ciberseguridad en México 2024–2025

31M

Intentos de ciberataques en 2024

55% del total de América Latina

111K

Ataques de troyanos bloqueados

Ago 2024 – Jun 2025

$483.85M

Pérdidas (MDP)

Incremento del 443% vs 2023

13.5M

Víctimas de phishing

Pérdida prom. $8,750 pesos

Ransomware avanzado

Doble extorsión y envenenamiento de datos. Grupos más pequeños, más ágiles.

Ataques con IA

Deepfakes, phishing hiperrealista y malware adaptable que evade detección tradicional.

Vulneración de APIs

Ataques a SPEI y banca abierta mediante APIs mal protegidas.

Fuente: Banco de México, Kaspersky, PwC Digital Trust Insights 2026

CASO 1 · PREGUNTA AL SALÓN

Levanten la mano quienes tienen backups que no han probado en los últimos 90 días.

... porque en abril de 202X, una SOFIPO con 2.3 millones de socios no los tenía listos cuando los necesitó.

Ransomware AKIRA

CASO 1 · RANSOMWARE 'AKIRA'

Resiliencia ante Ataque Ransomware

SOFIPO Mexicana

150 sucursales · 2.3M de socios
Abril 2024 · Ransomware 'Akira'
$16.38 MDP en pérdidas potenciales

1 **Respuesta < 4 horas**

Activación, contención y preservación de evidencia forense

2 **Aislamiento en 12 min**

127 endpoints infectados segmentados automáticamente

3 **Recuperación sin rescate**

Restauración desde backups inmutables. 100% de datos recuperados

4 **Controles fortalecidos**

EDR avanzado, MFA y políticas Zero Trust implementados

3.2 hrs Recuperación

100% Datos recuperados

$0 Rescate pagado

99.9% Uptime

CASO 1 · ARQUITECTURA TÉCNICA

Arquitectura de Respuesta y Recuperación

Segmentación de Red

Micro-firewalls por segmento con políticas de acceso restrictivas

Backups Inmutables

Snapshots cada 15 min · Retención 90 días · Aislados de red

Zero Trust

Verificación continua de identidad y dispositivo en cada acceso

Detección con IA

ML identificó anomalías en 3 minutos · Precisión 99.7%

3.2 hrs	100%	$0	99.9%
Recuperación	Datos	Rescate	Uptime

CASO 2 · PREGUNTA AL SALÓN

En su institución, ¿cuántas personas pueden autorizar una transferencia fuera de su catálogo habitual de beneficiarios?

... porque el vector de entrada no fue tecnología.
Fueron 23 empleados con credenciales robadas por phishing.

Fraude en Transferencias SPEI

CASO 2 · TRANSFERENCIAS ELECTRÓNICAS

Protección de Transferencias Electrónicas

Banco Mexicano Tier-2

850,000 clientes
180,000 transacciones/día
23 empleados comprometidos
847 transacciones fraudulentas intentadas
$124.11 MDP en intento de fraude

Detección en Tiempo Real

Motor de ML detectó patrones anómalos en milisegundos

Bloqueo Automático

847 transacciones fraudulentas detenidas antes de procesarse

Autenticación Adaptativa

MFA contextual por riesgo: ubicación, dispositivo, comportamiento

Monitoreo Continuo

$0 Pérdidas

100% Fraudes detenidos

<50ms Respuesta

CASO 2 · SISTEMA TÉCNICO

Sistema de Detección de Fraude en Tiempo Real

50,000 tx/seg

Procesamiento en tiempo real

ML entrenado

Con datos de 30 bancos mexicanos

Score de riesgo

Evaluación en tiempo real por transacción

Aprendizaje continuo

Adapta a nuevos patrones de ataque

Integración SPEI

Validación de cuentas y alertas

Dashboard en vivo

Threat intelligence y reglas dinámicas

CASO 3 · PREGUNTA AL SALÓN

¿Cuántos de sus socios recibieron un correo del SAT o del SPEI en los últimos 60 días?

... porque el troyano Grandoreiro no ataca tecnología.
Ataca a personas. Y sabe exactamente qué palabras usan los mexicanos.

Troyano Grandoreiro

CASO 3 · TROYANO 'GRANDOREIRO'

Neutralización de Troyano Bancario

La Amenaza

Variante brasileña adaptada para México

Código específico para 30 bancos mexicanos

Temas locales: CFDI, SAT, SPEI

Alta evasión de antivirus

1.8M de socios en riesgo · 2,400 endpoints

Identificación Temprana

Detección en fase inicial via threat intelligence

Firmas de Detección

Firmas específicas para variantes mexicanas del troyano

Despliegue Rápido

Parches en 2,400 endpoints en 48 horas

Capacitación Masiva

1,200 empleados entrenados en reconocimiento de amenazas

100% Endpoints

0 Cuentas comprometidas

48 hrs Respuesta

CASO 3 · ESTRATEGIA MULTICAPA

Estrategia de Defensa Multicapa

EDR Avanzado	Monitoreo comportamental heurístico en tiempo real	**99.7% detección**
Sandboxing	Archivos sospechosos en entornos aislados para análisis	**8 min respuesta**
Filtrado DNS	Bloqueo proactivo de dominios maliciosos y C2 servers	**15,000+ dominios**
Análisis de Tráfico	Inspección profunda de paquetes de red	**100% tráfico**
Concientización	Simulaciones de phishing · Talleres mensuales · Evaluaciones	**94% reducción**

