2025

Bienvenidos al

Taller de Sensibilización

de Seguridad de la Información

Proteger la información es responsabilidad de todos

¿Por qué importa la Seguridad de la Información?

$4.88M

Costo promedio de una brecha en 2024

IBM Cost of Data Breach 2024

Cada 39s

Ocurre un ciberataque en el mundo

University of Maryland

+72 %

Aumento de ataques globales en 3 años

Check Point Research 2024

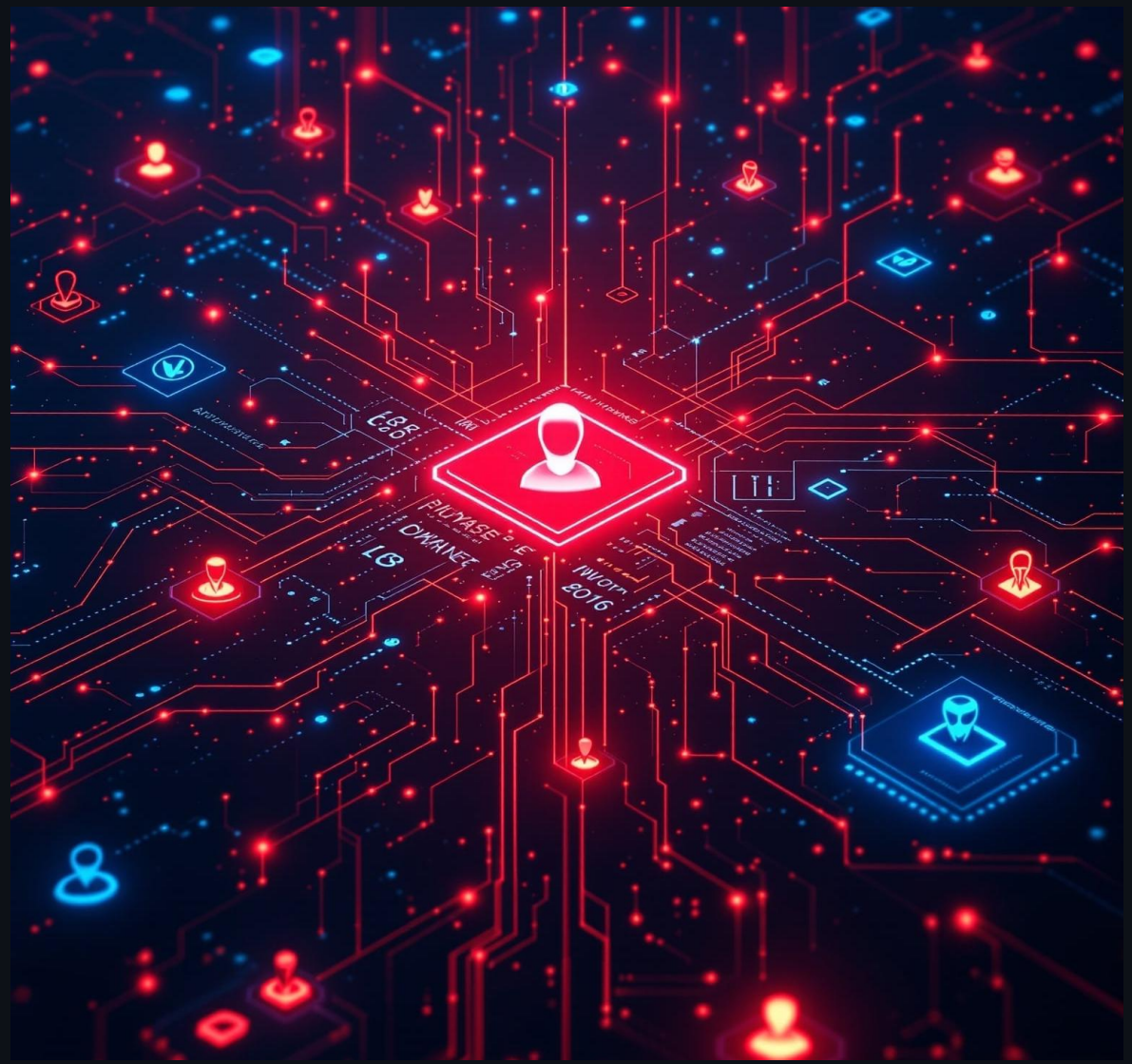
Panorama de Amenazas Actuales

Phishing
Correos falsos que roban credenciales

Ransomware
Secuestro de datos con cifrado malicioso

Ingeniería Social
Manipulación psicológica de personas

Ataques a Redes
Intercepción de comunicaciones



Casos Reales que Marcaron la Historia

⚠ 2017

Equifax

Brecha de Datos

147 millones de personas afectadas

Vulnerabilidad sin parchear en software

⚠ 2021

Colonial Pipeline

Ransomware

$4.4M pagados en rescate

Contraseña comprometida sin MFA

⚠ 2023

MOVEit / múltiples empresas

Cadena de Suministro

+2,500 organizaciones afectadas

Vulnerabilidad 0-day en software de transferencia

Los 3 Pilares de la Seguridad de la Información

La tríada CIA es la base de toda estrategia de seguridad

Confidencialidad

Solo personas autorizadas acceden a la información

Ej: Contraseñas, datos de clientes, información financiera

Integridad

La información no es alterada sin autorización

Ej: Registros contables, contratos, bases de datos

Disponibilidad

Los sistemas están operativos cuando se necesitan

Ej: Backups, redundancia, planes de continuidad

Marcos de Gobernanza de Seguridad

Guías reconocidas internacionalmente para gestionar la seguridad

ISO 27001

Sistema de Gestión de Seguridad de la Información

