La primera línea de defensa, capacitación

La Visión Práctica de un CISO
Ulises MA

SECRETARÍA DE FINANZAS

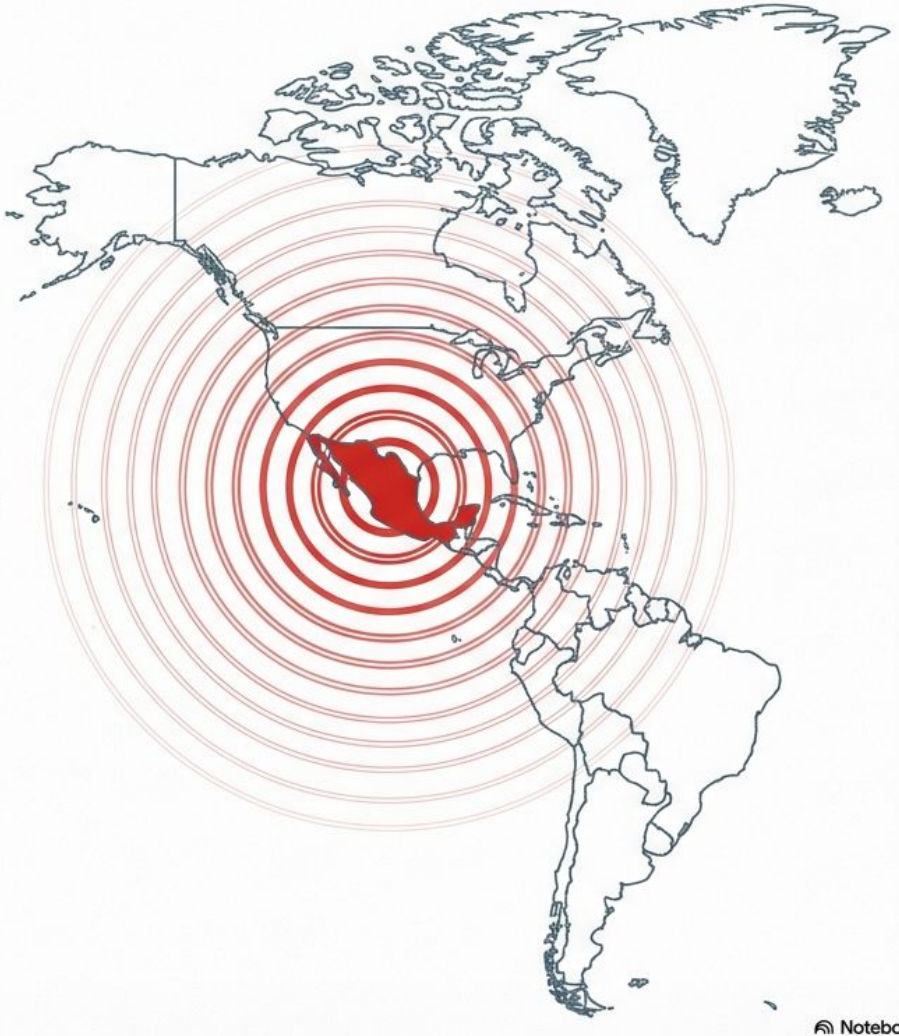
443%

Incremento de pérdidas económicas reportadas en instituciones financieras en México, 2024–2025


Imaginen sus cajas de ahorro o fábricas como fortalezas.
Antes, los ladrones usaban palancas y explosivos.
CAJA DE AHORRO / FÁBRICA
Hoy, usan teclados y código.
¡La ciberseguridad es la nueva muralla!

Resiliencia Digital y Cultura de Ciberseguridad en México 2025

Estrategia integral para la supervivencia económica en los sectores Financiero Popular e Industrial.



En el bienio 2024-2025, la seguridad digital ha dejado de ser una preocupación técnica para transformarse en un imperativo de supervivencia económica y estabilidad social.

Basado en la investigación ejecutiva de Ulises M. Álvarez, CISO Virtual.

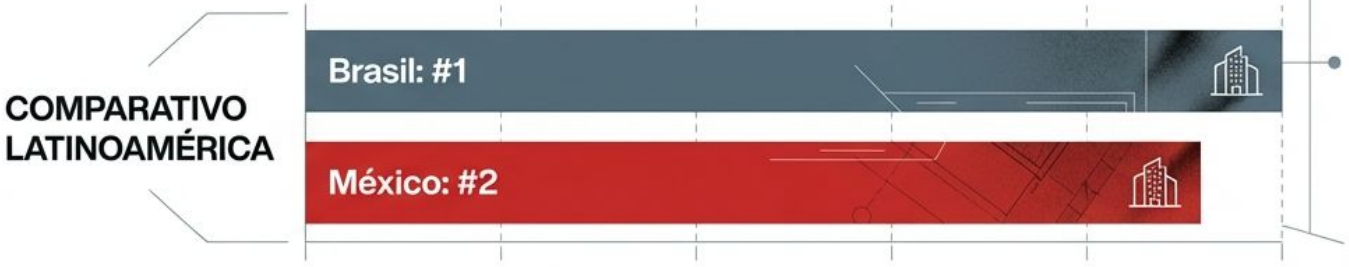
México: El segundo objetivo más asediado de América Latina

Esta cifra no es una anomalía, es el resultado de:

- Digitalización acelerada sin educación previa.
- Importancia estratégica en cadenas de suministro (T-MEC).
- Vacío persistente en cultura preventiva.

187,000 MILLONES

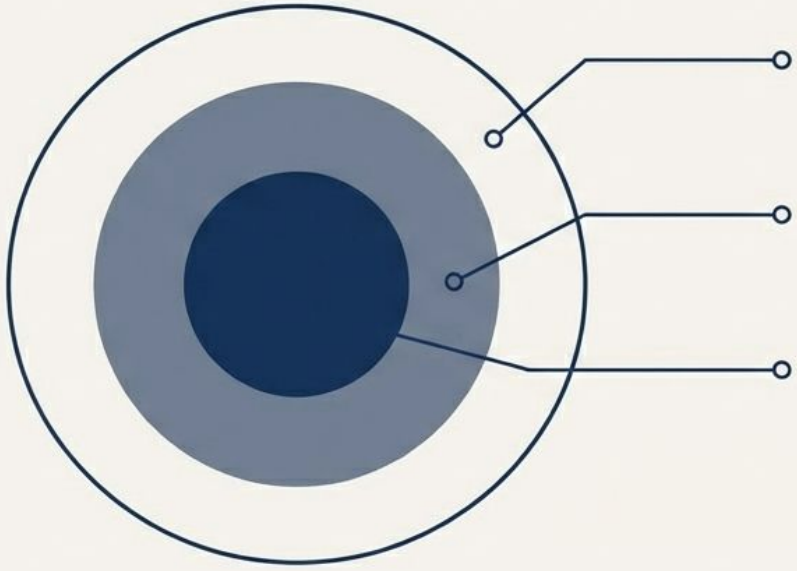
Intentos de ataque anuales



Insight: La ciberseguridad es hoy una condición de entrada para la economía global.

Mapa de Estándares: Defensa en Profundidad

Adoptar un lenguaje común con reguladores y socios internacionales.



Capa Estratégica (Gobierno): NIST CSF
(Gestión de Riesgos/Estrategia)

Capa Gestión: ISO/IEC 27001
(Gestión Formal / Certificación)

Capa Operativa (OT): IEC 62443
(Seguridad en Automatización y Control)

La combinación de estos marcos estructura una defensa que abarca Personas, Procesos y Tecnología.

