UVM | EDUCACIÓN CONTINUA

LAUREATE INTERNATIONAL UNIVERSITIES

DIPLOMADO

CIBERSEGURIDAD Y CIBERDEFENSA

DIPLOMADO

PRESENCIAL 128 HORAS

CIBERSEGURIDAD Y CIBERDEFENSA

OBJETIVO

Profundizar sobre los principales elementos de identificación, protección, detección, respuesta y recuperación ante una amenaza en ciberseguridad y alinear los recursos que ofrecen las tecnologías de la información con los objetivos de negocio o institucionales. Dirigir desde una visión integral la gestión de los procesos asociados a seguridad de la información en entornos empresariales y administrativos, sabiendo identificar las claves de éxito en los proyectos, y contribuyendo desde la Dirección de Seguridad de la Información a la estrategia empresarial.

Conocer cómo optimizar los flujos de gestión operativa a partir de la consideración, selección y puesta en marcha de procesos informatizados y de recolección de información que puede ayudar a conocer el desempeño en ciberseguridad.

Conocer cómo proteger los datos sensibles frente a las amenazas que pueden materializarse por parte de nuestros adversarios. Tener conocimiento de las principales herramientas, metodologías y servicios más adecuados para la gestión de proyectos de seguridad de la información.

Entender y tener una visión holística de tendencias en el sector de seguridad de la información, así como su aplicabilidad pragmática en los procesos de negocio y actividades comerciales.

CONOCE MÁS

UVM LAUREATE INTERNATIONAL UNIVERSITIES | EDUCACIÓN CONTINUA

BENEFICIOS

- Dar visión para generar las capacidades y la infraestructura tecnológica para prevenir delitos cibernéticos. Dar visión para el diseño de protocolos de operación para la prevención de delitos cibernéticos. Apoyar en la generación de defensas en el entorno digital con un enfoque de gestión de riesgos. Apoyar en el fortalecimiento y esquema de identificación, prevención y gestión de incidentes digitales.

- Generar una estrategia de protección y defensa de la infraestructura crítica cibernética. Dar visión para apoyar a salvaguardar la seguridad y privacidad digital. Apoyar en la visión y Detección de los puntos ciegos en temas de seguridad en las personas, procesos y tecnología. Concientizar a los participantes en el valor de la seguridad. Dar visión en la detección de riesgos y amenazas actuales dentro sus organizaciones y en nivel personal Generar una visión de cómo fortalecer las diversas capas de seguridad dentro de la organización.

- Apoyar en la concientización para generar controles que permitan la detección de riesgos y amenazas. Apoyar en la identificación de acciones preventivas más que reactivas ante riesgos y amenazas. Dar visión sobre la generación de controles de seguridad de acuerdo con normas y estándares internacionales. Dar visión para la detección de manera continua ante cualquier riesgo y/o amenaza dentro de la organización.

A QUIEN VA DIRIGIDO

A profesionales en tecnologías de la información que sean responsables sobre los aspectos de seguridad de la información.

CONOCE MÁS

Módulo 1

El Ecosistema de la Ciberseguridad

1. Introducción.
2. Conociendo en ecosistema de la ciberseguridad.

Módulo 2

Ciberseguridad Operativa

1. El proceder de un hacker.
2. Contraseñas
3. Criptología
4. Aplicaciones criptográficas.
5. Control de acceso.
6. Técnicas generales de ataques.
7. Vulnerabilidades en la web.
8. Vulnerabilidades en la programación.
9. Seguridad en las transacciones electrónicas.
10. Ethical Hacking.

Certificación a Obtener: EXIN Cyber & IT Security Foundation

Módulo 3

Ciberseguridad Táctica

1. Gobernanza y Administración de Riesgos.

CONOCE MÁS

UVM LAUREATE INTERNATIONAL UNIVERSITIES | EDUCACIÓN CONTINUA

Módulo 4

Ciberseguridad Estratégica

1. Entorno Global y Marco Normativo de la Ciberseguridad.
2. Gobierno de Seguridad de la Información.

Certificación a Obtener: EXIN Fundamentos de Seguridad de la Información basado en ISO IEC 27001

Módulo 5

Ciberinteligencia

1. Fundamentos.
2. Inteligencia de Fuentes Abiertas.
3. Metadatos.
4. Deep Web.

Módulo 6

Ciberseguridad en Entornos Cloud, Internet de las Cosas y ntornos Industriales

1. Seguridad en Entornos Cloud.
2. Seguridad en Internet de las Cosas.
3. Seguridad en Entornos Industriales.
4. Advanced Persistent Security.
5. Análisis Forense en Cloud y Aplicaciones Móviles.

Certificación a Obtener: EXIN Cloud Computing Foundation

CONOCE MÁS

UVM LAUREATE INTERNATIONAL UNIVERSITIES | EDUCACIÓN CONTINUA

Módulo 7

Computación Forense

1. Etapas de un análisis forense.
2. Adquisición de evidencias digitales.
3. Preservación de la integridad e identidad de las evidencias.
4. Cadena de custodia de las evidencias.
5. Análisis de las evidencias.
6. Laboratorio de análisis forense.

Módulo 8

Ciberdefensa

1. Ciberpatrullaje.
2. Estrategias de Ciberdefensas.
3. Ciberdefensa Personal.
4. Ciberdefensa Organizacional.

Módulo 9

Proyecto: Diseño de un Programa De Ciberseguridad

1. Diseño del Programa.
2. Modelización de Amenazas.
3. Respuesta a Incidentes.
4. Reacción inmediata en Ciberseguridad.
5. Funciones y responsabilidades del CISO.
6. Casos de Negocio en Ciberseguridad.

CONOCE MÁS

UVM LAUREATE INTERNATIONAL UNIVERSITIES | EDUCACIÓN CONTINUA

UVM | EDUCACIÓN CONTINUA

LAUREATE INTERNATIONAL UNIVERSITIES®

universidaduvm.mx