inesem
formación continua

Máster en Ciberseguridad & IA

Elige aprender en la escuela
líder en formación para profesionales

ÍNDICE

1 | Somos **INESEM**

2 | **Rankings**

3 | **Alianzas** y acreditaciones

4 | By **EDUCA EDTECH Group**

5 | **Metodología LXP**

6 | **Razones** por las que elegir Inesem

7 | **Programa** Formativo

8 | **Temario**

9 | Contacto

Ver en la web

inesem formación continua

SOMOS INESEM

INESEM es una **Business School online** especializada con un fuerte sentido transformacional. En un mundo cambiante donde la tecnología se desarrolla a un ritmo vertiginoso nosotros somos activos, evolucionamos y damos respuestas a estas situaciones.

Apostamos por **aplicar la innovación tecnológica a todos los niveles en los que se produce la transmisión de conocimiento.** Formamos a profesionales altamente capacitados para los trabajos más demandados en el mercado laboral; profesionales innovadores, emprendedores, analíticos, con habilidades directivas y con una capacidad de añadir valor, no solo a las empresas en las que estén trabajando, sino también a la sociedad. Y todo esto lo podemos realizar con una base sólida sostenida por nuestros objetivos y valores.

Más de **18** años de experiencia	Más de **300k** estudiantes formados	Más de un **90%** tasa de empleabilidad
Hasta un **100%** de financiación	Hasta un **50%** de los estudiantes repite	Hasta un **25%** de estudiantes internacionales

Ver en la web

inesem formación continua

A way to learn, a way to grow

Elige Inesem

QS, sello de excelencia académica

Inesem: 5 estrellas en educación online

RANKINGS DE INESEM

INESEM Business School ha obtenido reconocimiento tanto a nivel nacional como internacional debido a su firme compromiso con la innovación y el cambio.

Para evaluar su posición en estos rankings, se consideran diversos indicadores que incluyen la percepción online y offline, la excelencia de la institución, su compromiso social, su enfoque en la innovación educativa y el perfil de su personal académico.

Ver en la web

ALIANZAS Y ACREDITACIONES

Relaciones institucionales

Relaciones internacionales

Acreditaciones y Certificaciones

Ver en la web

BY EDUCA EDTECH

Inesem es una marca avalada por **EDUCA EDTECH Group,** que está compuesto por un conjunto de experimentadas y reconocidas **instituciones educativas de formación online.** Todas las entidades que lo forman comparten la misión de **democratizar el acceso a la educación** y apuestan por la transferencia de conocimiento, por el desarrollo tecnológico y por la investigación.

EDUCA EDTECH Group

ONLINE EDUCATION

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

inesem business school

INEAF BUSINESS SCHOOL

red educa.net

inesalud

EDU SPORT

EDUCA business school

educaopen tech school

Educa.Pro

ceupe European Business School

ESIBE ESCUELA IBEROAMERICANA DE POSTGRADO

CAPMAN testing solutions

UDAVINCI

Structuralia Engineering eLearning

Ver en la web

inesem formación continua

METODOLOGÍA LXP

La metodología **EDUCA LXP** permite una experiencia mejorada de aprendizaje integrando la AI en los procesos de e-learning, a través de modelos predictivos altamente personalizados, derivados del estudio de necesidades detectadas en la interacción del alumnado con sus entornos virtuales.

EDUCA LXP es fruto de la **Transferencia de Resultados de Investigación** de varios proyectos multidisciplinares de I+D+i, con participación de distintas Universidades Internacionales que apuestan por la transferencia de conocimientos, desarrollo tecnológico e investigación.

1. Flexibilidad

Aprendizaje 100% online y flexible, que permite al alumnado estudiar donde, cuando y como quiera.

2. Accesibilidad

Cercanía y comprensión. Democratizando el acceso a la educación trabajando para que todas las personas tengan la oportunidad de seguir formándose.

3. Personalización

Itinerarios formativos individualizados y adaptados a las necesidades de cada estudiante.

4. Acompañamiento / Seguimiento docente

Orientación académica por parte de un equipo docente especialista en su área de conocimiento, que aboga por la calidad educativa adaptando los procesos a las necesidades del mercado laboral.

5. Innovación

Desarrollos tecnológicos en permanente evolución impulsados por la AI mediante Learning Experience Platform.

6. Excelencia educativa

Enfoque didáctico orientado al trabajo por competencias, que favorece un aprendizaje práctico y significativo, garantizando el desarrollo profesional.

