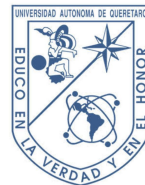


La primera línea de defensa, capacitación

La Visión Práctica de un CISO
Ulises MA



SECRETARÍA DE
FINANZAS



443%

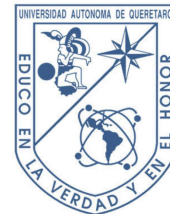
Incremento de pérdidas económicas reportadas en instituciones financieras
en México, 2024–2025



SECRETARÍA DE
FINANZAS



UNAM
JURIQUILLA



Imaginen sus cajas de ahorro o fábricas como fortalezas.

Antes, los ladrones usaban
palancas y explosivos.



Hoy, usan teclados y código.



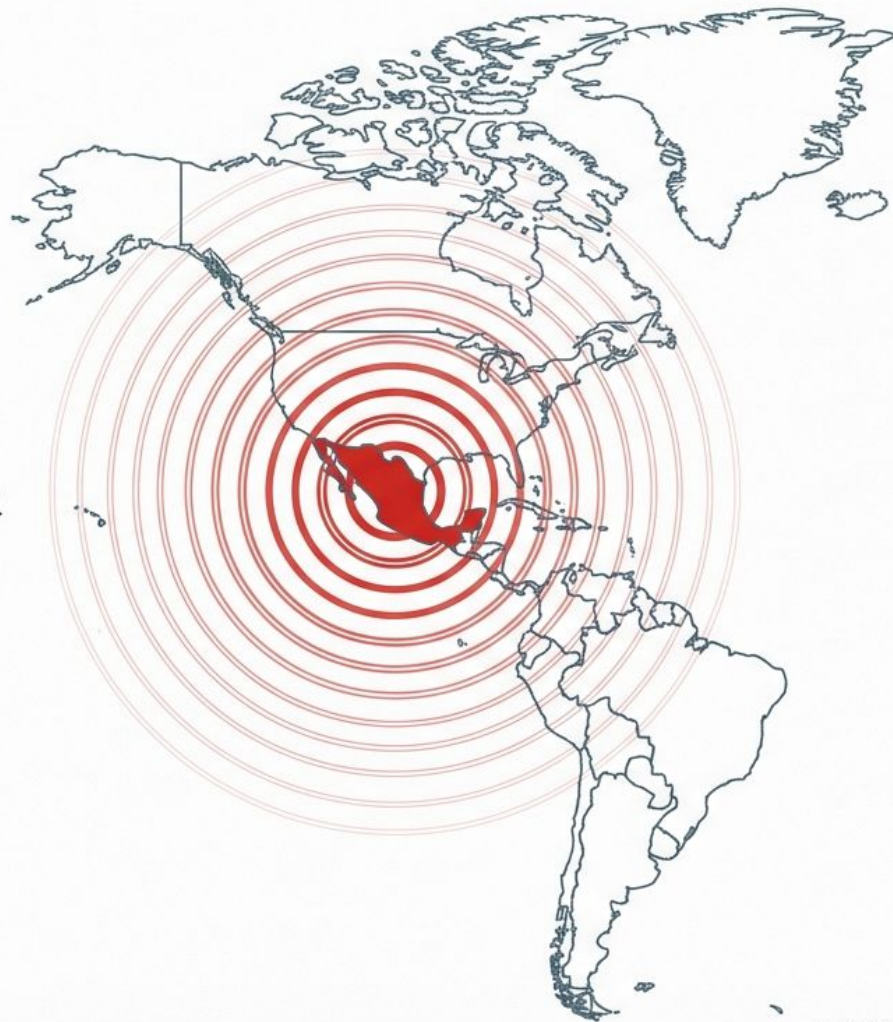
¡La ciberseguridad es la nueva muralla!

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

COMPARATIVO
LATINOAMÉRICA

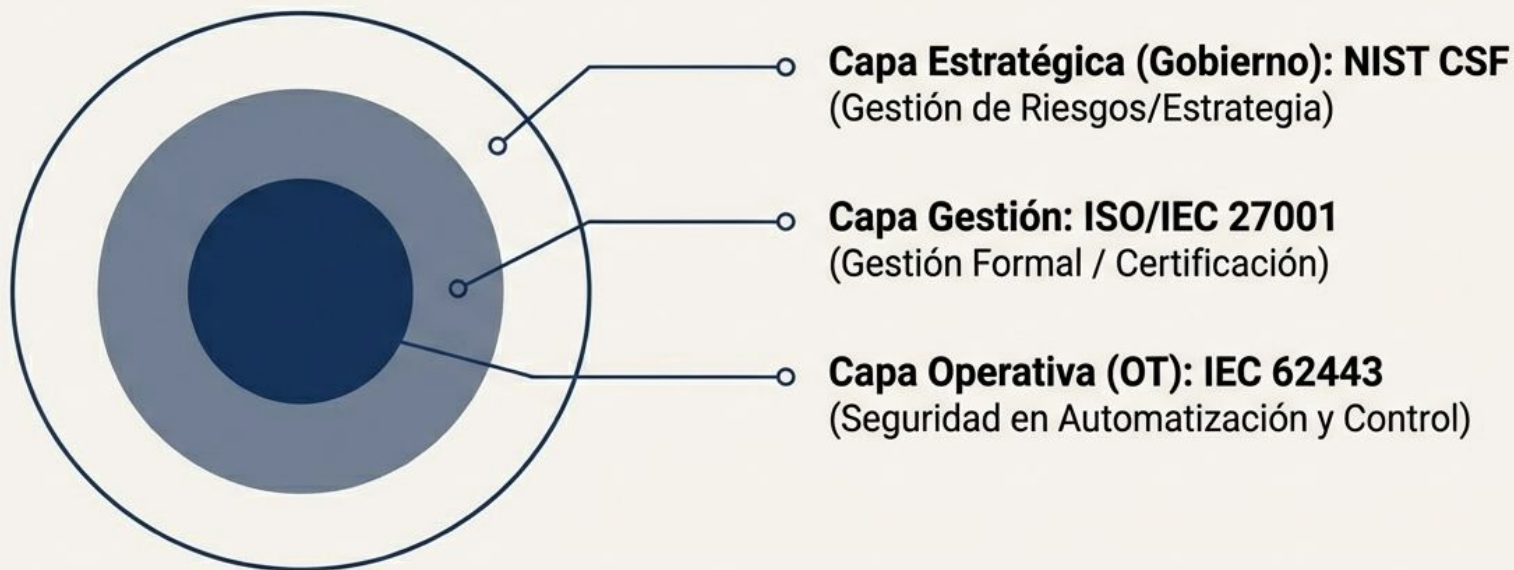
Brasil: #1

México: #2

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.



