DIPLOMA SUPERIOR DE POSTGRADO UNIVERSITARIO EN CIBERSEGURIDAD (NIVEL I)

"Un enfoque integral en el ciclo de vida de la seguridad de la información".

UNIVERSIDAD EUROPEA IMF
INSTITUTO UNIVERSITARIO LAURENTIA

OBJETIVOS DEL CURSO

1. Comprender los fundamentos de la ciberseguridad, incluyendo los conceptos clave, los riesgos y las amenazas a la seguridad de la información.

2. Conocer las mejores prácticas y marcos de trabajo para el ciclo de vida de la ciberseguridad, como ISO/IEC 27001, NIST, COBIT, entre otros.

3. Identificar los procesos clave para la gestión de la ciberseguridad en cada etapa del ciclo de vida de la información y los sistemas informáticos, incluyendo la planificación, la implementación, la evaluación y el mantenimiento.

4. Aprender a evaluar y mitigar los riesgos de seguridad de la información en todas las etapas del ciclo de vida, utilizando técnicas y herramientas adecuadas.

5. Conocer las técnicas y herramientas para la detección, respuesta y recuperación de incidentes de seguridad en todas las etapas del ciclo de vida de la información y los sistemas informáticos.

6. Desarrollar habilidades para la gestión efectiva de la seguridad de la información en organizaciones de diferentes tamaños y sectores, incluyendo la identificación y gestión de recursos para la ciberseguridad.

7. Desarrollar habilidades de comunicación y liderazgo para trabajar con equipos multidisciplinarios en la implementación y gestión de programas de ciberseguridad en organizaciones.

8. Obtener una comprensión de la regulación y normativa relacionada con la ciberseguridad, así como la ética y la privacidad en la gestión de la seguridad de la información.

PORQUE FORMARSE EN CIBERSEGURIDAD

Es un tema de gran relevancia en la actualidad:

Con el auge de la tecnología y la transformación digital, la ciberseguridad se ha vuelto cada vez más importante en las organizaciones y empresas de todo el mundo. Un postgrado en este campo puede preparar a los estudiantes para enfrentar los desafíos y riesgos de seguridad cibernética en el mundo actual.

Aumenta las oportunidades de empleo o de ascenso:

Con la creciente necesidad de seguridad cibernética en las organizaciones, se ha creado una gran demanda de profesionales capacitados en este campo. Un postgrado en el ciclo de vida de la ciberseguridad puede abrir muchas puertas en el mercado laboral y aumentar las oportunidades de empleo para los graduados.

Permite profundizar en el tema:

Un postgrado en el ciclo de vida de la ciberseguridad no solo proporciona una comprensión básica de los conceptos y técnicas, sino que también permite a los estudiantes profundizar en áreas específicas del campo y desarrollar habilidades especializadas.

Contribuye a la seguridad de la información:

La seguridad de la información es un problema crítico que enfrentan las organizaciones de todos los tamaños y sectores. Un postgrado en ciberseguridad puede ayudar a los estudiantes a comprender los riesgos de seguridad de la información y cómo mitigarlos, lo que puede mejorar la seguridad y protección de los datos y la información.

METODOLOGÍA DE ENSEÑANZA

Aprendizaje basado en problemas:

El aprendizaje basado en problemas es un método de enseñanza en el que se utilizan problemas complejos del mundo real como vehículo para promover el aprendizaje de conceptos y principios por parte de los estudiantes, en contraposición a la presentación directa de hechos y conceptos, esto les permite aplicar los conceptos teóricos y desarrollar habilidades prácticas.

Clases magistrales:

Aunque el aprendizaje basado en problemas es una herramienta muy efectiva, también es importante que los estudiantes reciban una base teórica sólida. Las clases magistrales se utilizan para presentar los conceptos clave, los marcos de trabajo y las mejores prácticas del ciclo de vida de la ciberseguridad.

Trabajo en equipo:

La ciberseguridad es un tema complejo que requiere de habilidades multidisciplinarias. Por lo tanto, es importante fomentar el trabajo en equipo para que los estudiantes puedan desarrollar habilidades de colaboración y comunicación. Durante el curso se asignan proyectos que pueden realizarse en grupo y que involucran la identificación y gestión de riesgos de seguridad de la información en diferentes etapas del ciclo de vida.