Programas

PROPIOS UNIVERSITARIOS OFICIALES

RAZONES POR LAS QUE ELEGIR INESEM

1. Nuestra Experiencia

- Más de **18 años de experiencia.**
- Más de **300.000 alumnos** ya se han formado en nuestras aulas virtuales
- Alumnos de los 5 continentes.
- **25%** de alumnos internacionales.
- **97%** de satisfacción
- **100% lo recomiendan.**
- Más de la mitad ha vuelto a estudiar en Inesem.

2. Nuestro Equipo

En la actualidad, Inesem cuenta con un equipo humano formado por más **400 profesionales.** Nuestro personal se encuentra sólidamente enmarcado en una estructura que facilita la mayor calidad en la atención al alumnado.

3. Nuestra Metodología

100% ONLINE

Estudia cuando y desde donde quieras. Accede al campus virtual desde cualquier dispositivo.

APRENDIZAJE

Pretendemos que los nuevos conocimientos se incorporen de forma sustantiva en la estructura cognitiva

EQUIPO DOCENTE

Inesem cuenta con un equipo de profesionales que harán de tu estudio una experiencia de alta calidad educativa.

NO ESTARÁS SOLO

Acompañamiento por parte del equipo de tutorización durante toda tu experiencia como estudiante

Ver en la web

inesem formación continua

4. Calidad AENOR

- Somos Agencia de Colaboración Nº99000000169 autorizada por el Ministerio de Empleo y Seguridad Social.
- Se llevan a cabo auditorías externas anuales que garantizan la máxima calidad AENOR.
- Nuestros procesos de enseñanza están certificados por **AENOR** por la ISO 9001.

5. Somos distribuidores de formación

Como parte de su infraestructura y como muestra de su constante expansión Euroinnova incluye dentro de su organización una **editorial y una imprenta digital industrial.**

Máster en Ciberseguridad & IA

DURACIÓN
1500 horas

MODALIDAD
ONLINE

ACOMPAÑAMIENTO
PERSONALIZADO

Titulación

Titulación Expedida y Avalada por el Instituto Europeo de Estudios Empresariales. "Enseñanza No Oficial y No Conducente a la Obtención de un Título con Carácter Oficial o Certificado de Profesionalidad."

inesem formación continua

INESEM BUSINESS SCHOOL

como centro acreditado para la impartición de acciones formativas
expide el presente título propio

NOMBRE DEL ALUMNO/A

con número de documento XXXXXXXXX ha superado los estudios correspondientes de

NOMBRE DEL CURSO

con una duración de XXX horas, perteneciente al Plan de Formación de Inesem Business School.
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX/XXXX-XXXX-XXXXXX.

Con una calificación XXXXXXXXXXXXX.

Y para que conste expido la presente titulación en Granada, a (día) de (mes) del (año).

NOMBRE ALUMNO/A
Firma del Alumno/a

NOMBRE DE AREA MANAGER
La Dirección Académica

Con Estatuto Consultivo, Categoría Especial del Consejo Económico y Social de la UNESCO (Num. Resolución 604/8)

Ver en la web

inesem formación continua

Descripción

El Máster en Ciberseguridad & IA te posiciona en la vanguardia de dos sectores en pleno auge: la ciberseguridad y la inteligencia artificial. En un mundo donde las amenazas digitales evolucionan constantemente y la inteligencia artificial redefine industrias, este máster te brinda las herramientas necesarias para sobresalir en el mercado laboral. Con un enfoque integral, abarca desde la protección de redes y la respuesta a incidentes de seguridad hasta el uso de IA para la detección inteligente de amenazas. Aprenderás sobre hacking ético y análisis forense, dotándote de habilidades críticas para proteger la información en un entorno digital cada vez más complejo. El máster también explora la relación entre IA y big data, permitiéndote aplicar algoritmos avanzados en ciberseguridad.

Objetivos

• Adquirir habilidades en protección de redes a través de protocolos seguros y estrategias avanzadas. - Implementar técnicas de detección y prevención de intrusiones en sistemas informáticos. - Aplicar algoritmos de inteligencia artificial para la detección de amenazas cibernéticas. - Analizar datos utilizando Python y R para mejorar la ciberseguridad. - Diseñar e implementar sistemas de gestión de seguridad de la información. - Integrar chatbots con inteligencia artificial para mejorar la interacción en seguridad. - Desarrollar competencias en análisis forense para la investigación de cibercrímenes.