Políticas, controles y mejora continua

Internacional · Certificable

NIST CSF

Marco de Ciberseguridad del NIST

Identificar, Proteger, Detectar, Responder, Recuperar

EE.UU. · Ampliamente adoptado globalmente

COBIT

Gobierno y Gestión de TI Empresarial

Alineación de TI con objetivos de negocio

Empresarial · Gobernanza corporativa

CIS Controls

Controles Críticos de Seguridad

18 controles priorizados por efectividad

Técnico · Operacional · Práctico

¿Qué marco es el adecuado?

Cada marco tiene un propósito y alcance distinto

ISO 27001	Gestión integral de seguridad	Toda la organización	✓ Sí	Certificación reconocida
NIST CSF	Ciberseguridad por funciones	TI y seguridad	✗ No	Flexibilidad y claridad
COBIT	Gobierno de TI	Directivos y auditores	✓ Sí	Alineación con negocio
CIS Controls	Controles técnicos prácticos	Equipos técnicos	✗ No	Implementación rápida

Metodologías de Proyectos TI Seguros

Integrar seguridad desde el inicio, no al final

Agile Security

Seguridad integrada en cada sprint y ciclo iterativo

Revisiones continuas en el backlog

DevSecOps

Desarrollo, Seguridad y Operaciones trabajando juntos

Seguridad automatizada en CI/CD

SDLC Seguro

Seguridad en cada fase del ciclo de vida del software

Desde requisitos hasta el retiro

El principio clave: "Security by Design" — la seguridad se diseña, no se agrega después

Seguridad en Cada Fase del Desarrollo

DevSecOps integra seguridad en el pipeline completo

1

Planificación

Requisitos de seguridad desde el inicio

2

Diseño

Modelado de amenazas y arquitectura segura

3

Desarrollo

Código seguro y análisis estático (SAST)

4

Pruebas

Pen testing y análisis dinámico (DAST)