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.



SECRETARÍA DE
FINANZAS



¿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)**.

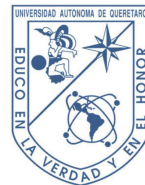
- ✓ Equivalencia total con ISO/IEC 27001.
- ✓ Avalada por organismos mexicanos (NYCE).
- ✓ Marco legal y normativo local.



SECRETARÍA DE
FINANZAS



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.



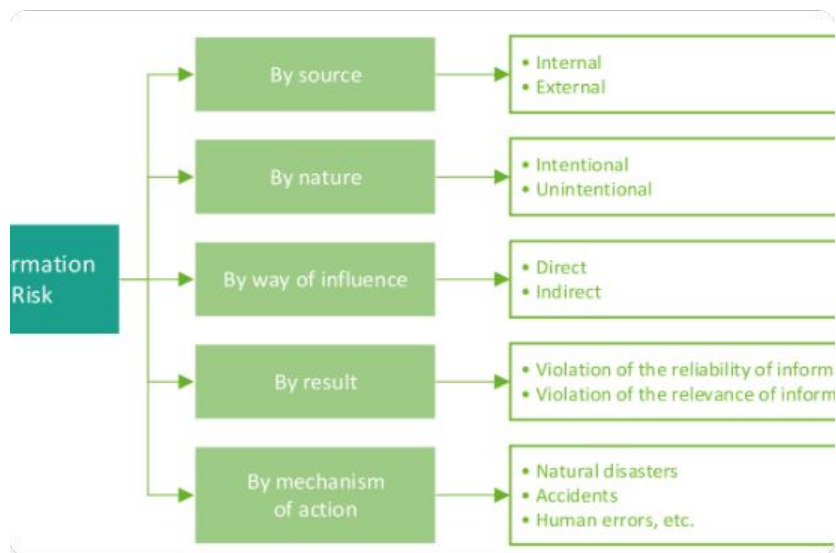
SECRETARÍA DE
FINANZAS



UNAM
JURIQUILLA



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



UNAM
JURIQUILLA



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.



SECRETARÍA DE
FINANZAS



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

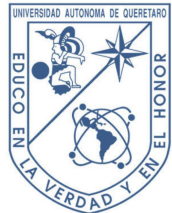


PODER EJECUTIVO DEL ESTADO DE
QUERÉTARO

SECRETARÍA DE
FINANZAS



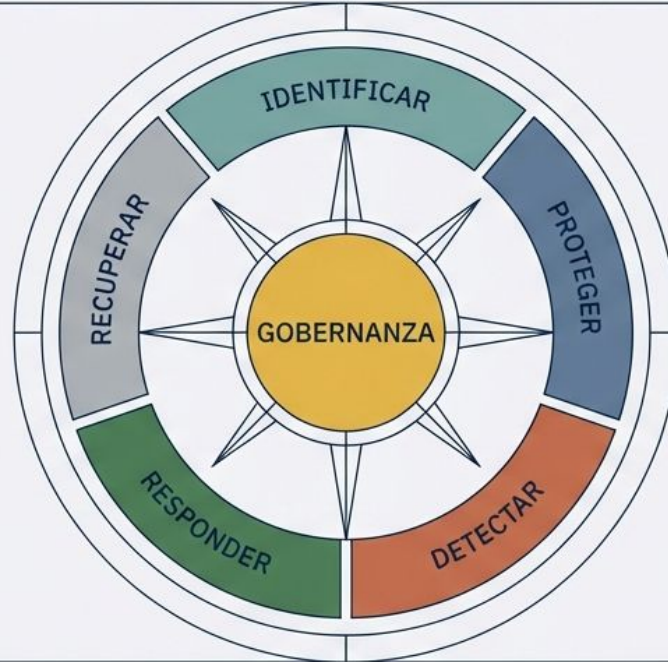
UNAM
JURIQUILLA



UNIVERSIDAD AUTÓNOMA DE QUERÉTARO
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