Para qué te prepara

El Máster en Ciberseguridad & IA está dirigido a profesionales y titulados del sector tecnológico que buscan ampliar sus conocimientos en áreas clave como la protección de redes, análisis forense, inteligencia artificial aplicada y gestión de incidentes de seguridad. Ideal para aquellos interesados en la detección inteligente de amenazas y el uso de IA en la ciberseguridad.

A quién va dirigido

El máster en Ciberseguridad & IA te prepara para enfrentar desafíos complejos en el ámbito digital. Aprenderás a proteger redes mediante la comprensión de protocolos y transmisión de datos, así como a identificar y mitigar ciberamenazas a través de técnicas de hacking ético e ingeniería social. Además, desarrollarás habilidades en inteligencia artificial, aplicando machine learning y deep learning para fortalecer la seguridad informática.

Salidas laborales

Las salidas laborales del máster en Ciberseguridad & IA abarcan puestos en los que se requiere la capacidad de anticipar, detectar y mitigar riesgos tecnológicos. Entre ellos destacan perfiles como analista de ciberseguridad, profesional de seguridad en redes y sistemas, responsable de gestión de

seguridad de la información y especialista en análisis forense digital.

TEMARIO

MÓDULO 1. CIBERSEGURIDAD Y REDES INFORMÁTICAS

UNIDAD DIDÁCTICA 1. CIBERSEGURIDAD

1. La sociedad de la información
2. Diseño, desarrollo e implantación
3. Factores de éxito en la seguridad de la información

UNIDAD DIDÁCTICA 2. INTRODUCCIÓN A LA RED

1. Elementos Principales de una red
2. Tecnología de redes
3. Soporte para la continuidad de la actividad

UNIDAD DIDÁCTICA 3. ESTANDARIZACIÓN DE PROTOCOLOS

1. Modelo OSI
2. Enfoque pragmático del modelo de capas
3. Estándares y organismos

UNIDAD DIDÁCTICA 4. TRANSMISIÓN DE DATOS EN LA CAPA FÍSICA

1. Papel de una interfaz de red
2. Opciones y parámetros de configuración
3. Arranque desde la red
4. Codificación de los datos
5. Conversión de las señales
6. Soportes de transmisión

UNIDAD DIDÁCTICA 5. SOFTWARE DE COMUNICACIÓN

1. Configuración de la tarjeta de red
2. Instalación y configuración del controlador de la tarjeta de red
3. Pila de protocolos
4. Detección de un problema de red

UNIDAD DIDÁCTICA 6. ARQUITECTURA DE RED E INTERCONEXIÓN

1. Topologías
2. Elección de la topología de red adaptada
3. Gestión de la comunicación
4. Interconexión de redes

UNIDAD DIDÁCTICA 7. CAPAS BAJAS DE LAS REDES PERSONALES Y LOCALES

1. Capas bajas e IEEE

2. Ethernet e IEEE 802.3
3. Token Ring e IEEE 802.5
4. Wi-Fi e IEEE 802.11
5. Bluetooth e IEEE 802.15
6. Otras tecnologías

UNIDAD DIDÁCTICA 8. REDES MAN Y WAN, PROTOCOLOS

1. Interconexión de la red local
2. Acceso remoto y redes privadas virtuales

UNIDAD DIDÁCTICA 9. PROTOCOLOS DE CAPAS MEDIAS Y ALTAS

1. Principales familias de protocolos
2. Protocolo IP versión 4
3. Protocolo IP versión 6
4. Otros protocolos de capa Internet
5. Voz sobre IP (VoIP)
6. Protocolos de transporte TCP y UDP
7. Capa de aplicación TCP/IP

UNIDAD DIDÁCTICA 10. PROTECCIÓN DE UNA RED

1. Comprensión de la necesidad de la seguridad
2. Herramientas y tipos de ataques
3. Conceptos de protección en la red local
4. Protección de la interconexión de redes

UNIDAD DIDÁCTICA 11. REPARACIÓN DE RED

1. Introducción a la reparación de red
2. Diagnóstico en capas bajas
3. Utilización de herramientas TCP/IP adaptadas
4. Herramientas de análisis de capas altas

UNIDAD DIDÁCTICA 12. INGENIERÍA SOCIAL, ATAQUES WEB Y PHISHING

1. Introducción a la ingeniería social
2. Recopilar información
3. Herramientas de ingeniería social
4. Técnicas de ataques
5. Prevención de ataques
6. Introducción al phishing
7. Phishing
8. Man in the middle