5

Operación

Monitoreo continuo y gestión de incidentes

Seguridad como Ventaja Competitiva

Proteger la información también es proteger el negocio

Confianza del Cliente

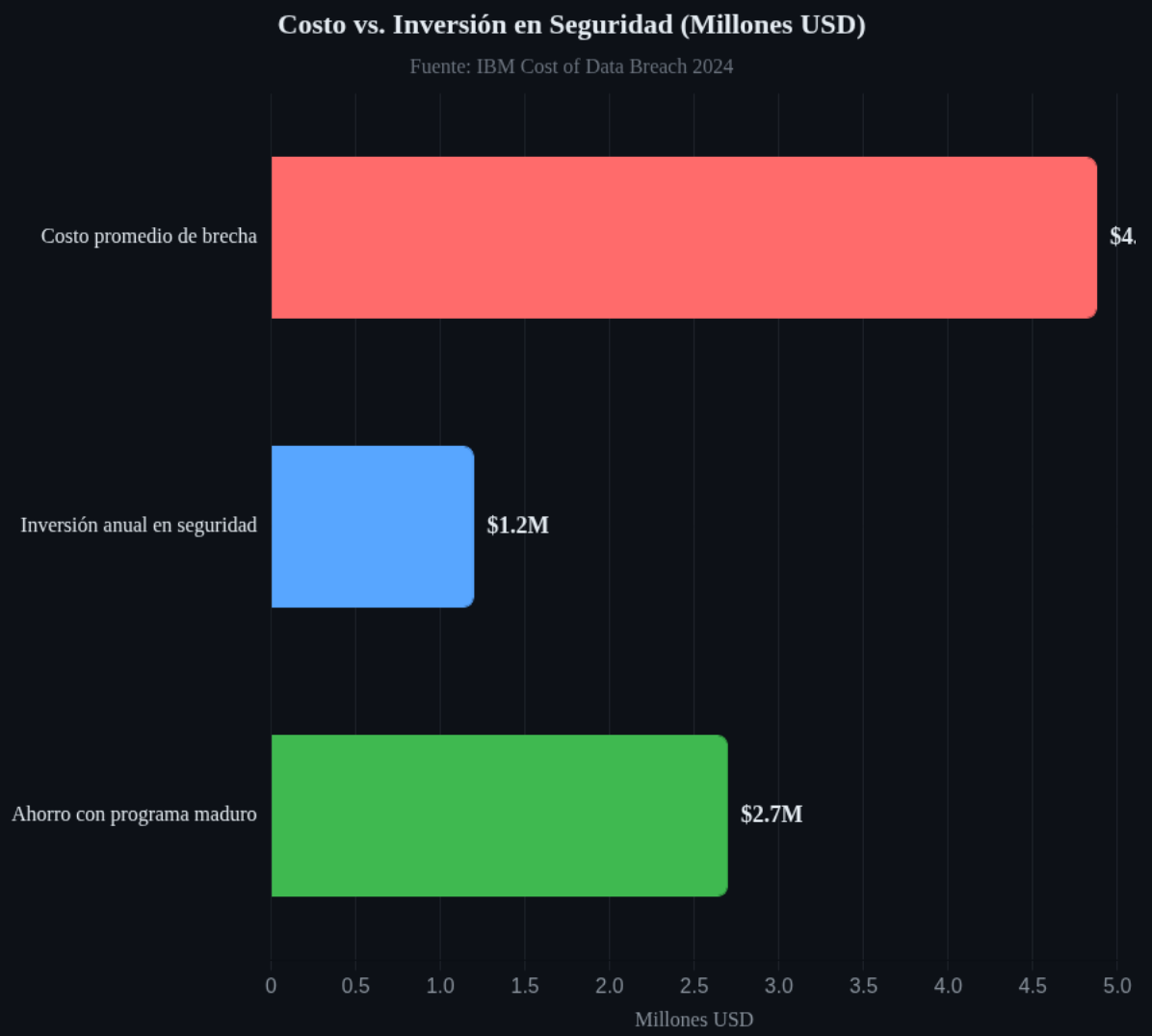
Clientes y socios prefieren organizaciones certificadas y seguras