ENFOQUE

Metodología : Enfoque Proactivo

01

Evaluación y Diagnóstico

Auditoría integral · Análisis de vulnerabilidades · Mapeo de activos · Cumplimiento

2–4 semanas

02

Diseño e Implementación

Arquitectura de seguridad · Controles técnicos · Políticas · Capacitación

4–8 semanas

03

Monitoreo y Respuesta

SOC 24/7/365 · Threat intelligence · Gestión de incidentes · Análisis forense

Continuo 24/7

04

Mejora Continua

Simulacros regulares · Análisis post-incidente · Actualización de defensas

Ciclo trimestral

IMPACTO CUANTIFICABLE

Resultados y Métricas de Impacto

$140.49 MDP
Pérdidas potenciales evitadas

100%
Continuidad operativa

4 hrs
Tiempo de respuesta promedio

99.9%
Tasa de detección

3,647
Endpoints protegidos

2.4M
Transacciones monitoreadas/día

18,500+
Amenazas bloqueadas/mes

98%
Satisfacción del cliente

87%
Reducción de incidentes

<3 min
Tiempo de detección

$200M+
Ahorro total estimado

ANTES DE QUE SALGAN

Una sola pregunta.
Contéstenla honestamente.

Si hoy ocurriera un incidente en tu SOCAP, ¿sabrías exactamente a quién llamar, qué aislar primero, y cómo demostrarle a la CNBV que tomaste las medidas correctas?

Si la respuesta tiene alguna duda — esa duda es el diagnóstico.

Indu Das · indu@hyperwise.io · www.hyperwise.io

P

Si tenían backups, ¿qué causó realmente las 3.2 horas de recuperación?

R

La tecnología fue rápida. Las decisiones alrededor de ella no lo fueron.

Esas 3.2 horas se dividen en cuatro fases. Primeros 45 minutos: contención — identificar qué está infectado, qué está limpio, aislar antes de tocar cualquier cosa. Saltarse esto arriesga reinfectar los datos restaurados. Siguientes 40 minutos: preservación forense — capturar evidencia del ataque antes de sobreescribirla. La necesitan para el reporte regulatorio y el seguro. Siguientes 60 minutos: restauración por etapas — primero los sistemas críticos, en orden de impacto al socio. Últimos 35 minutos: validación de integridad antes de reabrir cada sistema.

La mayoría de las instituciones con tiempos de recuperación más largos no están esperando datos. Están esperando decisiones.

P **Los backups resuelven el cifrado. No resuelven la exfiltración. ¿Qué pasa cuando amenazan con publicar sus datos?**

R Correcto. Son dos amenazas separadas y requieren dos defensas separadas.

La amenaza operativa — sistemas cifrados, no pueden trabajar — se resuelve con backups. La amenaza reputacional — tienen una copia de sus datos — no.

Lo que resuelve la segunda amenaza es saber exactamente qué datos tienen, dónde viven y cómo están clasificados. Si pueden demostrarle a la CNBV y a sus socios que los datos exfiltrados estaban debidamente protegidos — cifrados en reposo, tokenizados donde se requiere — el daño es contenible. Si no tienen ese inventario, están negociando a ciegas.

La respuesta no es pagar. La respuesta es construir la disciplina de clasificación de datos antes del ataque.

P **El SPEI liquida en menos de 30 segundos. Para cuando una alerta de 47 milisegundos dispara y un humano la revisa, ¿el dinero no se fue ya?**

R Esa es exactamente la pregunta correcta. La respuesta cambia cómo diseñan sus controles.

El SPEI es irreversible una vez que la instrucción se envía a la infraestructura de Banxico. Eso es verdad y no es negociable. La interceptación tiene que ocurrir antes de ese envío, no después.

La detección de 47 milisegundos disparó en el punto de creación de la instrucción dentro del sistema propio de la institución, antes de que la instrucción fuera enviada al SPEI. Es un punto de control en la puerta de salida, no en la calle.

Una vez que está en el SPEI, la ventana para revertirlo es extremadamente estrecha y requiere coordinación bilateral entre ambas instituciones y Banxico.

Monitorear después de que el SPEI confirma es forense. No es prevención.

P

¿Cómo hacen clic 23 empleados en el mismo correo de phishing sin que nadie note algo raro primero?

R

Porque el ataque no fue secuencial. Fue simultáneo.

No enviaron un correo, esperaron a que lo abrieran y luego enviaron el siguiente. Los 23 objetivos recibieron el correo en minutos entre sí. Cada empleado tomó su propia decisión en aislamiento. Nadie sabía que la persona a tres escritorios de distancia había hecho lo mismo.