MÓDULO 2. PERITAJE INFORMÁTICO FORENSE

UNIDAD DIDÁCTICA 1. INFORMÁTICA, CONECTIVIDAD E INTERNET

1. La informática
2. Componentes de un sistema informático
3. Estructura básica de un sistema informático
4. Unidad central de proceso en un sistema informático
5. Periféricos más usuales: conexión
6. Sistema operativo
7. Internet
8. Conectividad a Internet

UNIDAD DIDÁCTICA 2. FUNDAMENTOS DE LA INFORMÁTICA Y ELECTRÓNICA FORENSE

1. Concepto de informática forense
2. Objetivos de la informática forense
3. Usos de la informática forense
4. El papel del perito informático
5. El laboratorio informático forense
6. Evidencia digital
7. Cadena de custodia

UNIDAD DIDÁCTICA 3. CIBERCRIMINALIDAD

1. Delito informático
2. Tipos de delito informático
3. Cibercriminalidad

UNIDAD DIDÁCTICA 4. HACKING ÉTICO

1. ¿Qué es el hacking ético?
2. Aspectos legales del hacking ético
3. Perfiles del hacker
4. Test de vulnerabilidades
5. Sniffing
6. Tipos de test de seguridad en entornos web

UNIDAD DIDÁCTICA 5. ANÁLISIS FORENSE

1. El análisis forense
2. Etapas de un análisis forense
3. Tipos de análisis forense
4. Requisitos para el análisis forense
5. Principales problemas

UNIDAD DIDÁCTICA 6. SOPORTE DE DATOS

1. Adquisición de datos: importancia en el análisis forense digital
2. Modelo de capas
3. Recuperación de archivos borrados
4. Análisis de archivos

UNIDAD DIDÁCTICA 7. SISTEMA DE GESTIÓN DE SEGURIDAD EN LA INFORMACIÓN SGSI

1. La sociedad de la información
2. ¿Qué es la seguridad de la información?
3. Importancia de la seguridad de la información
4. Principios básicos de seguridad de la información: confidencialidad, integridad y disponibilidad
5. Descripción de los riesgos de la seguridad
6. Selección de controles
7. Factores de éxito en la seguridad de la información
8. Beneficios aportados por un sistema de seguridad de la información

MÓDULO 3. INTELIGENCIA ARTIFICIAL, MACHINE LEARNING Y DEEP LEARNING: TRES PILARES DE LA COMPUTACIÓN MODERNA

UNIDAD DIDÁCTICA 1. FUNDAMENTOS DE INTELIGENCIA ARTIFICIAL

1. Inmersión a la IA explicando sus principales modalidades
2. Breve noción sobre los principales algoritmos de IA
3. Análisis de los diferentes tipos de aprendizaje
4. Fundamentos matemáticos para el entendimiento del funcionamiento de distintos algoritmos basados en IA y conceptos básicos de programación
5. Implementación de conceptos matemáticos de IA utilizando Python como lenguaje de programación
6. Fundamentos estadísticos básicos para el entendimiento del funcionamiento de distintos algoritmos, preprocesamiento de datos y análisis de resultados
7. Implementación de conceptos estadísticos utilizando Python como lenguaje de programación
8. Puesta en marcha del entorno de trabajo
9. Detalle de los diferentes softwares y programas utilizados para la implementación de algoritmos basados en IA
10. Inmersión en el lenguaje Python

UNIDAD DIDÁCTICA 2. FUTURO DE LA INTELIGENCIA ARTIFICIAL

1. Futuro de la inteligencia artificial
2. Impacto de la IA en la industria
3. El impacto económico y social global de la IA y su futuro

UNIDAD DIDÁCTICA 3. INTRODUCCIÓN AL MACHINE LEARNING

1. Introducción
2. Clasificación de algoritmos de aprendizaje automático
3. Ejemplos de aprendizaje automático
4. Diferencias entre el aprendizaje automático y el aprendizaje profundo
5. Tipos de algoritmos de aprendizaje automático
6. El futuro del aprendizaje automático

