



Integración de Seguridad Informática en  
Redes y Sistemas de Software  
TC2007B

**M2: Seguridad en aplicaciones y redes**

Profesor de Cátedra:

Osvaldo Cecilia Martínez

[osvaldo.cecilia@tec.mx](mailto:osvaldo.cecilia@tec.mx)

# Semana 1.1

1. Presentación
  - a. Profesor
  - b. Estudiantes
2. Revisión de políticas
3. Evaluación

## 2.1. Introducción a la seguridad

- I. Objetivos del módulo
- II. Referencias
- III. Importancia de la ciberseguridad
- IV. Activos
- V. Triada de la seguridad (CIA)
- VI. Conceptos básicos
- VII. Marcos de referencia



# Profesor



**Contacto:** [osvaldo.cecilia@tec.mx](mailto:osvaldo.cecilia@tec.mx)

## Osvaldo Cecilia Martínez

- Ingeniero en Computación
- Maestro en Ciberseguridad
- Concentración en Ciberseguridad CSF

## Asesorías individuales y grupales:

- Viernes de 9:00 a 11:00 horas
- Previa cita y confirmación



# Estudiantes

1. Nombre completo
2. Acercamiento con la ciberseguridad
3. Expectativas laborales
4. Intereses y pasatiempos
5. Juramento



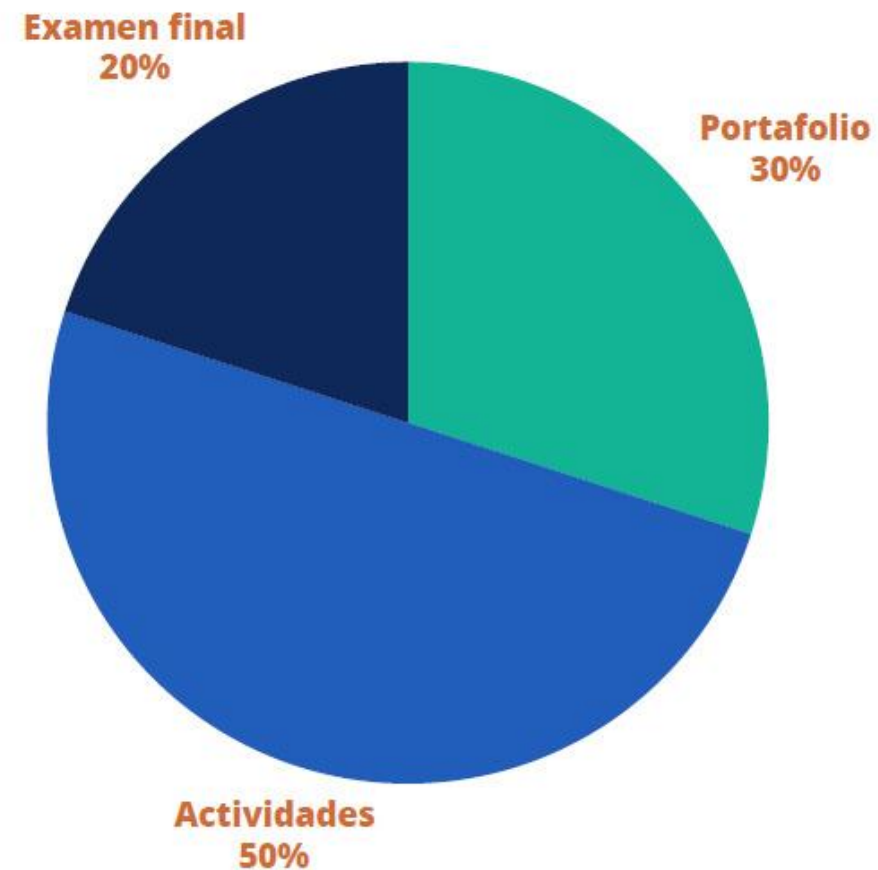
# Revisión de políticas

1. Horario del módulo 2 (M2)
2. Tolerancia en el inicio de clases
3. Distracciones
4. Periodos de descanso
5. Participación en clase
6. Re-entregas para el M2
7. Entregas a destiempo (30%, 60%, 90%)
8. Uso de IA para el M2
9. Consulta todas las políticas en Canvas



# Evaluación

1. Actividades
2. Evaluación final (escrita)



# Módulo 2: Seguridad en Aplicaciones y redes



# Objetivo M2

Explorar los principios fundamentales de la seguridad, procesos, tecnología, mejores prácticas y marcos de referencia para implementarlos a lo largo del ciclo de desarrollo y despliegue de software.