Gobernanza y Gestión: ISO 27001 vs. NIST CSF

ISO/IEC 27001 (NMX-I-27001-NYCE)

- **Enfoque:** Certificación formal y auditada.
- **Uso Principal:** Prueba de cumplimiento ante terceros (Clientes/CNBV).
- **Clave:** Enfoque basado en riesgos y mejora continua (PDCA).

NIST Cybersecurity Framework

- **Enfoque:** Autoevaluación y madurez flexible.
- **Uso Principal:** Guía estratégica interna y comunicación con la Junta Directiva.
- **Las 6 Funciones:** Gobernar, Identificar, Proteger, Detectar, Responder, Recuperar.

Recomendación: Utilizar NIST para la estrategia operativa y ISO 27001 para la validación comercial.

NMX-I-27001-NYCE 2023

Excelencia en Gestión de Seguridad de la Información.

Estrategia de protección de activos digitales para empresas en México.

PODER EJECUTIVO DEL ESTADO DE QUERÉTARO

SECRETARÍA DE FINANZAS

UNAM JURIQUILLA

UNIVERSIDAD AUTONOMA DE QUERETARO

EDUCO EN LA VERDAD Y EN EL HONOR

¿Qué es la NMX-I-27001-NYCE?

Es la norma mexicana que adopta el estándar internacional **ISO/IEC 27001**. Establece los requisitos para establecer, implementar, mantener y mejorar un **Sistema de Gestión de Seguridad de la Información (SGSI)**.

- Equivalencia total con ISO/IEC 27001.
- Avalada por organismos mexicanos (NYCE).
- Marco legal y normativo local.

SECRETARÍA DE FINANZAS
QUERÉTARO
UNAM JURIQUILLA

Objetivos del Sistema (SGSI)

Confidencialidad

Asegurar que la información sea accesible solo para quienes tienen autorización.

Integridad

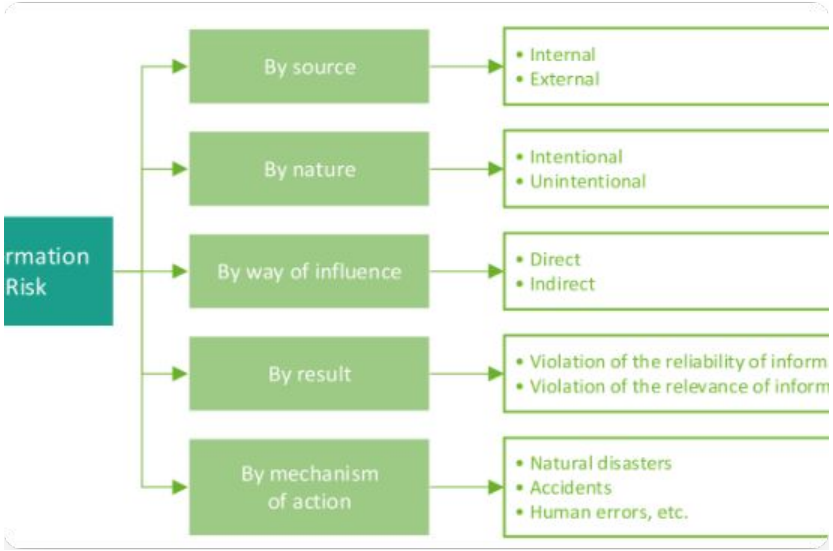
Garantizar la exactitud y completitud de la información y sus métodos de procesamiento.

Disponibilidad

Asegurar que los usuarios autorizados tengan acceso cuando lo requieran.

SECRETARÍA DE FINANZAS
QUERÉTARO
UNAM
JURIQUILLA
UNIVERSIDAD AUTÓNOMA DE QUERÉTARO
EDUCO EN LA VERDAD Y EN EL HONOR

El Corazón: Gestión de Riesgos



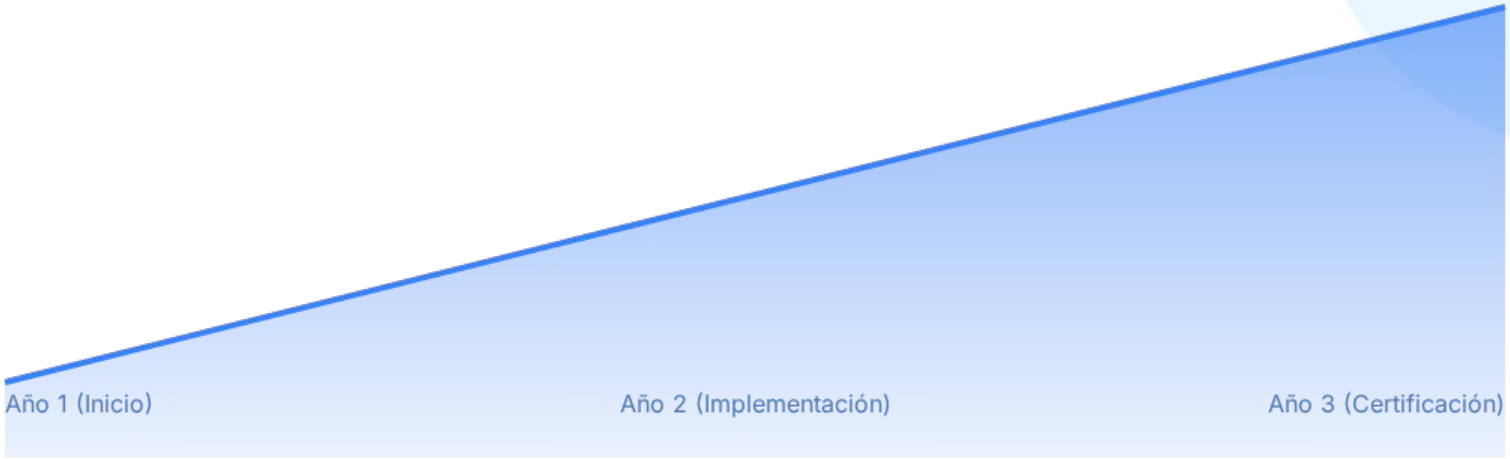
La norma se basa en un enfoque de riesgos para seleccionar controles proporcionales a las amenazas.

Pasos críticos:

1. Identificación de activos y amenazas.
2. Evaluación de probabilidad e impacto.
3. Definición del plan de tratamiento (Mitigar, Transferir, Evitar, Aceptar).

SECRETARÍA DE FINANZAS
QUERÉTARO
UNAM JURIQUILLA
UNIVERSIDAD AUTÓNOMA DE QUERÉTARO
EDUCO EN LA VERDAD Y EN EL HONOR

Crecimiento de Amenazas vs Madurez



La implementación progresiva de NMX-I-27001 reduce la superficie de ataque y el costo de incidentes en un promedio del 60% tras el primer ciclo de mejora.

Ruta hacia la Certificación

Etapa 1

Análisis de Brechas (GAP Analysis) y Diagnóstico.

Etapa 2

Diseño e Implementación de Controles.

Etapa 3

Auditoría Interna y Revisión Directiva.

Etapa 4

Auditoría Externa y Certificación NYCE.