UNIDAD DIDÁCTICA 4. EXTRACCIÓN DE ESTRUCTURA DE LOS DATOS: CLUSTERING

1. Introducción
2. Algoritmos

UNIDAD DIDÁCTICA 5. REDES NEURONALES Y DEEP LEARNING

1. Componentes
2. Aprendizaje

UNIDAD DIDÁCTICA 6. SISTEMAS DE ELECCIÓN

1. Introducción
2. El proceso de paso de DSS a IDSS
3. Casos de aplicación

UNIDAD DIDÁCTICA 7. DEEP LEARNING CON PYTHON, KERAS Y TENSORFLOW

1. Aprendizaje profundo
2. Entorno de Deep Learning con Python
3. Aprendizaje automático y profundo

MÓDULO 4. INTELIGENCIA ARTIFICIAL CON CHATBOTS Y COPILOT

UNIDAD DIDÁCTICA 1. EL POTENCIAL DE LA INTELIGENCIA ARTIFICIAL

1. Introducción a la inteligencia artificial
2. Historia
3. La importancia de la IA
4. Tipos de inteligencia artificial
5. Algoritmos aplicados a la inteligencia artificial

UNIDAD DIDÁCTICA 2. ¿QUÉ ES UNA HERRAMIENTA COPILOT?

1. ¿Qué son las herramientas Copilot?
2. Beneficios de usar herramientas Copilot
3. Requisitos para usar herramientas Copilot
4. Tipos de herramientas Copilot
5. Comparación de diferentes herramientas Copilot

UNIDAD DIDÁCTICA 3. INTRODUCCIÓN A LOS MODELOS DE LENGUAJE

1. Concepto de modelo de lenguaje
2. Evolución de los modelos de lenguaje
3. Arquitecturas principales de modelos de lenguaje: Transformer, GPT-3, LaMDA
4. Parámetros y datasets
5. Aplicaciones de los modelos de lenguaje

UNIDAD DIDÁCTICA 4. CHATGPT: FUNDAMENTOS Y FUNCIONAMIENTO

1. DeepMind y OpenAI
2. La arquitectura de red neuronal de ChatGPT: GPT-3 y sus variantes
3. Entrenamiento de ChatGPT
4. Capacidades de ChatGPT
5. Limitaciones y riesgos de ChatGPT

UNIDAD DIDÁCTICA 5. GEMINI: LA PROPUESTA DE GOOGLE

1. Bard: el modelo de lenguaje de Google AI
2. Diferencias entre Gemini y GPT-3
3. Capacidades de Gemini
4. Integración de Gemini con otros productos de Google
5. Futuro de Gemini

UNIDAD DIDÁCTICA 6. BING CHAT: EL MODELO DE MICROSOFT

1. Microsoft y Bing: su apuesta por la IA conversacional
2. Características de Bing Chat
3. Integración de Bing Chat con el motor de búsqueda Bing
4. Comparación entre Bing Chat y ChatGPT
5. Futuro de Bing Chat

UNIDAD DIDÁCTICA 7. ASPECTOS TÉCNICOS AVANZADOS

1. Tokenización y embeddings
2. Attention mechanism
3. Beam search y otros algoritmos de decodificación
4. Optimización del entrenamiento
5. Evaluación de modelos de lenguaje

UNIDAD DIDÁCTICA 8. COPILOT CON DIFERENTES CHATBOTS

1. Tipos de chatbots
2. Copilot y ChatGPT
3. Copilot y Gemini de Google
4. Copilot y Bing Chat de Microsoft
5. Copilots y Chatbots específicos de industrias

MÓDULO 5. CIENCIA DE DATOS E INTELIGENCIA ARTIFICIAL

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LA CIENCIA DE DATOS

1. ¿Qué es la ciencia de datos?
2. Herramientas necesarias para el científico de datos
3. Data Science & Cloud Compunting

UNIDAD DIDÁCTICA 2. BASES DE DATOS RELACIONALES

1. Modelo de datos
2. Tipos de datos
3. Claves primarias
4. Índices
5. El valor NULL
6. Claves ajenas
7. Vistas
8. Lenguaje de descripción de datos (DDL)
9. Lenguaje de control de datos (DCL)

UNIDAD DIDÁCTICA 3. BASES DE DATOS NOSQL Y EL ALMACENAMIENTO ESCALABLE

1. ¿Qué es una base de datos NoSQL?
2. Bases de datos Relaciones Vs Bases de datos NoSQL
3. Tipo de Bases de datos NoSQL: Teorema de CAP
4. Sistemas de Bases de datos NoSQL