Por eso el modelo de detección no puede depender del reconocimiento humano de patrones en toda la organización. Para cuando el empleado dos hace clic, el atacante ya tiene dos credenciales válidas.

El control tiene que ser técnico — un sistema que vea los 23 eventos como un patrón correlacionado en tiempo real, no como 23 incidentes no relacionados en diferentes bandejas de entrada.

P

Si Europol e INTERPOL no pudieron detenerlo, ¿qué puede hacer realísticamente una SOCAP con tres personas de IT?

R

El arresto interrumpió la operación central, no el malware. Solo se detuvo parte de la red. Los operadores restantes dividieron el código en versiones más ligeras y continuaron.

No pueden desmantelar la operación criminal. Sí pueden convertirse en un objetivo más difícil que la institución de al lado.

Grandoreiro simula específicamente movimientos de ratón similares a los humanos para evadir herramientas de seguridad con aprendizaje automático — está diseñado para vencer las defensas estándar. Lo que lo derrota es el monitoreo conductual en la capa de red: detectar la comunicación saliente que el troyano hace hacia sus servidores de comando y control. Ese tráfico es anómalo, es detectable y no requiere infraestructura empresarial.

Tres personas con las herramientas correctas observando las señales correctas pueden detectar esto antes de la ejecución. La brecha no es la cantidad de personas. Es saber qué señales observar.

P

El troyano secuestra una sesión ya autenticada. ¿Eso significa que el MFA no sirve?

R

Correcto — y esto es una de las cosas más importantes para entender sobre esta clase de amenaza.

El MFA protege el evento de autenticación. Una vez que la autenticación está completa y la sesión está abierta, el MFA hizo su trabajo y ya no está en juego. El troyano no necesita su contraseña ni su OTP. Espera a que ustedes proporcionen todo eso y luego monta la sesión autenticada.

Lo que derrota a los troyanos de secuestro de sesión no es una autenticación más fuerte. Es el monitoreo de integridad de sesión — biometría conductual que rastrea cómo un usuario normalmente interactúa con la interfaz. Si una sesión que normalmente tarda cinco minutos en completar una transferencia ejecuta de repente 12 transferencias en 40 segundos, esa desviación es detectable sin importar qué tan limpiamente se autenticó al inicio.

El MFA es necesario. Contra esta amenaza, no es suficiente.

P

¿Cuál es la postura mínima de seguridad viable para una SOCAP con presupuesto limitado?

R

Cuatro controles. En este orden.

1. Integridad de backups. No si tienen backups — si han probado una restauración completa en los últimos 90 días. No cuesta nada excepto disciplina.

2. Segmentación de accesos. Cada empleado accede solo a lo que su función específica requiere. Auditen sus permisos. Revoquen lo que no corresponde.

3. Monitoreo de tráfico de red. Detección básica de anomalías en conexiones salientes. Existen opciones de código abierto que un equipo de una persona puede gestionar. Buscan comunicación hacia destinos que sus sistemas no tienen razón de contactar.

4. Un procedimiento escrito de respuesta a incidentes. Una página. Tres columnas: qué pasó, a quién llaman, qué hacen en los primeros 30 minutos. Imprímanlo — porque cuando el ransomware golpea, puede que no puedan abrir una computadora.

Estos cuatro, ejecutados con disciplina, reducen su superficie explotable más que cualquier compra de tecnología individual.

AMENAZAS ACTIVAS · MÉXICO Y LATAM · 2026

Vector	Tendencia	Caso real 2026	Fuente
Ransomware doble extorsión	↑↑ +294K intentos/año en México (2025) 805 por día	SHF México · ene 2026 LockBit 5.0 · 277 GB exfiltrados Expedientes en dark web · Banxico confirmó	*Banxico Q1 2026* *Silikn*
Ransomware dirigido (targeted)	⬡ Qilin activo Selecciona víctimas con precisión quirúrgica	Inst. financiera MX · feb 2026 Qilin ransomware · transferencias electrónicas comprometidas	*Banxico · CNBV* *La Jornada · abr 2026*
Secuestro de sesión bancaria (session hijack)	↑↑ 11,695 ataques MX solo en 2025 +3.6x móvil vs 2023	JanelaRAT 'Gold-Label' MX Overlay falso sobre banca real Usuario no detecta nada	*Kaspersky GReAT* *Securelist · abr 2026*
Troyanos bancarios vía WhatsApp	⬡ NUEVO · activo abr 2026 · predicción cumplida en 4 meses	Casbaneiro/Water Saci Campaña en español · activa Hispanoamérica objetivo	*Dark Reading* *abr 2, 2026*
Account Takeover (ATO) + IA	↑↑ +324% en México 2024 → 2026 +344% fraude dispositivo	México lidera LATAM en ATO 36 inst. financieras · 300M clientes Identidades sintéticas con IA	*BioCatch · 2026* *México Business News*

Impacto acumulado sistema financiero MX 2020–2025: MXN 1,079 millones | Banxico 2026 · Kaspersky 2026 · BioCatch 2026