# Referencias sugeridas

1. Security in computing / Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies ([Disponible en biblioteca digital](#))
2. [CyBOK](#)
3. Applied Cryptography / Bruce Schneier
4. [ENISA Technical Trainings](#)
5. CCNA Cyber Ops SECFND #210-250 Official Cert Guide / Certification Guide 2017



## 2.1 Introducción a la seguridad



# Reflexión:

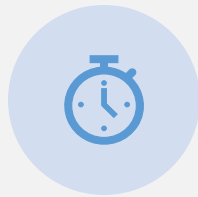
## ¿Por qué es importante la ciberseguridad?



# Importancia de la ciberseguridad



El costo global de la ciberdelincuencia aumentará a \$23.84 billones USD para 2027, contra a \$0.86 billones USD en 2018 (Statista)



A los equipos de seguridad les toma un promedio de 277 días identificar y contener una violación de datos en 2023 (IBM)



En 2023, el 66% de las organizaciones informaron haber sido blanco de ransomware (SC Media)



El phishing se identificó como el principal vector de infección en el 41 % de los incidentes de ciberseguridad en 2023 (IBM Security X-Force)



El 85 % de los profesionales de la ciberseguridad atribuye el aumento de los ciberataques a los actores maliciosos que utilizan IA generativa (CFO).

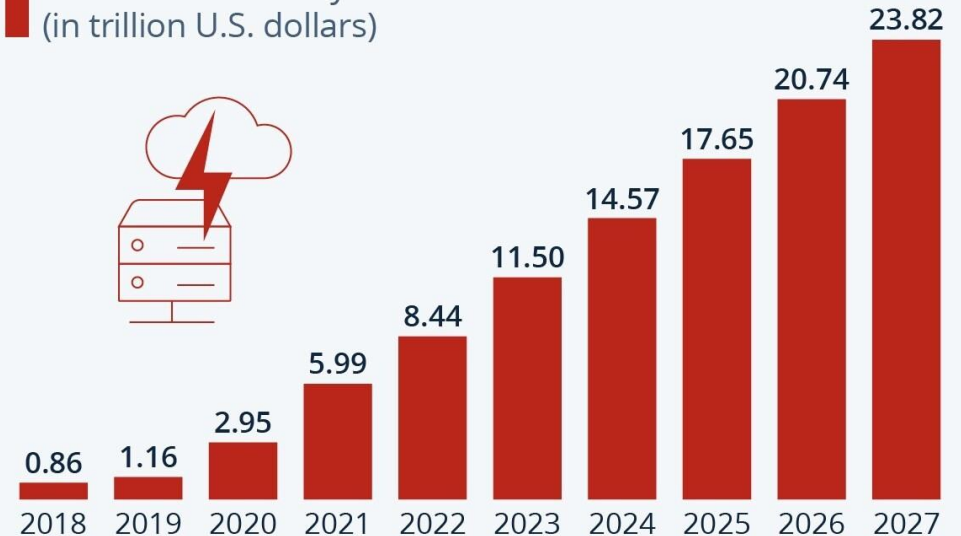


# Importancia de la ciberseguridad

1. Crecimiento de las amenazas
2. Impacto económico y reputacional
3. Necesidad de una estrategia de ciberseguridad robusta

## Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide  
(in trillion U.S. dollars)



As of November 2022. Data shown is using current exchange rates.