PODER EJECUTIVO DEL ESTADO DE QUERÉTARO
SECRETARÍA DE FINANZAS
UNAM JURIQUILLA
UNIVERSIDAD AUTÓNOMA DE QUERÉTARO
EDUCO EN LA VERDAD Y EN EL HONOR

Liderazgo y Cultura

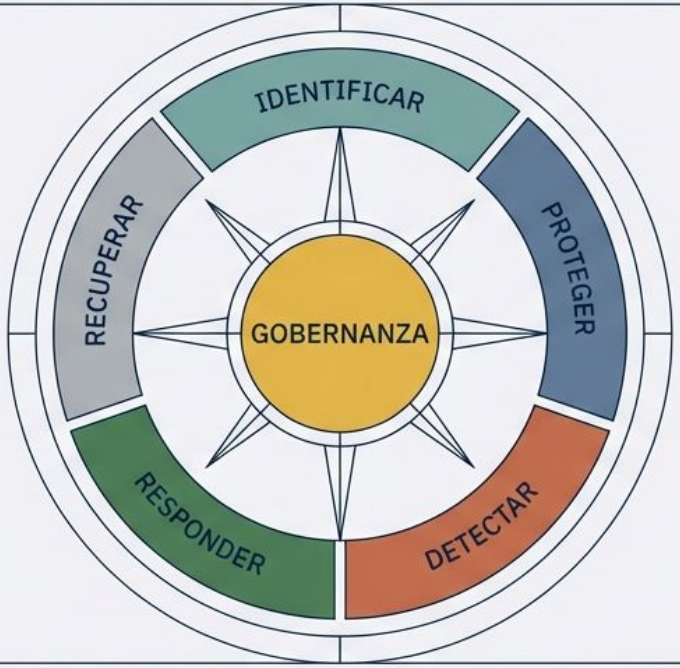
El éxito de la norma no reside en la tecnología, sino en el **factor humano**. El compromiso de la alta dirección es el motor que impulsa la asignación de recursos y la concienciación de todo el personal. Sin una cultura de seguridad, los controles técnicos fallan.

De la teoría a la práctica

PODER EJECUTIVO DEL ESTADO DE QUERÉTARO
SECRETARÍA DE FINANZAS
UNAM JURIQUILLA
UNIVERSIDAD AUTONOMA DE QUERETARO
EDUCO EN LA VERDAD Y EN EL HONOR

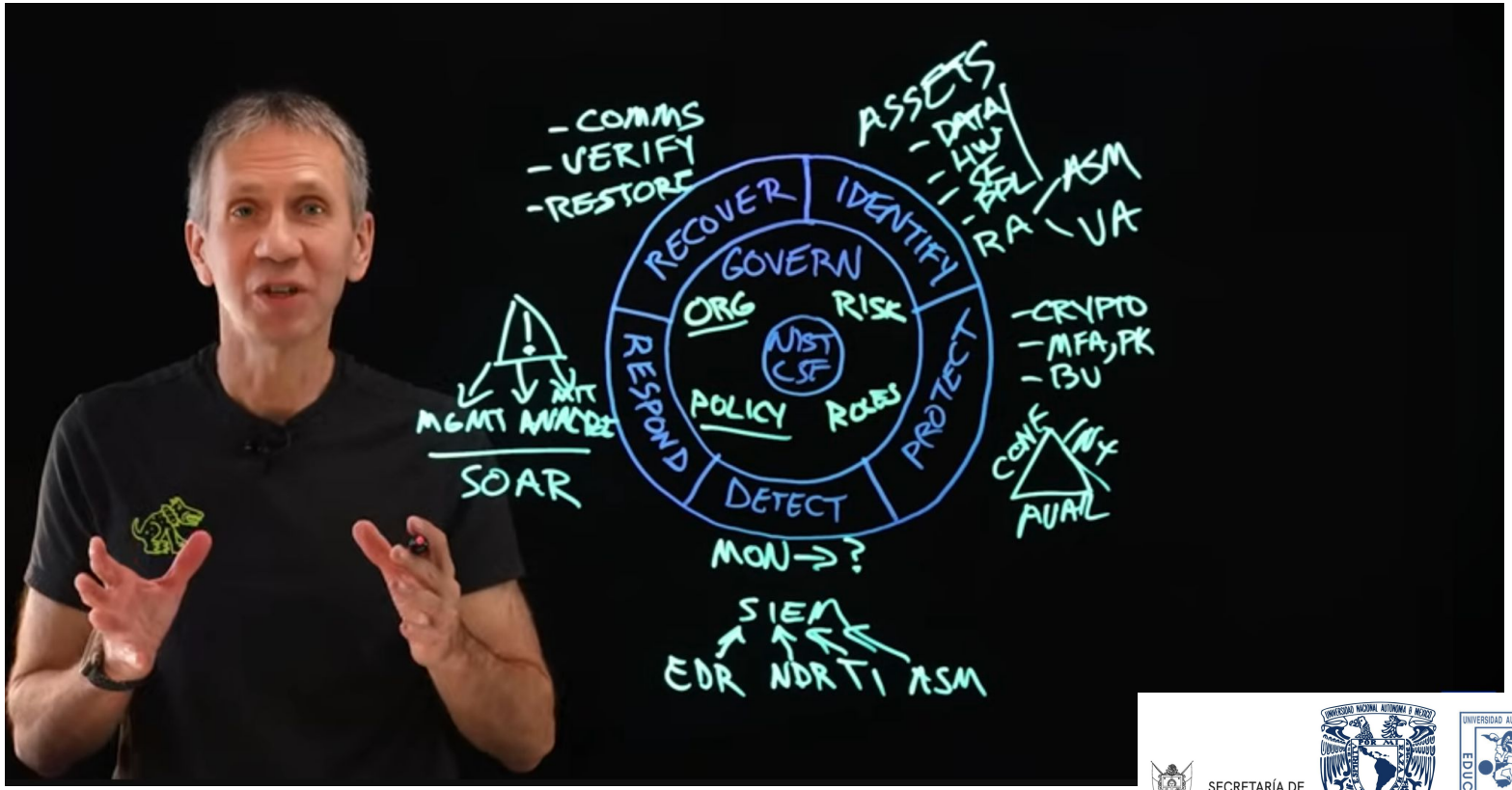
Construyendo un Programa de Ciberseguridad Sólido

Una guía práctica basada en el **Marco NIST 2.0 para navegar el caos digital.**



Manual de Estrategia | Versión 2.0

PODER EJECUTIVO DEL ESTADO DE QUERÉTARO
SECRETARÍA DE FINANZAS
UNAM JURIQUILLA
UNIVERSIDAD AUTÓNOMA DE QUERÉTARO
EDUCO EN LA VERDAD Y EN EL HONOR



