

# TALLER DE CIBERSEGURIDAD PARA LÍDERES EMPRESARIALES

**Coordinador:**  
**Mtro. Radamés Hernández Alemán**

## Objetivo:

Brindar al alumno de los principales conceptos y prácticas de ciberseguridad para liderar las acciones y procesos que permitan mitigar eficazmente los riesgos cibernéticos de su organización.

## Beneficios:

El alumno se familiarizará con los principales conceptos, metodologías, normativas y prácticas nacionales e internacionales para participar en el desarrollo y valoración de las estrategias de gestión y respuesta a riesgos y amenazas cibernéticas.

## Perfil de Ingreso:

- Coordinadores, Gerentes y Directores de empresas públicas y privadas interesados en participar y desarrollar en planes estratégicos de prevención y gestión de riesgos y amenazas cibernéticas.
- Todo aquel profesional interesado en actualizar sus conocimientos en materia de ciberseguridad.

## Perfil de Egreso:

- Al concluir este programa académico el alumno sabrá cómo identificar, evaluar y priorizar los riesgos de ciberseguridad en su organización.
- Tendrá las herramientas necesarias para definir políticas y procedimientos que guíen las actividades de seguridad, así como garantizar el cumplimiento de las leyes y normativas nacionales e internacionales.
- Podrá desarrollar un plan de comunicación interno sobre la importancia de la cultura de la ciberseguridad en su organización.

## Módulo 1: presentación e introducción al taller

- Introducción a las TIC.
- Perspectiva global.
- Marco conceptual.
- Estudio sobre los hábitos de internet en México.
- Tecnologías emergentes, innovación tecnológica y sus riesgos.

Práctica 1. Buenas prácticas para equipos de cómputo.

## Módulo 2: modalidades de ataques y delitos cibernéticos

- Aspectos de la Legislación internacional y nacional.
- Marcos de referencia y estándares.
- Delitos cibernéticos más comunes.
- Aspectos de la penalización de los delitos cibernéticos en México.

Práctica 2. Buenas prácticas para dispositivos móviles.

## Módulo 3: riesgos a la información digital

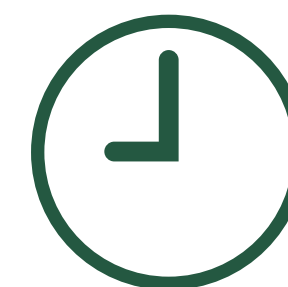
- Principales tipos de ciberataques:
- Malware
- Phishing
- Man-in-the-middle attack (MitM)
- Distributed denial-of-service attack (DDoS)
- SQL injection
- Zero-day attack

Práctica 3. Buenas prácticas para evitar ataques de ingeniería social.

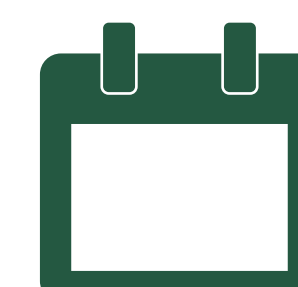
## Módulo 4: ciberseguridad para la empresa

- Seguridad de sistemas y la WEB
- Empleados
- Seguridad en la Red
- Estafa y fraude
- Privacidad y seguridad de los datos
- Correo electrónico
- Seguridad física

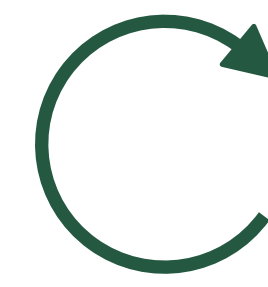
Práctica 4. Ejercicio de evaluación de riesgos.



Horario  
**Sábado** 09:00 h - 13:00 h



Inicio:  
**Sábado 01**  
julio 2023



Duración  
**16 horas**



Modalidad  
**100% online**