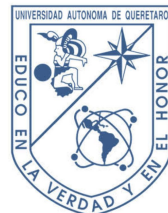


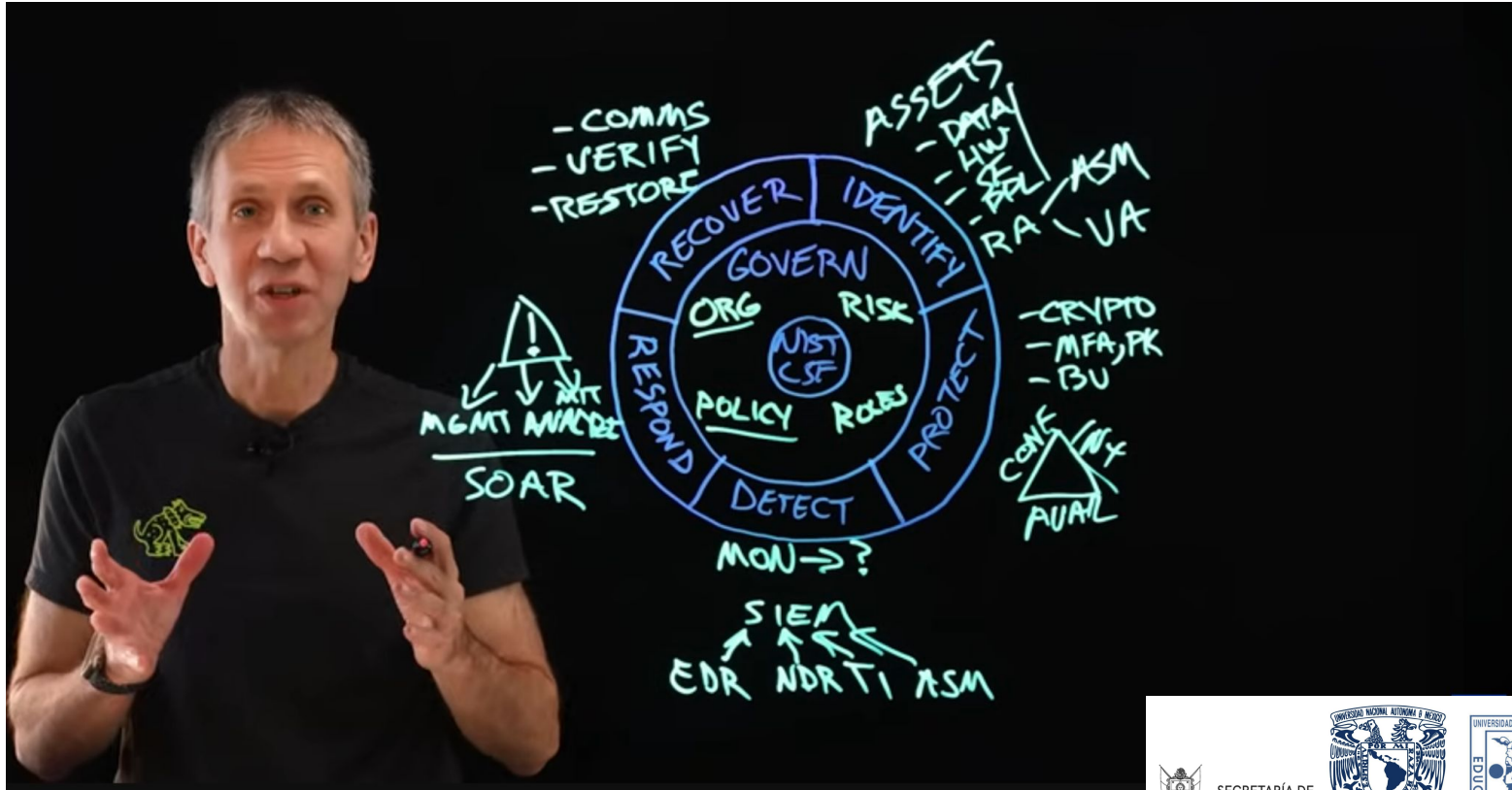
GOBIERNO DEL ESTADO DE
QUERÉTARO

SECRETARÍA DE
FINANZAS



UNAM
JURIQUILLA





<https://youtu.be/U1a3TG8QS7g?si=q32RnaYLjoLgONzw>



SECRETARÍA DE
FINANZAS



UNAM
JURIQUILLA



HERRAMIENTAS BÁSICAS DE CIBERSEGURIDAD

¡URGENTE!

① FIREWALL
(red)



② WAF
(servicios web y APIs)



③ EDR
(endpoints)



④ CULTURA DE LA CIBERSEGURIDAD



TU ORGANIZACIÓN




1) La puerta - Firewall

FortiGate VM64-KVM Forti-FW2 HA: Primary admin


- Dashboard
- Security Fabric
- Network
- System
- Policy & Objects
- Security Profiles**
 - AntiVirus
 - Web Filter
 - DNS Filter
 - Application Control
 - Intrusion Prevention
 - File Filter
 - SSL/SSH Inspection
 - Application Signatures
 - IPS Signatures** ☆
 - Web Rating Overrides
 - Web Profile Overrides
- VPN
- User & Authentication
- WiFi & Switch Controller
- Log & Report

Severity



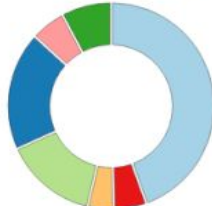
- High
- Critical
- Medium
- Low
- Information

Target



- Server
- Client

OS



- Windows
- Linux
- MacOS
- All
- BSD
- Solaris
- Other

[+ Create New](#) [Edit](#) [Delete](#) Search [Extended Package](#)

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 14,721					
1024CMS.Standard.PHP.File.Inclusion	High	Server	Windows Linux BSD Solaris MacOS	Block	
2Wire.Wireless.Router.XSRF.Password.Reset	High	Server Client	Linux	Block	CVE-2007-4387
3Com.3CDaemon.FTP.Server.Buffer.Overflow	High	Server	Windows	Block	CVE-2005-0277
3Com.3CDaemon.FTP.Server.Information.Disclosure	Medium	Client	Windows	Block	CVE-2005-0278
3Com.Intelligent.Management.Center.Information.Disclosure	High	Server	Windows	Block	
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	High	Server	Linux	Block	
3Com.OfficeConnect.Utility.CGI.Remote.Command.Execution	High	Server	Linux	Block	

2) El escudo - WAF



Navigation menu (left sidebar)

- System
- Status
- Attack Event History (selected)
- Policy Status
- HA Topology
- Network
- Firewall
- Config
- Admin
- Certificates
- Maintenance
- FortiView
- User
- Policy
- Server Objects
- Application Delivery
- Web Protection
- DoS Protection
- Tracking
- Auto Learn
- Web Vulnerability Scan
- Log&Report
- Monitor

Content Page (main area)

Attack Event History

Attacks by: Attack Type | Time Interval: 1 Hour

Toolbar (above chart): Attack Type, Time Interval

Attack Type	Total	Drilldown
SQL Injection	3986	+
Bad Robot	3200	+
Trojans	2414	+
Cross Site Scripting	842	+
Generic Attacks	786	+
Known Exploits	786	+

Total Attacks: 12014

System Resources

- CPU Usage: 0%
- Memory Usage: 44%
- Log Disk Usage: 78%
- Connections: Total Connections:27, Total Connections/Sec:6