Sources: Statista Technology Market Outlook,  
National Cyber Security Organizations, FBI, IMF



statista



# Situación de la Ciberseguridad en México

Código Penal Federal > Título 9º > Capítulo II “Acceso ilícito a sistemas y equipos de informática” > Art. 211 bis (1-7)

LFPDPPP

INAI

Guardia Nacional > CERT-MX

Organismos estatales. Ejemplo: “Policía Cibernética” de la SSC de la CDMX



# Situación de la Ciberseguridad en México

“En 2023, el sector financiero en México sufrió el 60% de los ataques cibernéticos, siendo phishing y ransomware los vectores más comunes.”

- Deloitte México



# Activos de TI (IT Assets)

Cualquier elemento de tecnología de la información utilizado para agregar valor a la organización. Por ejemplo: Hardware, Software, información,...

## Tangibles:

- Servidores
- Ruteadores
- NAS
- Dispositivos IoT

## Intangibles:

- Sistemas Operativos
- Aplicaciones
- Datos financieros de clientes
- Reputación





# CIA

## Pilares de la seguridad



**Confidencialidad:** no autorización/autorización de accesos



**Integridad:** precisión y confiabilidad, cambios autorizados



**Disponibilidad:** acceso autorizado cuando se necesite



# ¿De qué pilar (CIA) se está afectando?


1. Un empleado descarga datos sensibles de clientes sin autorización
2. Un dispositivo de almacenamiento USB es robado y contiene datos sin cifrar
3. Un ataque de ransomware encripta los archivos de una empresa, bloqueando el acceso
4. Un programador cambia el código de una aplicación para introducir una puerta trasera
5. Un incendio en el centro de datos destruye servidores críticos sin respaldo
6. Acceder al campus sin credencial



# Seguridad: Un Enfoque Holístico

“La ciberseguridad efectiva requiere una combinación de tecnología avanzada, procesos robustos y un personal debidamente capacitado.”

- SANS Institute

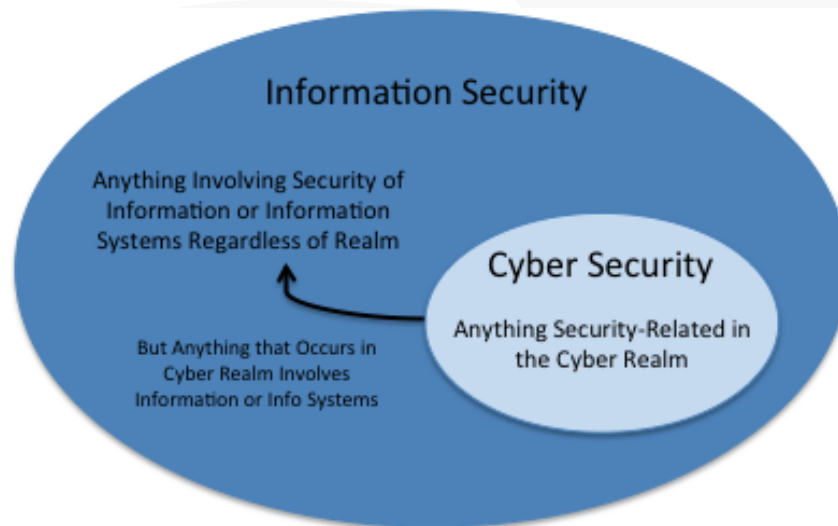
- 
1. Personas
  2. Procesos
  3. Tecnología