Continuidad del Negocio

Menor impacto de incidentes gracias a planes de respuesta

Cumplimiento Regulatorio

Evitar multas y sanciones legales por incumplimiento



Tu Rol es Fundamental

Buenas prácticas que marcan la diferencia

Contraseñas fuertes y únicas

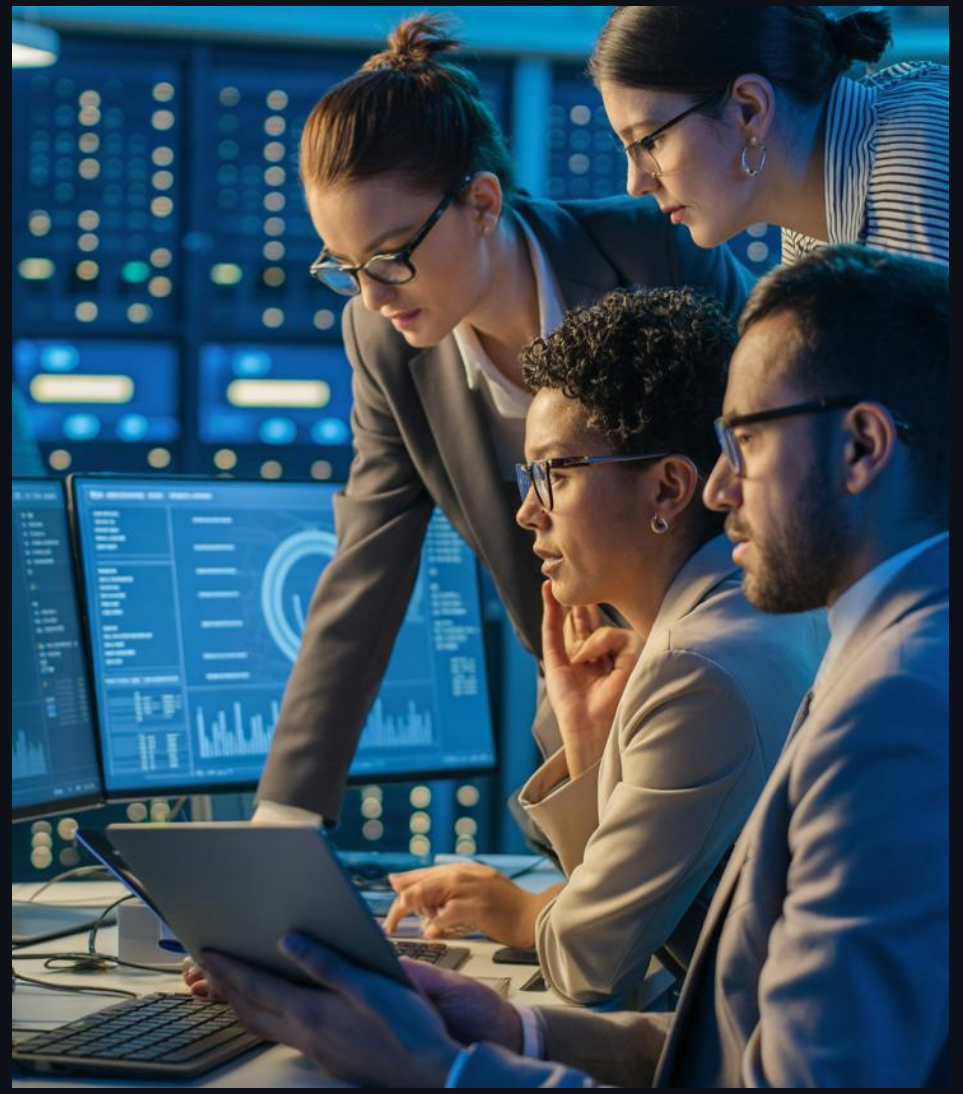
Activar autenticación 2FA

Reportar correos sospechosos

Evitar redes Wi-Fi públicas

Hacer copias de seguridad

Mantener software actualizado



Errores Comunes que Nos Ponen en Riesgo

¿Los reconoces en tu día a día?

❌ El Error	✓ La Solución
Usar la misma contraseña en todo	Usar un gestor de contraseñas
Hacer clic en enlaces sin verificar	Verificar remitente y URL antes de hacer clic
Compartir credenciales con compañeros	Cada usuario tiene sus propias credenciales

Actividad: ¿Qué harías tú?

Analiza cada escenario y elige la mejor respuesta

01

Recibes un correo del 'CEO' pidiendo transferir fondos urgentemente desde una dirección desconocida.

¿Qué haces?

02

Estás en un café y necesitas acceder al sistema de la empresa. Hay Wi-Fi gratuito disponible.

¿Qué haces?

03

Encuentras una USB en el estacionamiento de la empresa. La quieres revisar para saber de quién es.

¿Qué haces?

04

Una persona llama diciendo ser de soporte técnico y pide tu contraseña para 'arreglar un problema'.

¿Qué haces?

Discutamos en grupo las respuestas — ¡No hay respuestas incorrectas al participar!

Mi Compromiso de Seguridad

Acciones que puedo tomar hoy mismo

1. Cambiar y fortalecer mis contraseñas esta semana
2. Activar doble factor en mis cuentas críticas
3. Verificar remitente antes de hacer clic en cualquier enlace
4. Reportar cualquier actividad sospechosa al área de TI

Yo protejo la información

de mi organización

#SeguridadEsDeTodos

La seguridad comienza contigo

"El eslabón más fuerte en la cadena de seguridad es una persona bien informada."

Actúa hoy

- Comparte lo aprendido con tu equipo
- Aplica las buenas prácticas desde mañana
- Reporta incidentes, no los ignores

#JuntosSomosSeguridad

Taller de Sensibilización de Seguridad de la Información · 2025