Buttons: Reboot, ShutDown, Reset

HTTP Throughput Monitor

Policy: Total HTTP Throughput

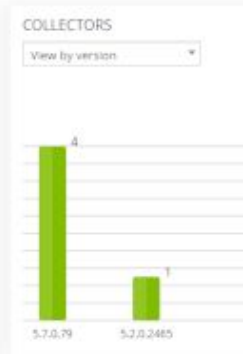
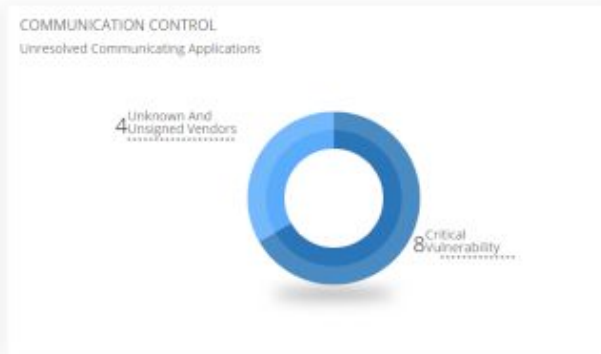
Dashboard Widget (label pointing to the HTTP Throughput Monitor)

Attack Log Widget

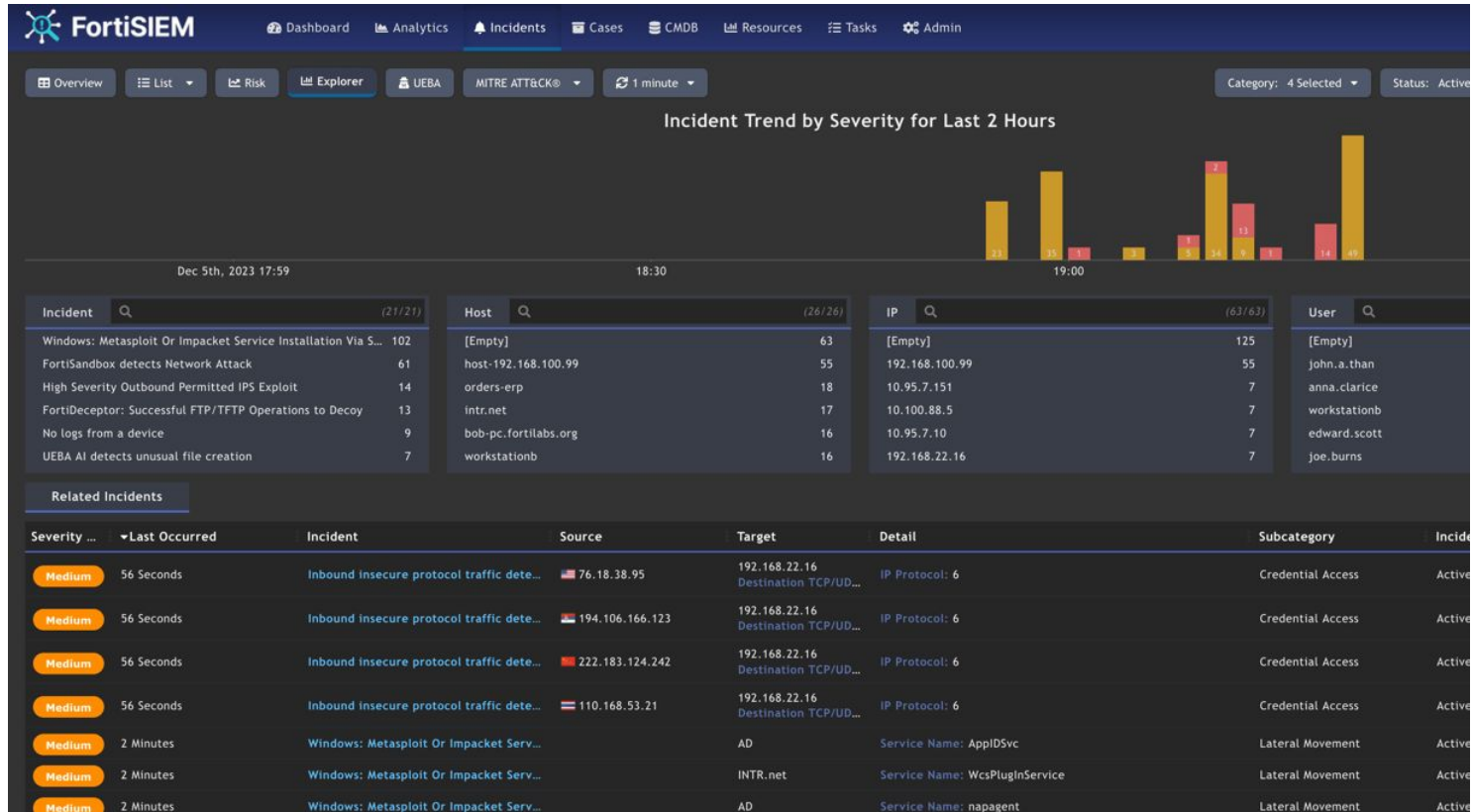
2017-10-12 09:34:42	HTTP Header triggered signature ID 110000001 of Signatures policy Signature-Fortiview-Pol
2017-10-12 09:34:42	HTTP Header triggered signature ID 110000001 of Signatures policy Signature-Fortiview-Pol

3) EL SWAT - EDR

Home1 | DASHBOARD | EVENT VIEWER 26 | FORENSICS | COMMUNICATION CONTROL 180 | SECURITY SETTINGS | INVENTORY 2 | ADMINISTRATION  |  Prevention



4) La memoria - SIEM



The screenshot displays the FortiSIEM dashboard interface. At the top, there is a navigation bar with tabs for Dashboard, Analytics, Incidents, Cases, CMDb, Resources, Tasks, and Admin. Below this, a secondary navigation bar includes Overview, List, Risk, Explorer, UEBA, MITRE ATT&CK, and a refresh button set to 1 minute. The main content area features a bar chart titled "Incident Trend by Severity for Last 2 Hours" showing incident counts over time. Below the chart, there are four filterable tables for Incident, Host, IP, and User. At the bottom, a "Related Incidents" table lists recent events with columns for Severity, Last Occurred, Incident, Source, Target, Detail, Subcategory, and Incident Status.