Protección de  
la CIA



# Seguridad de la Información vs. Ciberseguridad

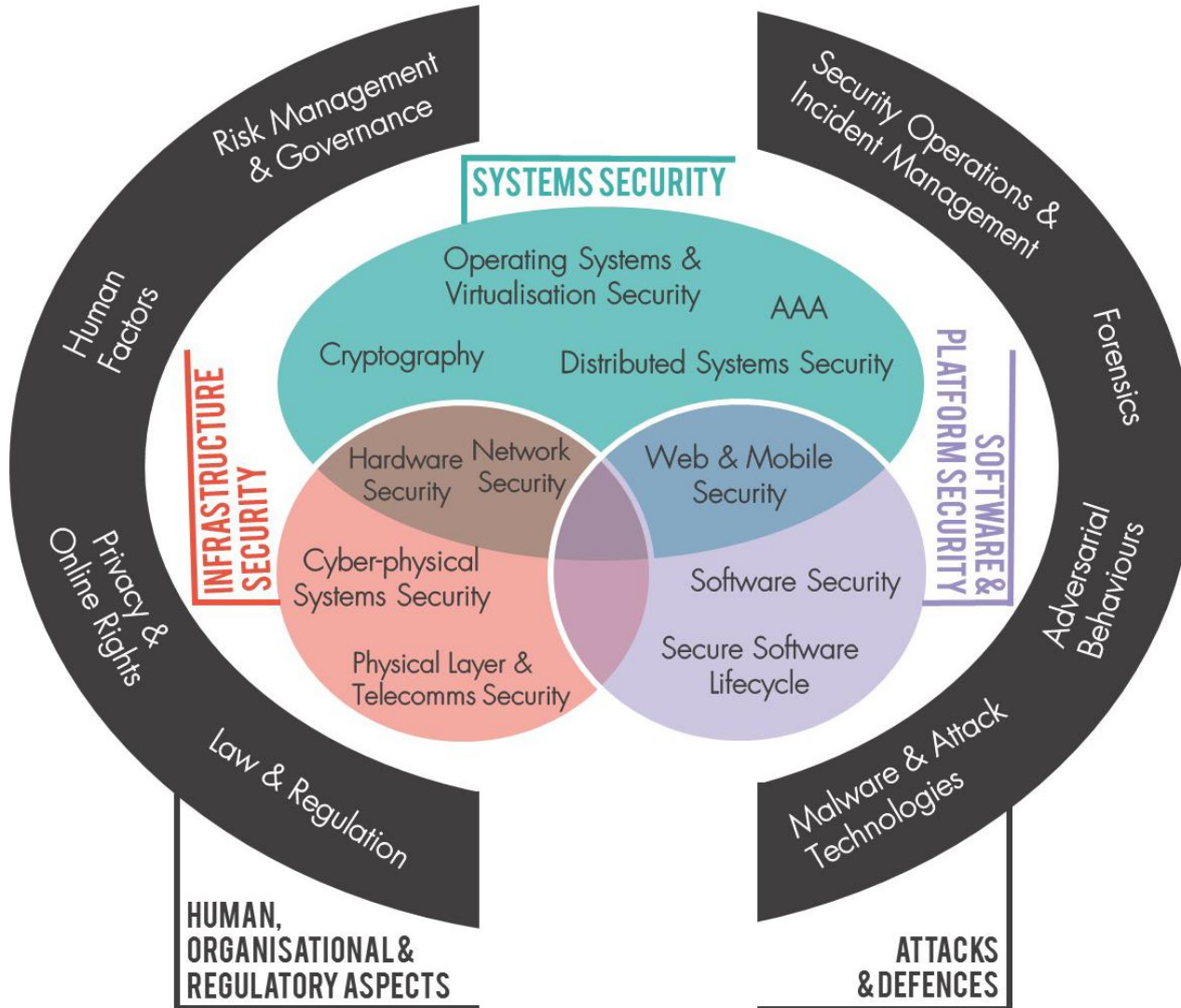
“La ciberseguridad es una subdisciplina de la seguridad de la información, enfocada en proteger los sistemas y redes digitales.” - ISACA



