

Especialización en Seguridad de la información y ciberseguridad



7 meses de clases Online



La ciberseguridad no sólo es implementar tecnología, por ello te mostraremos las **metodologías, procesos y formas** de cuidar tu información, no importa el sector, el tamaño de la organización o presupuesto, aprenderás desde el análisis de riesgos hasta la implementación de controles para prevenir, reaccionar y recuperarte de incidentes bajo el marco de referencia **NIST, ISO 27001 - 27005, 27032, PCI** en 7 meses de cursos.



Educamos - Integramos - Innovamos

cursos@iciberseguridad.io
www.iciberseguridad.io
+52 812-587-2530

7 DE MAYO -
26 DE NOVIEMBRE
30 SESIONES

OBJETIVO:

Poder conocer las normativas y estándares aplicables en materia de seguridad de la información y ciberseguridad, así como los procedimientos, metodologías, controles y documentación aplicable para su implementación.

Al finalizar el curso el participante podrá:

- Conocer e identificar los componentes para la implementación de un Sistema de gestión de seguridad de la información.
- Conocer el proceso de implementación de un sistema de gestión de seguridad de información.
- Conocer la normativa ISO 27001 y la forma en la que ayuda a la protección de la información.
- Conocer las metodologías y herramientas que nos permitirán protegernos ante este tipo de amenazas e incidentes de seguridad.
- Generar las estrategias de seguridad a implementar en la organización, así como los planes de prevención y respuesta a incidentes.
- Realizar un análisis de riesgos
- Identificar vulnerabilidades en procesos organizacionales
- Conocer e identificar las amenazas organizacionales
- Conocer cómo corregir los fallos en la organización
- Proponer contramedidas o soluciones de seguridad con base en las mejores prácticas de seguridad.
- Conocer y prevenir cualquier tipo de ataque a través del marco Mitre ATT&CK
- Conocer las metodologías y herramientas que nos permitirán protegernos ante este tipo de amenazas e incidentes de seguridad.

DIRIGIDO A:

- Personal directivo de TI.
- Administradores de sistemas.
- Administradores de redes.
- Personal de soporte técnico.
- Cualquier persona interesada en conocer el mayor peligro en la actualidad para nuestra información.

Duración del curso: 7 meses**Inicio:** 7 de mayo 2022**Finalización:** 26 de noviembre**Horario:** 9:00 – 13:00 (UTC-6)

Costo: \$6500 pesos mexicanos (320 DLS). 7 pagos mensuales de 980 pesos mexicanos o 53 dólares mensuales hasta completar el costo total de la especialidad.

Mayores informes e inscripciones.**whatsapp:** <https://wa.me/message/XLMOBC7ABUGAA1>**Correo electrónico:** cursos@iciberseguridad.io

CONTENIDO TEMÁTICO:**Módulo 1: Generalidades de la seguridad de la información**

- Seguridad de la información vs ciberseguridad
- Perspectivas de la seguridad
- Tipos de seguridad
- Objetivos de la seguridad
- ¿Qué protegemos?
- ¿Cómo lo protegemos?
- Triada CID
- Composición de la seguridad
- Personas, procesos y tecnología
- Definiendo los requerimientos de seguridad
- Marcos de referencia
- ¿Cómo seleccionamos un marco de referencia?
- ¿Cómo se implementa la seguridad?

Módulo 2 – Seguridad de la información

- Comprendiendo la familia ISO 27000
- Conociendo la Norma ISO 27001
- Conociendo la Norma ISO 27002
- Normativas aplicables
- Contexto de la organización
- Alcance del SGSI
- Liderazgo de seguridad
- Políticas de seguridad
- Planificación de la seguridad
- Documentación mandataria
- Conociendo los controles de seguridad (Anexo A)
- Normas de implementación de controles

Módulo 3 – Entorno general en Ciberseguridad

- Ciberseguridad vs seguridad de la información
- Seguridad en el ciberespacio
- Composición de la ciberseguridad
- Cómo se implementa la seguridad
- Consideraciones para implementar ciberseguridad
- Qué protegemos
- Conociendo los controles de seguridad
- Principios de la seguridad
- Seguridad en Capas
- Contexto general de la ciberseguridad
- Ataques informáticos
- Consecuencias de los ataques
- Amenazas informáticas
- Identificando la superficie de ataque

Módulo 4: Implementar seguridad

- Seguridad con base en regulación
- Beneficios y apoyo de alta dirección
- Establecimiento de objetivos en la seguridad
- Uso de marcos de referencia
- Gestión de la implementación
- Gestión de riesgos
- Implementación de mecanismos de protección
- Capacitación y concienciación

Módulo 5 – Mecanismos técnicos de seguridad - laboratorios

- Seguridad en aplicaciones
- Seguridad en estaciones de trabajo
- Seguridad en correo electrónico
- Seguridad de infraestructura
- Seguridad de los datos e información
- Seguridad de identidades

Módulo 6: Gestión de riesgos y vulnerabilidades

- Contexto general del análisis de riesgos
- Introducción al análisis de riesgos y vulnerabilidades
- Flujo de la gestión de riesgos
- Definición de un proyecto de gestión de riesgos
- Inventariado de activos
- Definición de Amenazas
- Análisis de riesgos
- Tipos de Vulnerabilidades
- Identificación de impacto de negocio
- Plan de implementación de contramedidas

Módulo 7.- Gestión de riesgos - Laboratorio

- Identificación de vulnerabilidades
- Definición de amenazas e impacto de negocio
- Planteamiento de soluciones o contramedidas
- Justificación de contramedidas
- Aplicación de contramedidas

Material Entregable y adicionales

- Cuenta de Office 365
- Material grabado
- 10 horas de consultoría en caso de implementación de seguridad en la organización.
- Entrega de recursos complementarios al taller (Formatos y contenido de estudio)
- Entrega de constancia DC3 (Sólo México) + Diploma por cada curso
- Posibilidad de realizar prácticas profesionales en seguridad.