https://youtu.be/Ula3TG8QS7g?si=q32RnaYLjoLgONzw

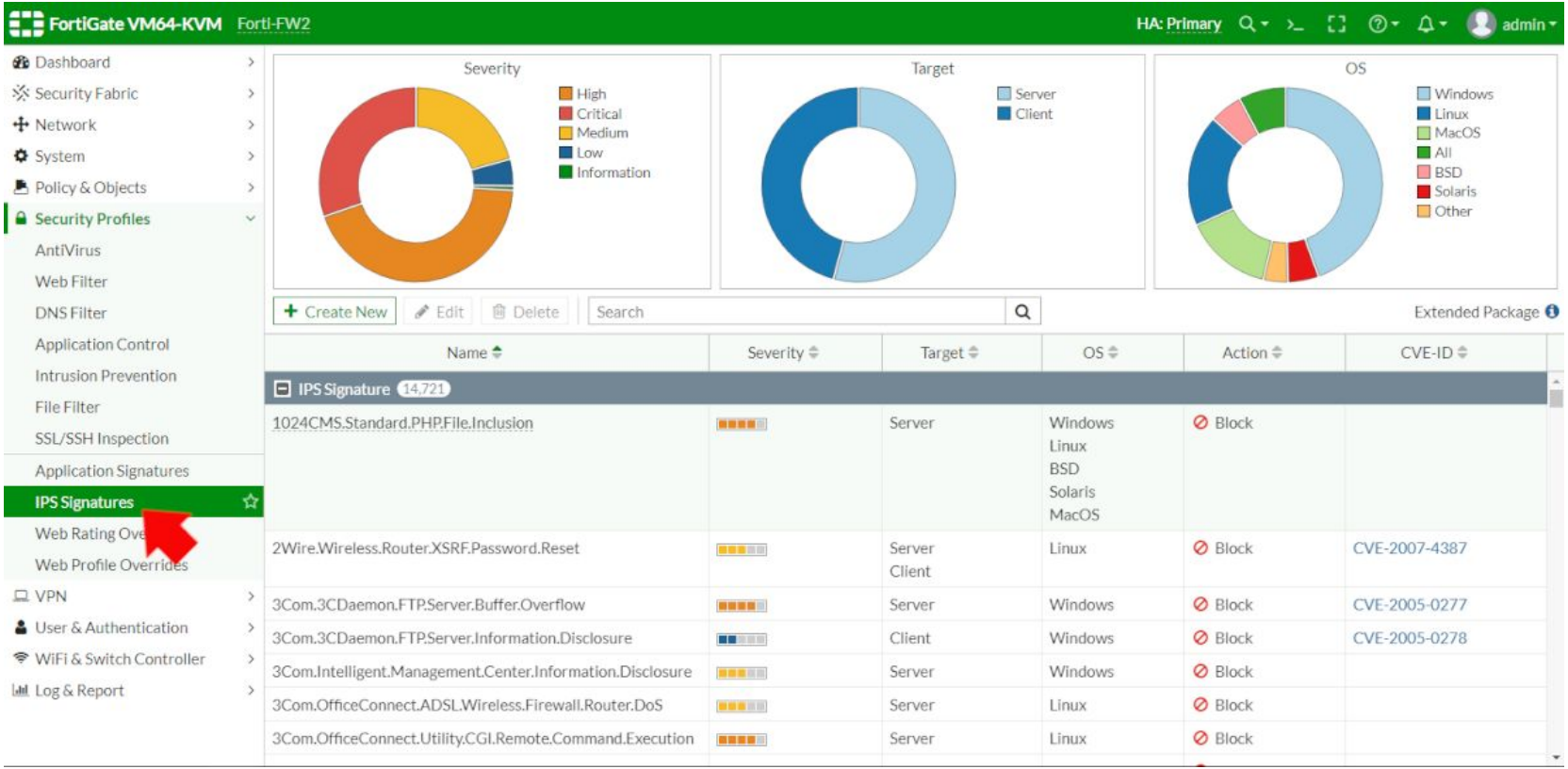
SECRETARÍA DE FINANZAS
QUERÉTARO

UNAM
JURIQUILLA

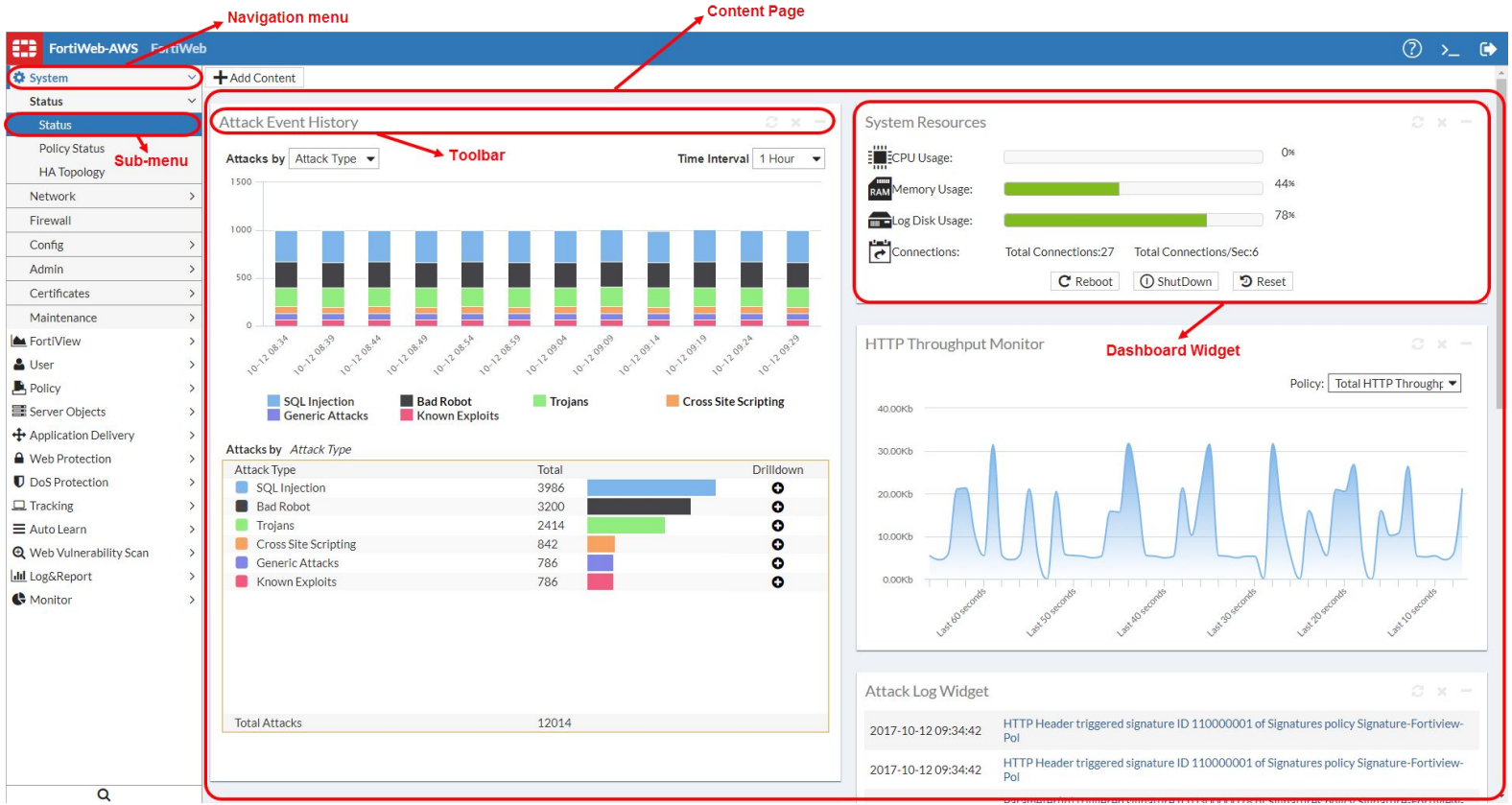
UNIVERSIDAD AUTÓNOMA DE QUERÉTARO
EDUCO EN LA VERDAD Y EN EL HONOR


HERRAMIENTAS BÁSICAS DE CIBERSEGURIDAD
¡URGENTE!
① FIREWALL
(red)
TU
ORGANIZACIÓN
③ EDR
(endpoints)
② WAF
(servicios web y APIs)
④ CULTURA DE LA CIBERSEGURIDAD