Protección de la información en cualquier formato. Ej. Digital o física

Protección del ámbito cibernético. Ej. Internet



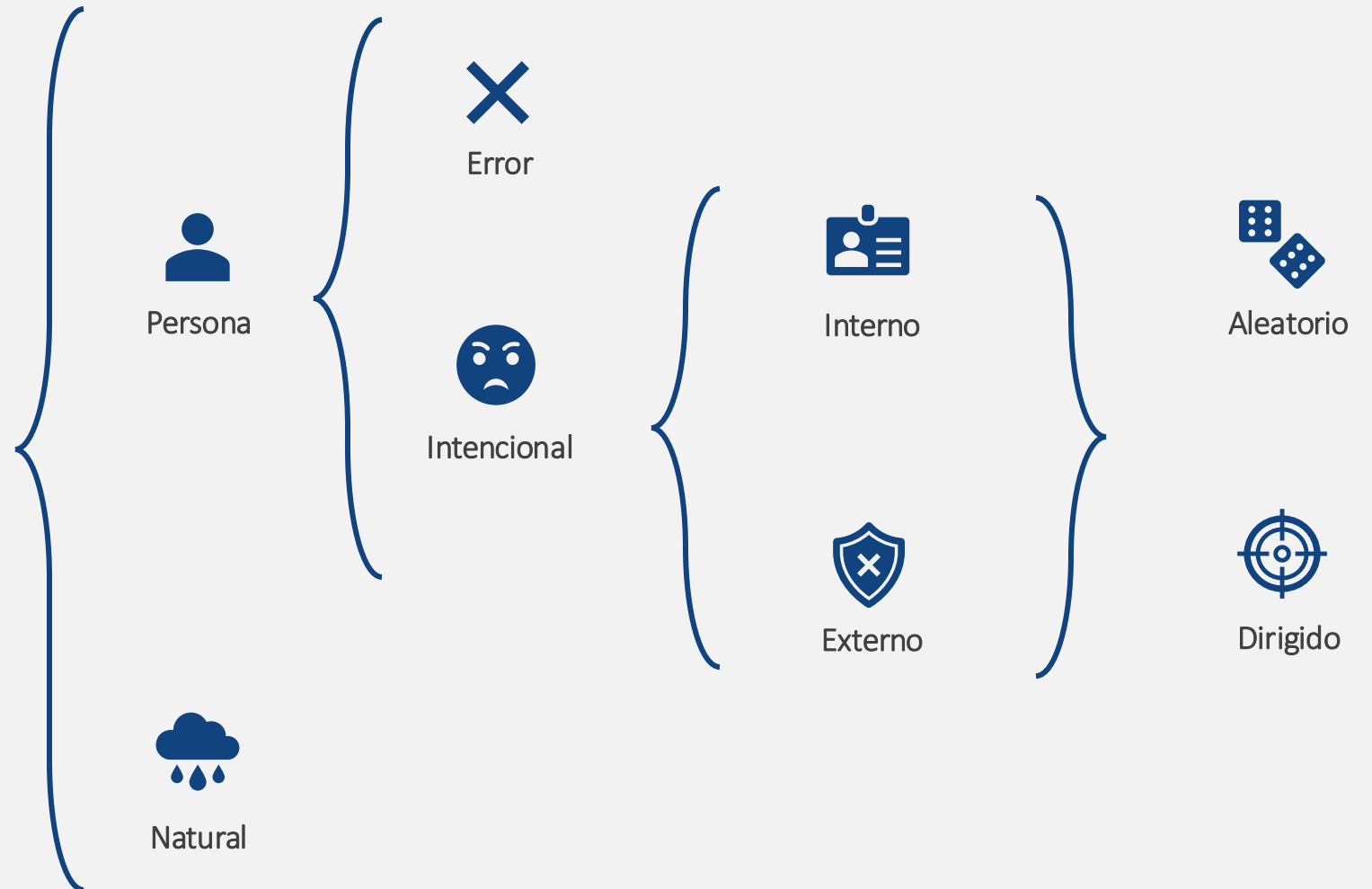


# Áreas en Seguridad



# Actores de amenaza

Los actores de amenaza son entidades que pueden comprometer la seguridad de una organización