Estudios de caso:

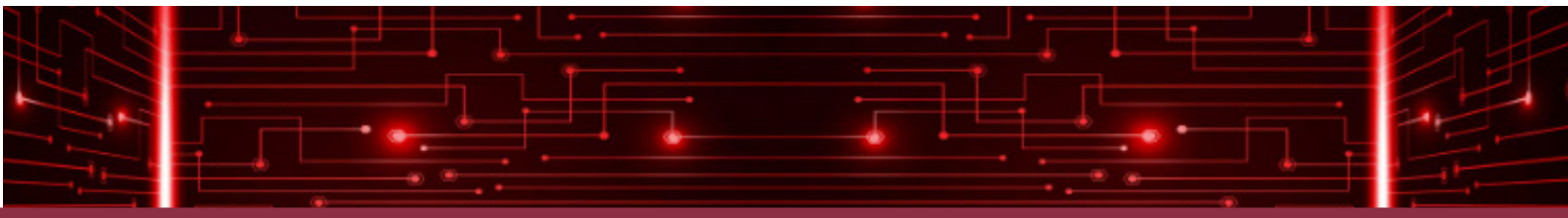
Los estudios de caso son una herramienta valiosa para que los estudiantes puedan analizar situaciones reales y aprender de la experiencia de otros. Durante el curso se analizan casos de ciberataques exitosos y se trabaja sobre los mismos para identificar las vulnerabilidades y los errores que permitieron ese ataque.

Laboratorios y ejercicios:

La ciberseguridad es un tema muy técnico, por lo que es importante que los estudiantes tengan la oportunidad de trabajar con herramientas y tecnologías de ciberseguridad en un ambiente controlado. Los estudiantes utilizarán los laboratorios y ejercicios prácticos para desarrollar habilidades técnicas en el análisis de riesgos, la detección y respuesta a incidentes, y la implementación de medidas de seguridad.

Evaluación continua:

La evaluación continua es importante para asegurar que los estudiantes estén comprendiendo los conceptos y desarrollando las habilidades necesarias. Durante el curso se evaluará a los estudiantes mediante la asistencia a las sesiones, participación en proyectos y ejercicios prácticos, y para finalizar la realización de un trabajo de fin de postgrado.



CONTENIDO DEL CURSO

INTRODUCCIÓN

01

1. ¿Qué es la ciberseguridad?
2. Transformación digital.
3. Entornos (IT/OT/IOT/IIOT).
4. Tecnologías relevantes.
5. Riesgos y posibles impactos derivados de las nuevas tecnologías.
6. Conceptos básicos
7. Introducción de la gestión del riesgo de seguridad y ciclo de vida de la ciberseguridad.
8. Principales desafíos de la ciberseguridad.

GOBIERNO, LEGISLACIÓN Y POLÍTICAS

02

1. Funciones en una organización, modelos organizativos y modelos relacionales.
2. Desarrollo, documentación e implementación de políticas de seguridad, estándares, procedimientos y guías.
3. Leyes y categorías (GDPR o ley de ciberseguridad de estados unidos).
4. Cumplimiento.
5. Contratación y adquisición.

DIRECCIÓN, DISEÑO Y ESTRATEGIA

03

1. Plan director y “cyber-Security frameworks” (CSF).
2. Modelo operativo objetivo o “Target operating model” (TOM).
3. Plan de continuidad del negocio o “Business Continuity Plan” (BCP).
4. Análisis de impacto a la organización o “Business Impact Analysis” (BIA).

GESTIÓN DEL RIESGO

04

1. Programas de concienciación y educación de empleados y externos.
2. Metodologías de “Threat Modeling”.
3. Evaluación de riesgos (inventario de activos, identificación de amenazas y vulnerabilidades).
4. Selección de contramedidas e implementación de controles (prevención, detección y corrección).
5. Monitorización, informes, mejora continua y “Security Control Assessment (SCA)”.
6. Frameworks y programas para la gestión de riesgo.

SEGURIDAD EN LOS ACTIVOS

05

1. Ciclo de vida de la ciberseguridad.
2. Seguridad física.
3. Seguridad en redes y sus componentes.
4. Criptografía.
5. Desarrollo seguro.
6. Cloud
7. Dispositivos OT

EVALUACIÓN Y PRUEBAS DE SEGURIDAD

06

1. Introducción al hacking ético.
2. Ética y legalidad.
3. Footprinting & fingerprinting.
4. Seguridad en redes.
5. Vulnerabilidades.
6. Herramientas.
7. Ataques a credenciales.
8. Análisis de perfiles de navegación.

GESTIÓN DE VULNERABILIDADES

07

1. Sistemas tipo cliente/servidor.
2. Evaluación y mitigación de vulnerabilidades (database, webs, móviles).
3. Gestión según los entornos (IT/OT/IOT/IIOT).
4. Vulnerabilidades en “Industrial Control Systems” (ICS).

MONITORIZACIÓN Y GESTIÓN DE AMENAZAS

08

1. Logs y registros.
2. Ciclo de vida de los eventos.
3. Gestión de identidades (VPN, PAM, LDAP, etc.).
4. Control y monitorización de eventos (SOC, SIEM y NUC).
5. Detección y gestión de amenazas.