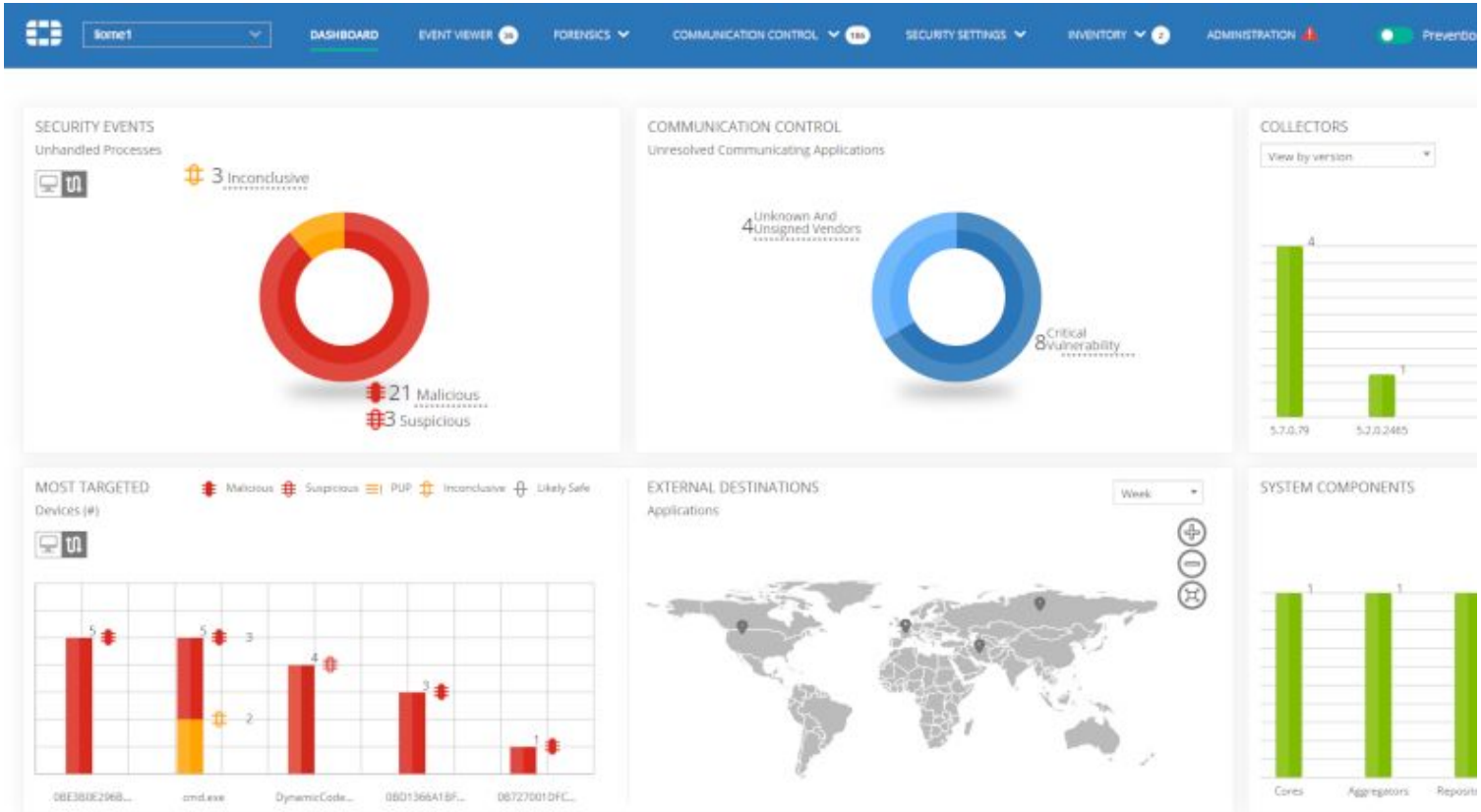
1) La puerta 🔥 - Firewall



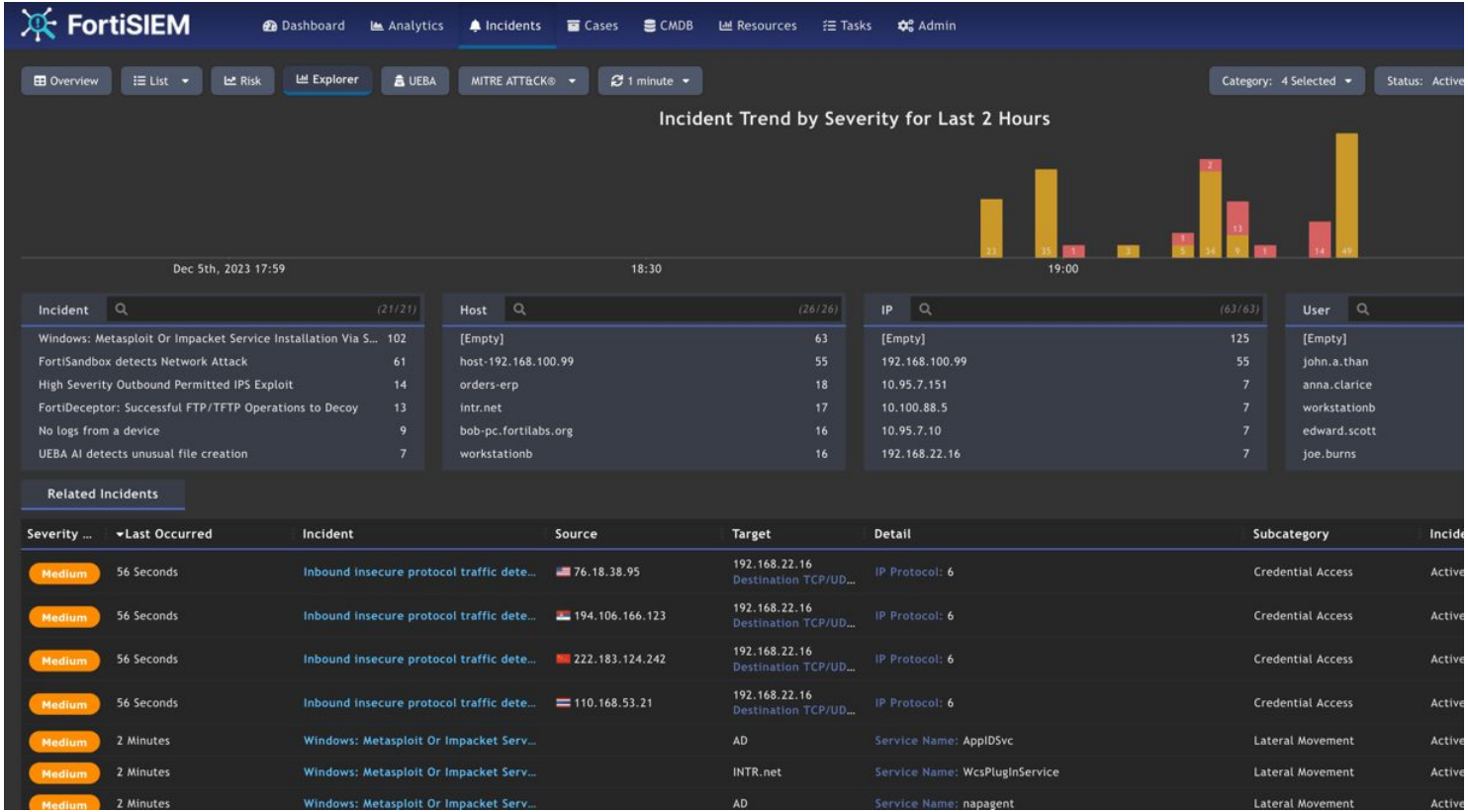
2) El escudo - WAF



3) El SWAT 🚨 - EDR

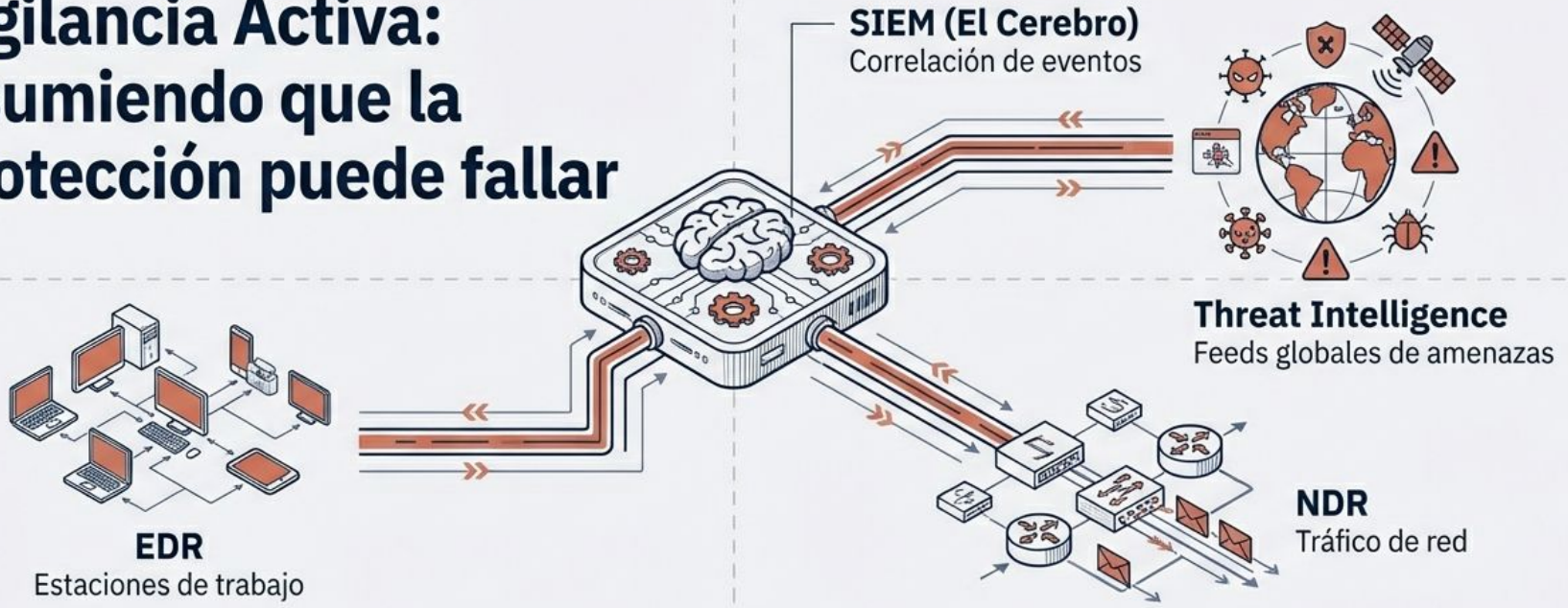

DASHBOARD
EVENT VIEWER
FORENSICS
COMMUNICATION CONTROL
SECURITY SETTINGS
INVENTORY
ADMINISTRATION
SECURITY EVENTS
Unhandled Processes
3 Inconclusive
21 Malicious
3 Suspicious
COMMUNICATION CONTROL
Unresolved Communicating Applications
4 Unknown And Unsigned Vendors
8 Critical Vulnerability
COLLECTORS
View by version
MOST TARGETED
Devices (#)
Malicious
Suspicious
PUP
Inconclusive
Likely Safe
cmd.exe
DynamicCode...
EXTERNAL DESTINATIONS
Applications
Week
SYSTEM COMPONENTS
Cores
Aggregators

4) La memoria 🧠 - SIEM



DETECTAR

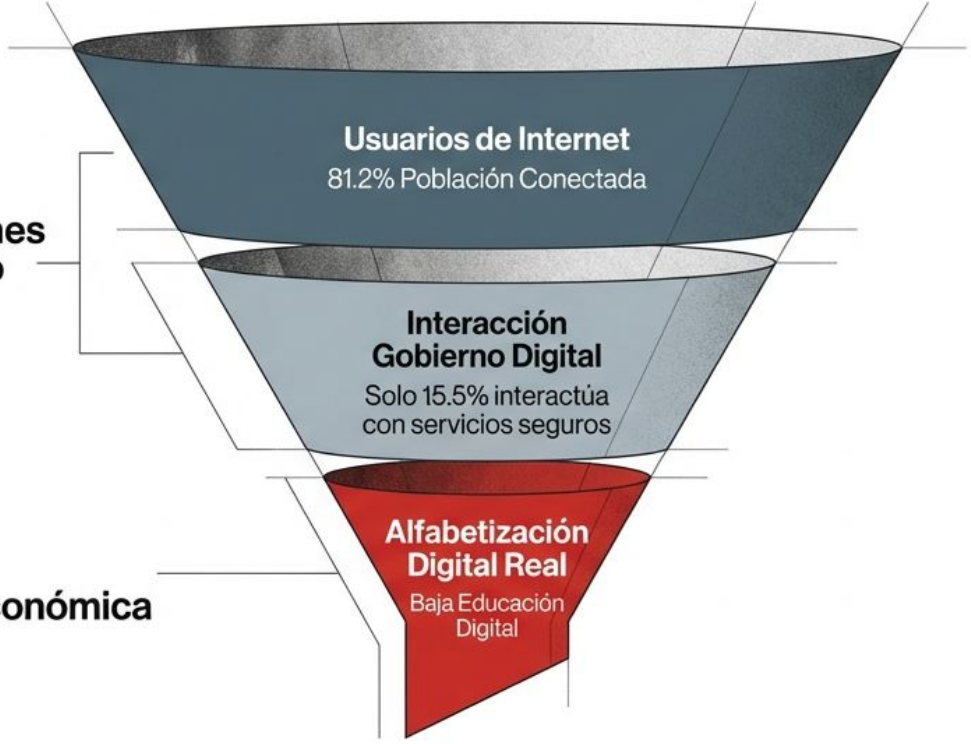
Vigilancia Activa: Asumiendo que la protección puede fallar



Necesitamos ojos en todas partes para identificar anomalías y eventos adversos en tiempo real.

5) Todos para uno - Cultura

Alta conectividad, baja higiene digital: El caldo de cultivo del fraude



10.2 Millones sin acceso
(Brecha de desigualdad)

55.3% Barrera económica

Riesgos Asimétricos

La disparidad crea un Riesgo Asimétrico. El usuario promedio domina las redes sociales de entretenimiento, pero carece de protocolos para transacciones seguras. Esto los convierte en blancos fáciles para la Ingeniería Social en entornos que consideran "seguros" como WhatsApp.

- **Exposición a Phishing dirigido**
- **Suplantación de identidad en redes**
- **Fraudes financieros en plataformas "confiables"**
- **Compromiso de datos sensibles**

La paradoja de la inclusión financiera y el riesgo digital

32%

De los usuarios financieros desconfían de las instituciones por experiencias de fraude.

- El Reto: Digitalizar servicios para comunidades remotas expande la superficie de ataque.
- Perfil de Riesgo: Socios con baja educación digital son vulnerables a Ingeniería Social (vishing, clonación).
- Implicación: La seguridad debe incluir educación constante al socio para preservar el vínculo cooperativo.

El Eslabón Humano: Donde la tecnología falla, la psicología prevalece

Los atacantes no “rompen” firewalls; “hackean” a las personas usando urgencia, miedo y curiosidad.

La tecnología por sí sola es insuficiente.