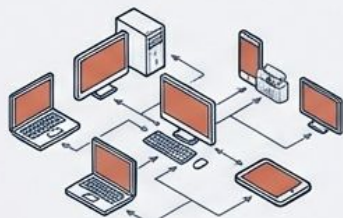
Time	High	Medium	Low
18:00	15	1	1
18:30	1	5	1
19:00	13	6	1
19:30	14	4	1

Incident	Count	Host	Count	IP	Count	User	Count
Windows: Metasploit Or Impacket Service Installation Via S...	102	[Empty]	63	[Empty]	125	[Empty]	0
FortiSandbox detects Network Attack	61	host-192.168.100.99	55	192.168.100.99	55	john.a.than	1
High Severity Outbound Permitted IPS Exploit	14	orders-erp	18	10.95.7.151	7	anna.clarice	1
FortiDeceptor: Successful FTP/TFTP Operations to Decoy	13	intr.net	17	10.100.88.5	7	workstationb	1
No logs from a device	9	bob-pc.fortilabs.org	16	10.95.7.10	7	edward.scott	1
UEBA AI detects unusual file creation	7	workstationb	16	192.168.22.16	7	joe.burns	1

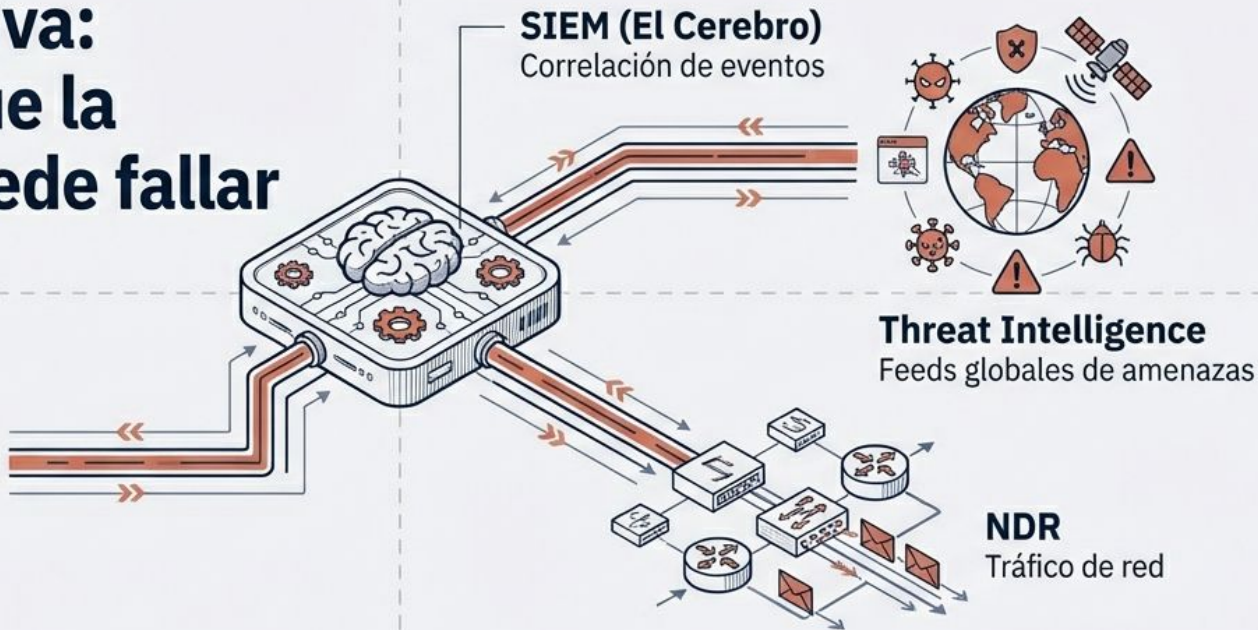
Severity	Last Occurred	Incident	Source	Target	Detail	Subcategory	Incident Status
Medium	56 Seconds	Inbound insecure protocol traffic dete...	76.18.38.95	192.168.22.16	IP Protocol: 6	Credential Access	Active
Medium	56 Seconds	Inbound insecure protocol traffic dete...	194.106.166.123	192.168.22.16	IP Protocol: 6	Credential Access	Active
Medium	56 Seconds	Inbound insecure protocol traffic dete...	222.183.124.242	192.168.22.16	IP Protocol: 6	Credential Access	Active
Medium	56 Seconds	Inbound insecure protocol traffic dete...	110.168.53.21	192.168.22.16	IP Protocol: 6	Credential Access	Active
Medium	2 Minutes	Windows: Metasploit Or Impacket Serv...		AD	Service Name: AppIDSvc	Lateral Movement	Active
Medium	2 Minutes	Windows: Metasploit Or Impacket Serv...		INTR.net	Service Name: WcsPluginService	Lateral Movement	Active
Medium	2 Minutes	Windows: Metasploit Or Impacket Serv...		AD	Service Name: napagent	Lateral Movement	Active