# Vulnerabilidades

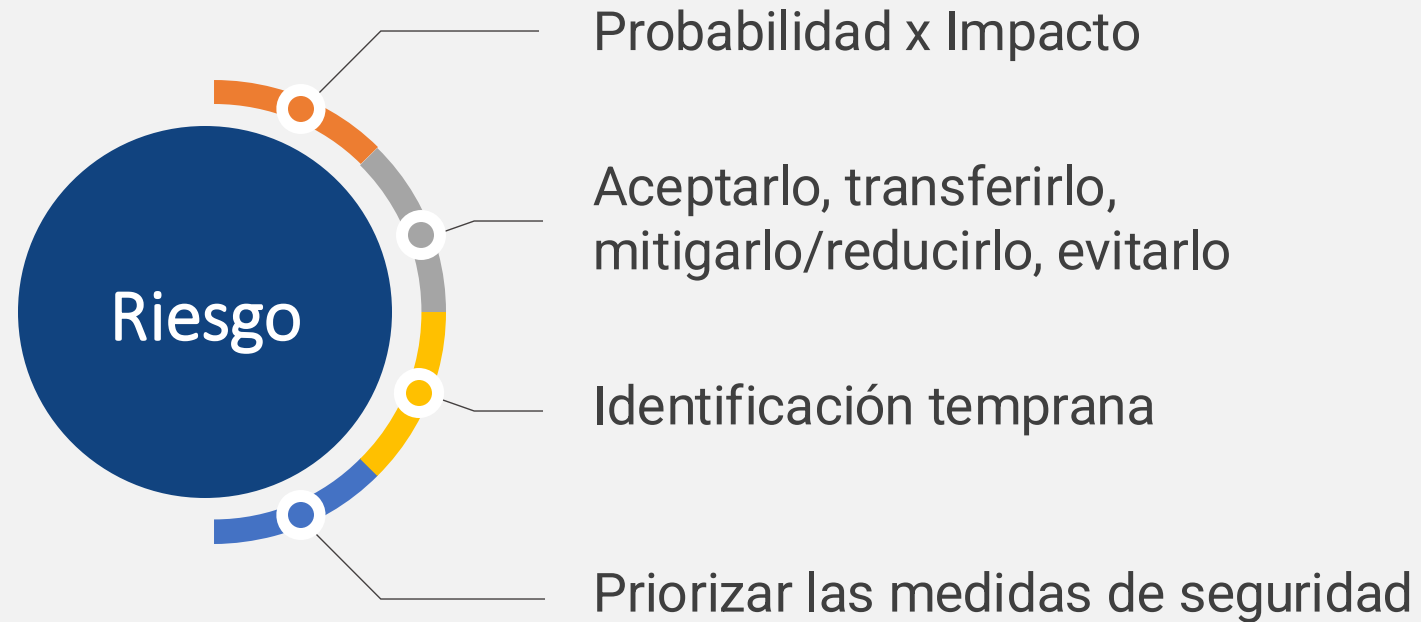
“Las vulnerabilidades son debilidades que pueden ser explotadas por actores de amenaza para comprometer un sistema o información.” - OWASP

Ejemplos de vulnerabilidades:

- Errores en el código (inicialización de variables)
- Sistema operativo desactualizado
- Configuración incorrecta en firewall (por default)
- Contraseña débil



# Riesgos





# Controles

Acción, dispositivo, política,  
proceso, aparato o técnica  
que ayuda a reducir el riesgo,  
ya sea la probabilidad o el  
impacto.



Detección: IDS



Prevención: firewall



Mitigación: parches  
de seguridad



Recuperación:  
backup



Disuasión:  
cumplimiento  
normativo



Transferencia:  
seguros financieros



# ¿Qué tipo de control es?

Detección	1. Outsourcing de Seguridad	2. Segmentación de red	3. NACL
Prevención			
Mitigación	4. SIEM	5. Política de contraseñas seguras	6. IPS
Recuperación			
Disuasión			
Transferencia	7. DRP	8. Logs de un sistema	9. Corrección de configuración





## Modelo de Defensa en Profundidad



# Marcos de Referencia

- NIST (gestión de riesgos)
- ISO/IEC 27001 (seguridad de la información)
- CIS Controls (controles técnicos)

Sector específico:

- PCI-DSS (financiero)
- HIPAA (salud)



# ¿Tienes alguna duda?