PREVENCIÓN Y RESPUESTA ANTE INCIDENTES

09

1. Tipos de incidentes.
2. Estrategias de recuperación.
3. Resiliencia y tolerancia a los fallos.
4. Planes de recuperación.
5. Formación, documentación y aprendizaje.
6. Prueba y mantenimiento de las metodologías.

ANALISIS FORENSE

10

1. Introducción a la ciencia forense.
2. Legislación y regulación.
3. Proceso de investigación.
4. Adquisición de evidencias.
5. Herramientas.
6. Discos y sistemas de ficheros.
7. Análisis de correos electrónicos.
8. Leyes aplicadas a la ciencia forense.

TRABAJO DE FINAL DE POSTGRADO

El trabajo de postgrado es de libre elección para los alumnos, sin embargo, se les facilitan las siguientes temáticas y una tutoría para decidirlo desde el inicio del curso.

1. **Análisis comparativo de los principales marcos de trabajo para la gestión de la ciberseguridad.** Este trabajo podría centrarse en comparar diferentes marcos de trabajo para la gestión de la ciberseguridad, como el NIST Cybersecurity Framework, el ISO 27001, el CIS Controls, entre otros. Se podría realizar una evaluación detallada de cada marco, identificando sus fortalezas y debilidades, y analizando su aplicabilidad en diferentes contextos empresariales.

2. **Evaluación de las técnicas de evaluación de riesgos de ciberseguridad.** Este trabajo podría centrarse en comparar diferentes técnicas de evaluación de riesgos de ciberseguridad, como la metodología OCTAVE, el análisis de amenazas y vulnerabilidades, la gestión de vulnerabilidades, entre otros. Se podría realizar una evaluación detallada de cada técnica, identificando sus fortalezas y debilidades, y analizando su aplicabilidad en diferentes contextos empresariales.

3. **Análisis de casos de incidentes de seguridad**. Este trabajo podría centrarse en analizar casos reales de incidentes de seguridad, como el ataque a SolarWinds o el ransomware WannaCry. Se podría realizar una evaluación detallada de cada caso, identificando las debilidades de ciberseguridad que permitieron que se produjera el incidente, y analizando las posibles medidas que se podrían haber tomado para prevenir o mitigar el impacto del incidente.

4. **Desarrollo de un plan de ciberseguridad para una organización.** Este trabajo podría centrarse en el desarrollo de un plan de ciberseguridad para una organización, que contemple todas las fases del ciclo de vida de la ciberseguridad. Se podría realizar una evaluación detallada de los riesgos de seguridad de la organización, identificando las medidas de seguridad necesarias para prevenir, detectar y responder ante incidentes de seguridad. Se podría incluir un análisis de costos y beneficios, así como un plan de implementación detallado.

PERFIL DE ACCESO

El curso se encuentra diseñado para permitir a los alumnos fortalecer sus campos de interés y proporcionar una visión global. Por lo que cualquier persona sin experiencia previa sobre ciberseguridad puede cursarlo y aplicarlo. Sin embargo, es interesante tener conocimientos básicos de informática, ciberseguridad o habilidades de resolución de problemas.

Las personas que posean un título oficial de grado o equivalente, recibirán un Diploma Superior Universitario de Postgrado. Si no se dispone de grado universitario o equivalente, se obtendrá un diploma de aprovechamiento.

La **Universidad Europea IMF** (eUniv), es una institución privada de enseñanza superior del Principado de Andorra autorizada por su Gobierno de acuerdo con la ley andorrana de universidades, para impartir enseñanzas estatales de bachelor, máster y doctorado. El Principado de Andorra forma parte del Espacio Europeo se Enseñanza Superior (EEES) desde la Conferencia de Berlín (2003) y todos los títulos estatales de su sistema universitario están plenamente adaptado a las exigencias de estructuración en niveles, garantía interna de la calidad, transparencia y reconocimiento de los títulos europeos

CLAUSTRO

DIRECCIÓN DEL PROGRAMA

Dr. Luis G. Jiménez
Doctor por la Universidad de Barcelona especialista en Áreas de investigación: Organizaciones Complejas; Seguridad & Tecnología.

PROFESORADO

Integrado por académicos y profesionales del sector público y privado certificados, entre otras, en:

Con apoyo de PWNCAT, empresa multinacional especializada en servicios de ciberseguridad.
"Precios subvencionados para integrantes de Fuerzas y Cuerpos de Seguridad"

UNIVERSIDAD EUROPEA IMF
INSTITUT UNIVERSITARI LAURENTIA

Diploma Superior de Postgrado universitario en cibersegridad
(nivel I)
secretaria@iu-laurentia.com