DETECTAR

Vigilancia Activa: Asumiendo que la protección puede fallar



EDR
Estaciones de trabajo

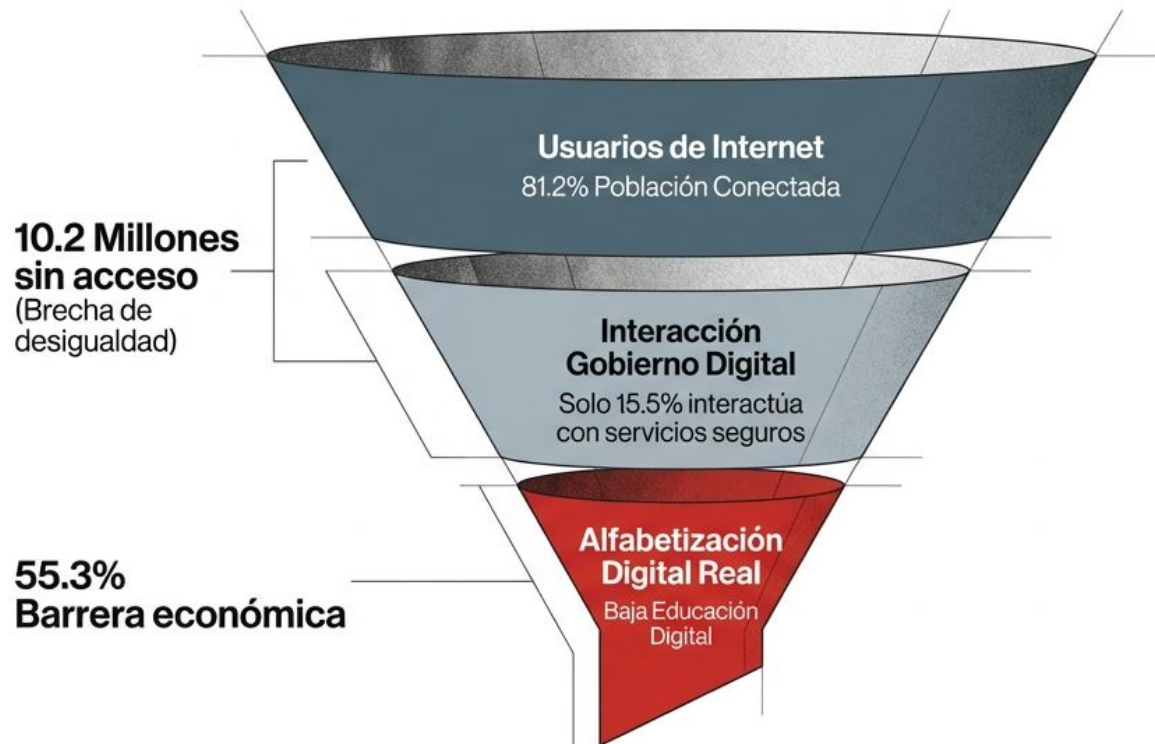


Necesitamos ojos en todas partes para identificar anomalías y eventos adversos en tiempo real.

5) Todos para uno - Cultura



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



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.

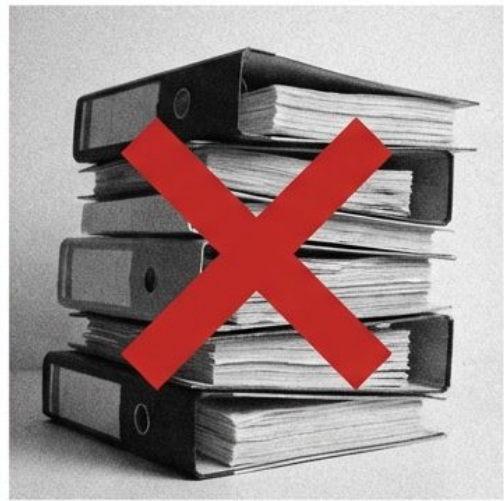
Estrategia Cultural 1: Programa de Embajadores de Ciberseguridad

- 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.