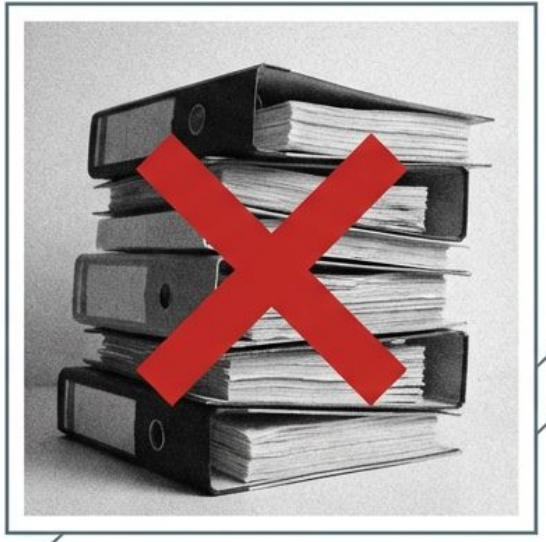
Dato Clave: El ROI de la capacitación en seguridad es del 340% al prevenir tiempos de inactividad catastróficos.

Estrategia Cultural 1: Programa de Embajadores de Ciberseguridad

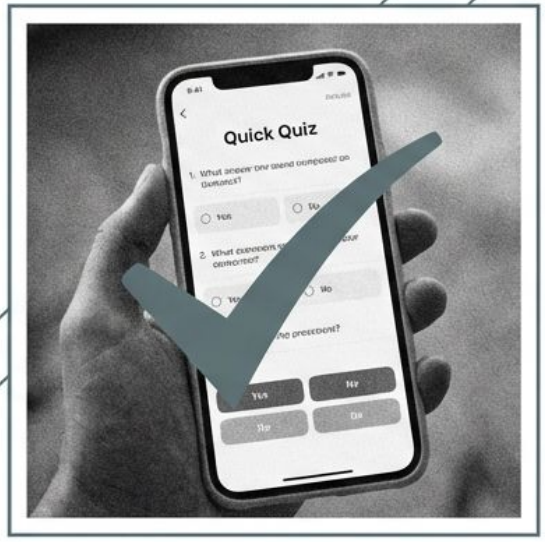
- 1. **Descentralización**: Seleccionar "campeones" en áreas no técnicas.
- 2. **Perfil**: Buscar comunicadores e influencers internos, no expertos técnicos.
- 3. **Enfoque 'Habilidad de Vida'**: Capacitar para proteger a su familia y finanzas personales. Si valoran la seguridad en casa, la aplicarán en el trabajo.
- 4. **Comunicación**: Canales seguros para reportar sin miedo al castigo.

Estrategia Cultural 2: Gamificación y ‘Memoria Muscular’ Digital

El objetivo es crear reflejos condicionados ante las amenazas, no memorizar teoría.



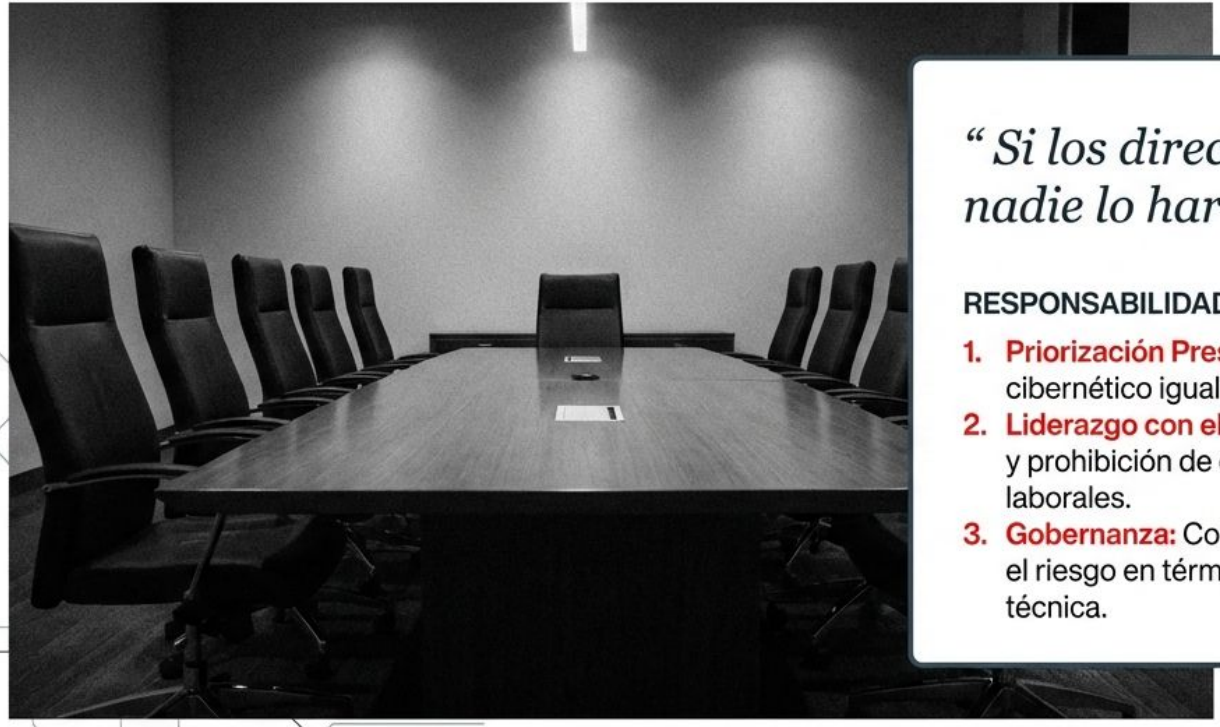
Curso Anual Aburrido



Micro-aprendizaje

- **Simulaciones de Phishing**: Entrenamiento en tiempo real. Recompensa al que reporta, educa (no castiga) al que cae.
- **Micro-módulos**: 5-10 minutos de contenido semanal.
- **Historias de Éxito**: Compartir casos reales donde un empleado detuvo un ataque (‘Near Misses’).

El Rol de la Alta Dirección: La cultura fluye en cascada



“ Si los directivos no cumplen, nadie lo hará.”

RESPONSABILIDADES DE LA JUNTA:

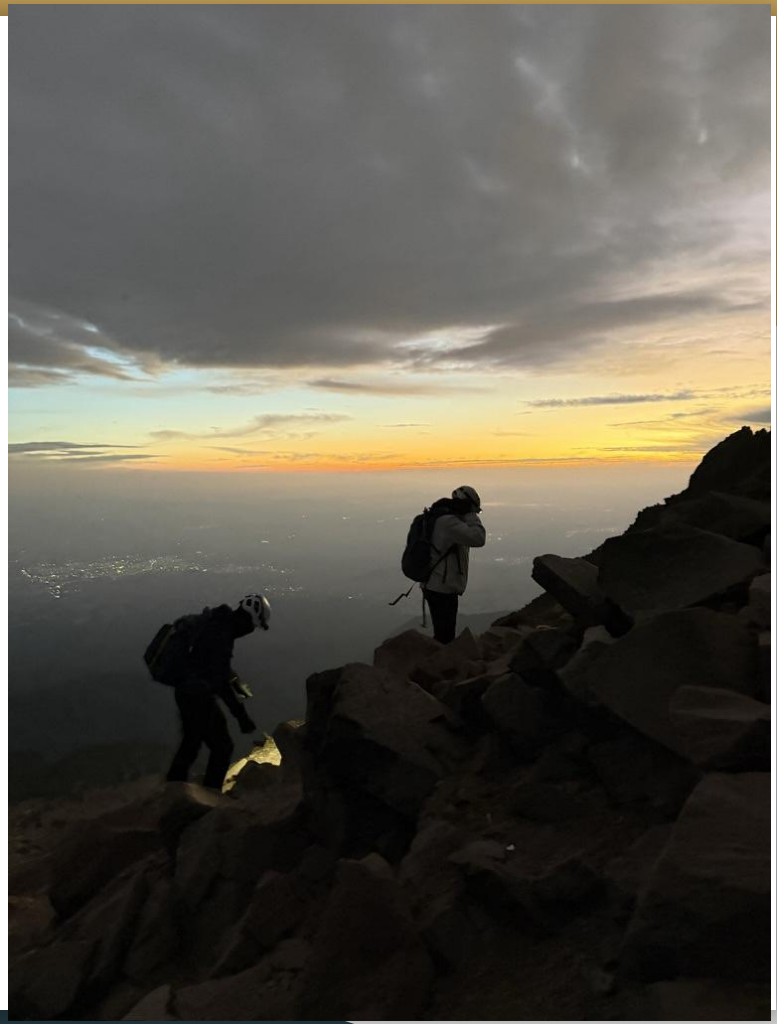
1. **Priorización Presupuestal:** Tratar el riesgo cibernético igual que el financiero.
2. **Liderazgo con el Ejemplo:** Uso obligatorio de MFA y prohibición de correo personal para temas laborales.
3. **Gobernanza:** Comités de supervisión que evalúen el riesgo en términos de negocio, no en jerga técnica.