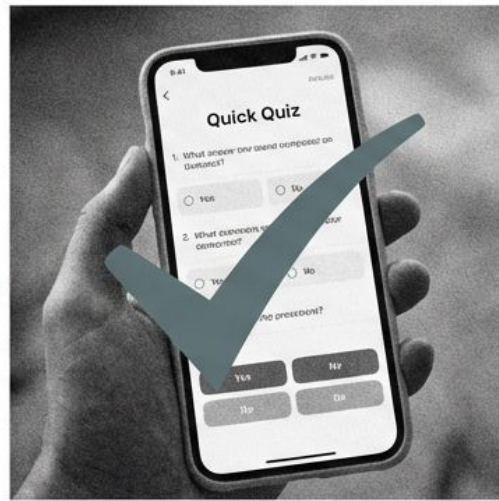


Estrategia Cultural 2: Gamificación y 'Memoria Muscular' Digital

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



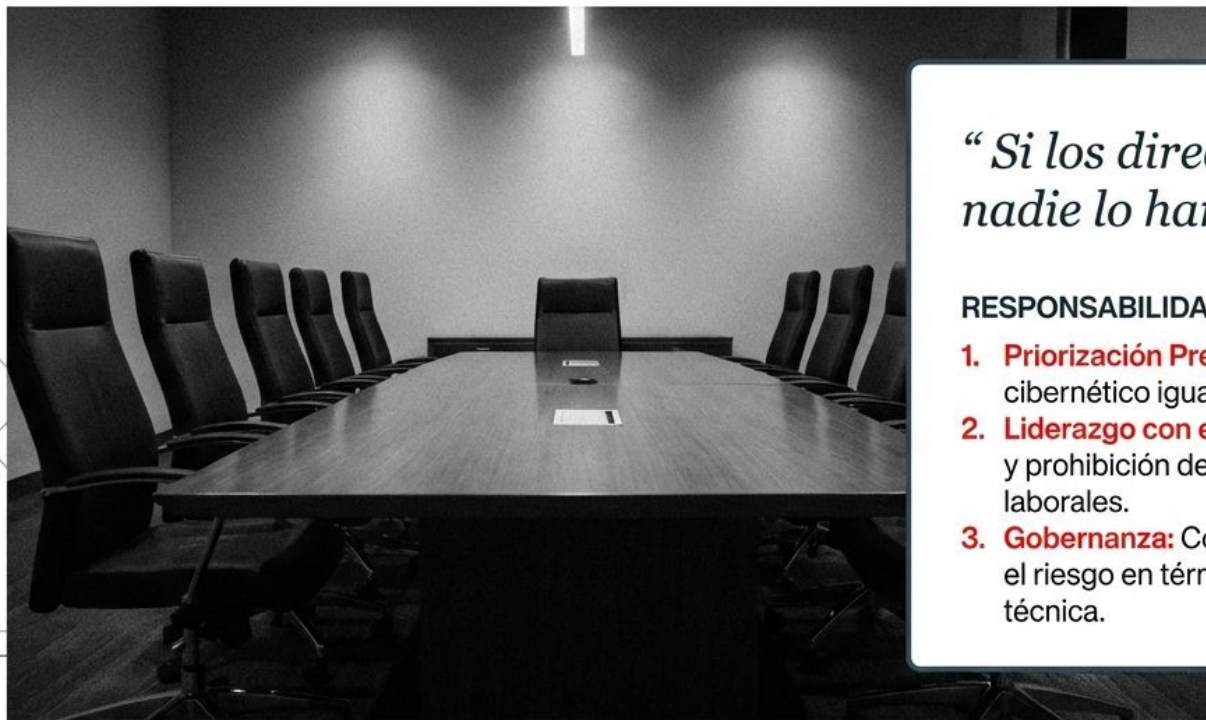
Curso Anual Aburrido



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

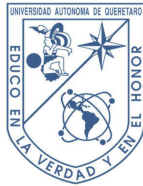
Una meta inalcanzable



SECRETARÍA DE
FINANZAS



UNAM
JURIQUILLA



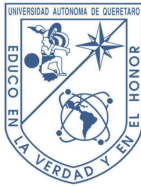
Planea y prepara



SECRETARÍA DE
FINANZAS



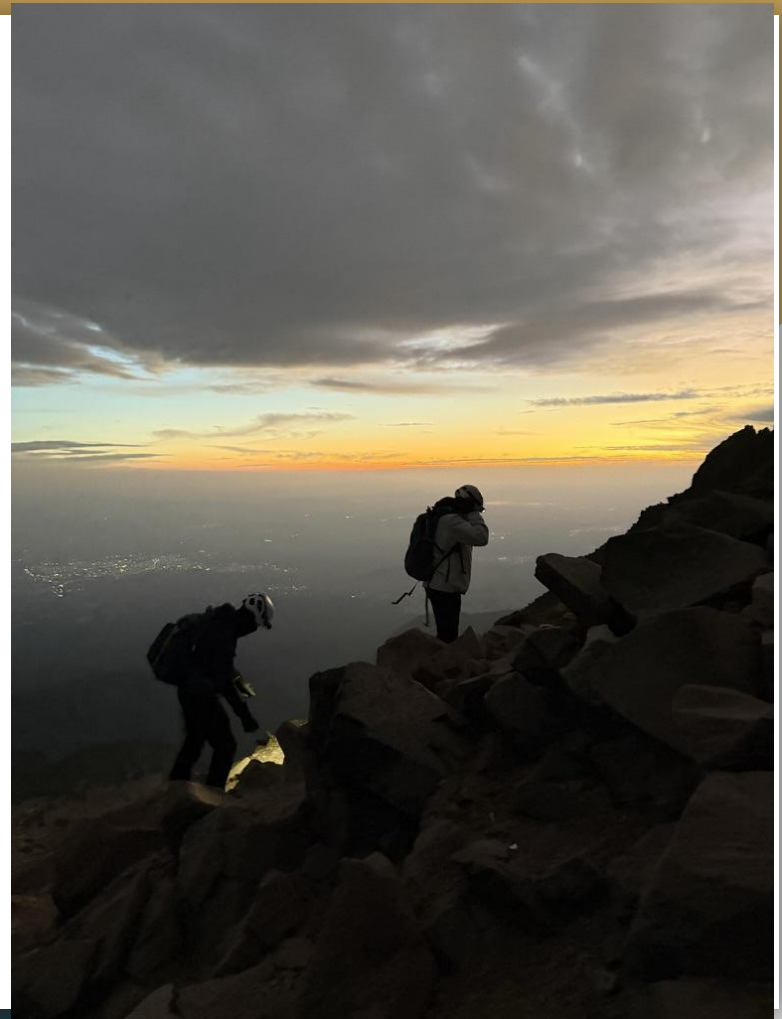
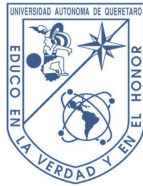
UNAM
JURIQUILLA



Ataca



SECRETARÍA DE
FINANZAS



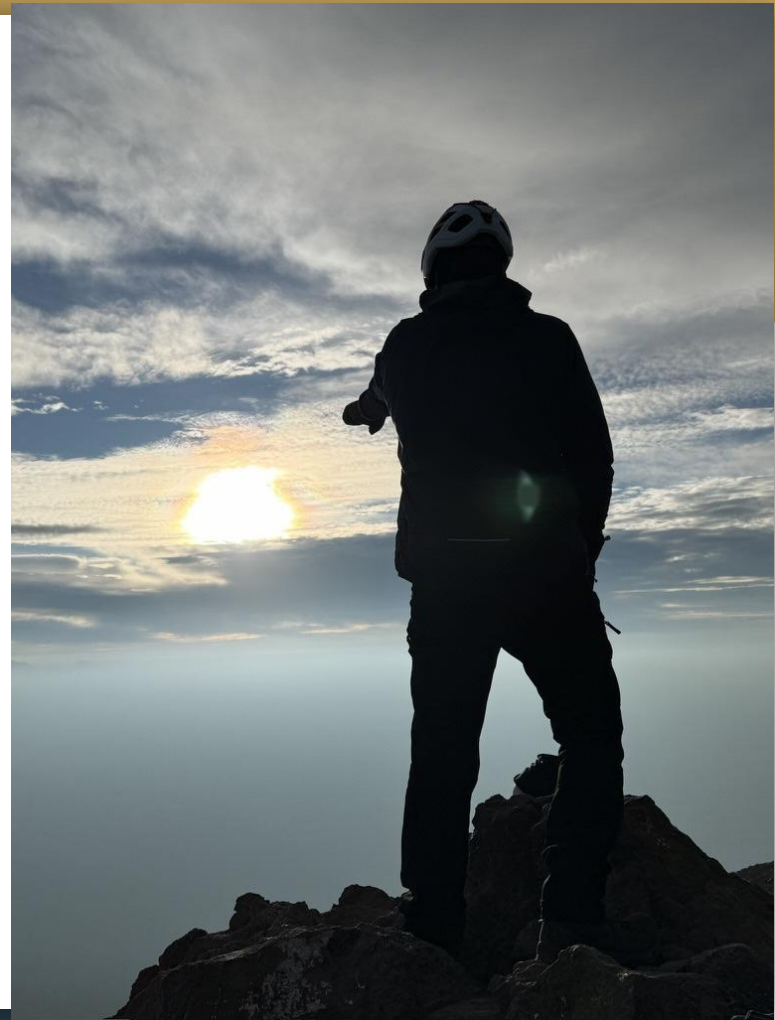
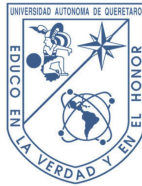
Celebra cada logro



SECRETARÍA DE
FINANZAS



UNAM
JURIQUILLA



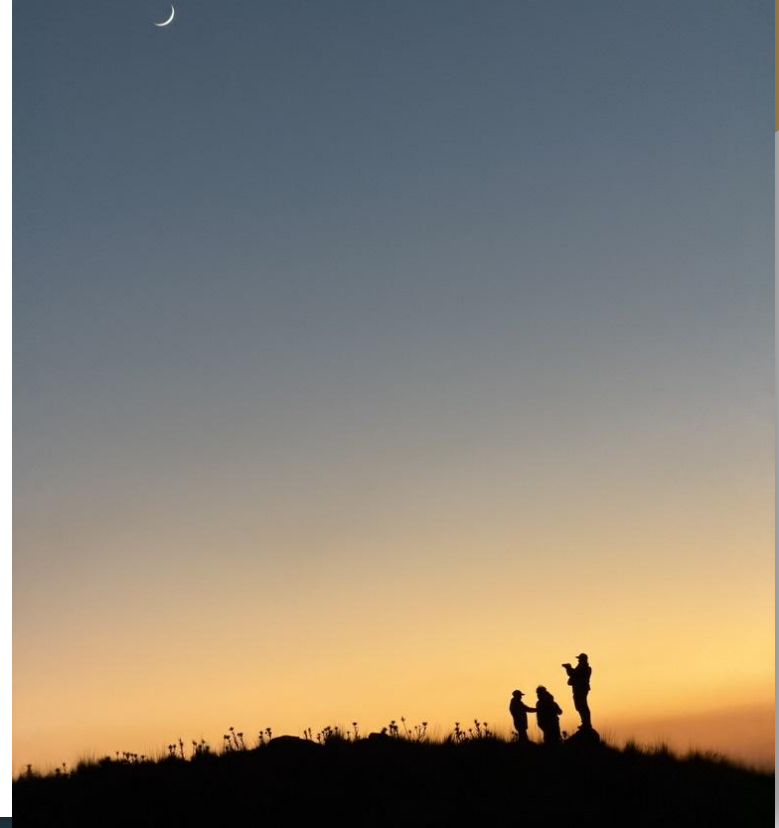
Ajusta y adapta



SECRETARÍA DE
FINANZAS



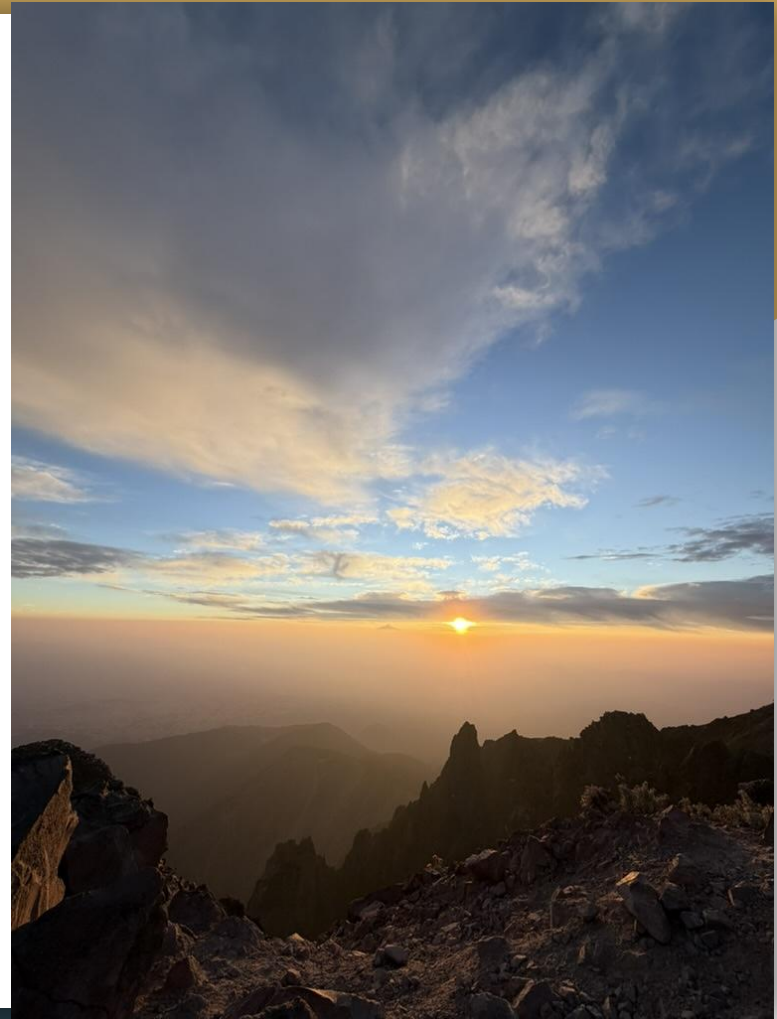
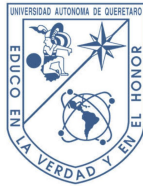
UNAM
JURIQUILLA



Establece nuevas metas



SECRETARÍA DE
FINANZAS



Cultiva y crece
tu equipo



SECRETARÍA DE
FINANZAS

QUERÉTARO

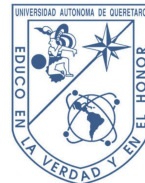




SECRETARÍA DE
FINANZAS



UNAM
JURIQUILLA



ciso@queretaro.gob.mx

De la estrategia a la acción



SECRETARÍA DE
FINANZAS

QUERÉTARO



UNAM
JURIQUILLA