La importancia del equipo

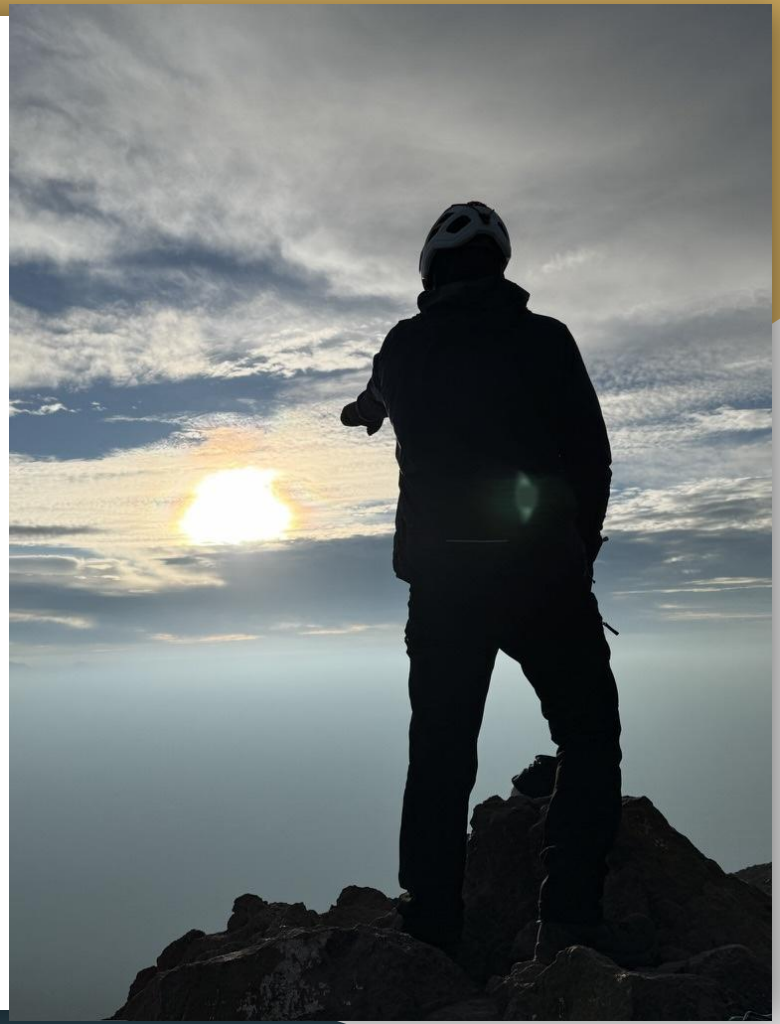
Una meta inalcanzable

Planea y prepara

Ataca

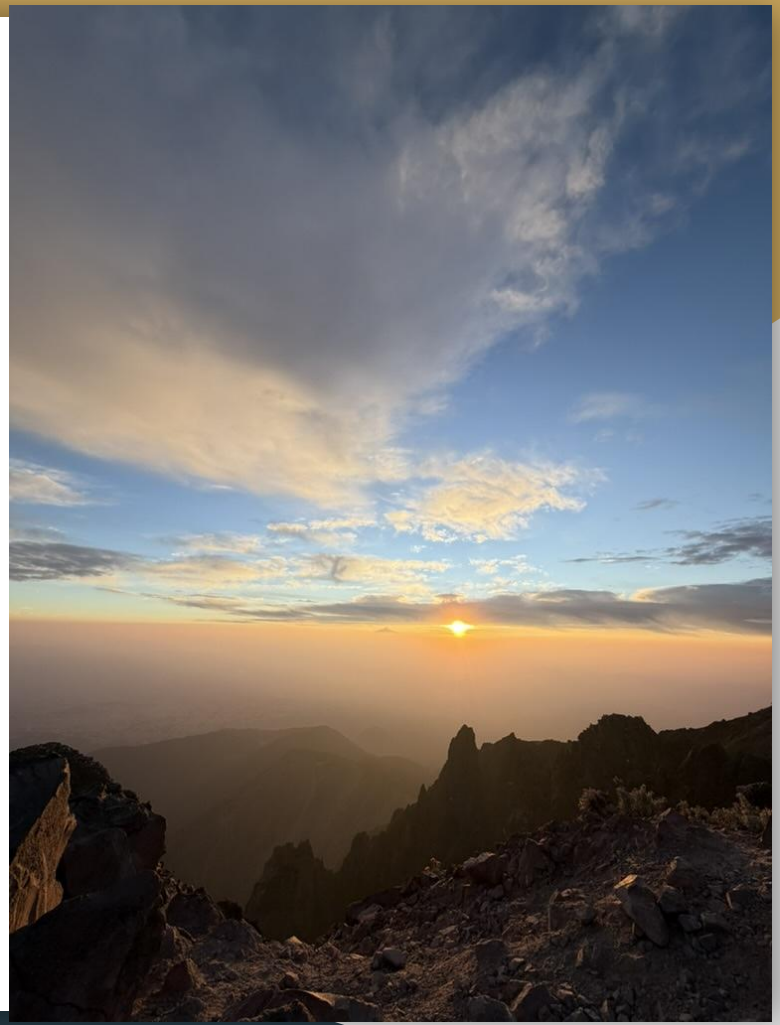


Celebra cada logro



Ajusta y adapta

Establece nuevas metas



Cultiva y crece tu equipo

QUERÉTARO
SECRETARÍA DE FINANZAS
UNAM JURIQUILLA
UNIVERSIDAD AUTONOMA DE QUERETARO
EDUCO EN LA VERDAD Y EN EL HONOR

PODER EJECUTIVO DEL ESTADO DE QUERÉTARO
SECRETARÍA DE FINANZAS
UNAM JURIQUILLA
UNIVERSIDAD AUTONOMA DE QUERETARO
EDUCO EN LA VERDAD Y EN EL HONOR

ciso@queretaro.gob.mx

De la estrategia a la acción

PODER EJECUTIVO DEL ESTADO DE QUERÉTARO
SECRETARÍA DE FINANZAS
UNAM JURIQUILLA
UNIVERSIDAD AUTÓNOMA DE QUERÉTARO
EDUCO EN LA VERDAD Y EN EL HONOR