UNIDAD DIDÁCTICA 4. INTRODUCCIÓN A UN SISTEMA DE BASE DE DATOS NOSQL, MONGODB

1. ¿Qué es MongoDB?
2. Funcionamiento y usos de MongoDB
3. Primeros pasos con MongoDB: Instalación y Shell de comandos
4. Creando nuestra primera base de datos NoSQL: Modelo e inserción de datos
5. Actualización de datos en MongoDB: Sentencias set y update
6. Trabajando con índices en MongoDB para optimización de datos
7. Consulta de datos en MongoDB

UNIDAD DIDÁCTICA 5. PYTHON Y EL ANÁLISIS DE DATOS

1. Introducción a Python
2. ¿Qué necesitas?
3. Librerías para el análisis de datos en Python
4. MongoDB, Hadoop y Python Dream Team del Big Data

UNIDAD DIDÁCTICA 6. R COMO HERRAMIENTA PARA BIG DATA

1. Introducción a R
2. ¿Qué necesitas?
3. Tipos de datos
4. Estadística Descriptiva y Predictiva con R
5. Integración de R en Hadoop

UNIDAD DIDÁCTICA 7. PRE-PROCESAMIENTO & PROCESAMIENTO DE DATOS

1. Obtención y limpieza de los datos (ETL)
2. Inferencia estadística
3. Modelos de regresión
4. Pruebas de hipótesis

UNIDAD DIDÁCTICA 8. ANÁLISIS DE LOS DATOS

1. Inteligencia Analítica de negocios
2. La teoría de grafos y el análisis de redes sociales
3. Presentación de resultados

MÓDULO 6. GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

1. Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención

2. Identificación y caracterización de los datos de funcionamiento del sistema
3. Arquitecturas más frecuentes de los IDS
4. Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
5. Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

UNIDAD DIDÁCTICA 2. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS

1. Análisis previo
2. Definición de políticas de corte de intentos de intrusión en los IDS/IPS
3. Análisis de los eventos registrados por el IDS/IPS
4. Relación de los registros de auditoría del IDS/IPS
5. Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

UNIDAD DIDÁCTICA 3. CONTROL MALWARE

1. Sistemas de detección y contención de Malware
2. Herramientas de control de Malware
3. Criterios de seguridad para la configuración de las herramientas de protección frente a Malware
4. Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a Malware
5. Relación de los registros de auditoría de las herramientas de protección frente a Malware
6. Establecimiento de la monitorización y pruebas de las herramientas de protección frente a Malware
7. Análisis de Malware mediante desensambladores y entornos de ejecución controlada

UNIDAD DIDÁCTICA 4. RESPUESTA ANTE INCIDENTES DE SEGURIDAD

1. Procedimiento de recolección de información relacionada con incidentes de seguridad
2. Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad
3. Proceso de verificación de la intrusión
4. Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales

UNIDAD DIDÁCTICA 5. PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN

1. Establecimiento de las responsabilidades
2. Categorización de los incidentes derivados de intentos de intrusión
3. Establecimiento del proceso de detección y herramientas de registro de incidentes
4. Establecimiento del nivel de intervención requerido en función del impacto previsible
5. Establecimiento del proceso de resolución y recuperación de los sistemas
6. Proceso para la comunicación del incidente a terceros

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE INFORMÁTICO

1. Conceptos generales y objetivos del análisis forense
2. Exposición del Principio de Lockard
3. Guía para la recogida de evidencias electrónicas
4. Guía para el análisis de las evidencias electrónicas recogidas
5. Guía para la selección de las herramientas de análisis forense

MÓDULO 7. HACKING TRAINING PLATFORMS

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A HACKING TRAINING PLATFORMS

1. ¿Qué es el hacking ético?
2. Máquinas virtuales
3. Plataformas para practicar hacking ético

UNIDAD DIDÁCTICA 2. HACK THE BOX (HTB)

1. Introducción a Hack The Box
2. Crear una cuenta
3. Tutoriales

UNIDAD DIDÁCTICA 3. TRYHACKME

1. ¿Qué es TryHackMe?
2. Crear una cuenta
3. Interfaz de TryHackMe
4. Introducción a la ciberseguridad
5. Seguridad ofensiva
6. Ciencia forense digital

UNIDAD DIDÁCTICA 4. HACKER101

1. ¿Qué es Hacker101?
2. Hacker101 CTF
3. Tutoriales

UNIDAD DIDÁCTICA 5. VULNHUB

1. ¿Qué es Vulnhub?
2. Interfaz de Vulnhub
3. Tutoriales

UNIDAD DIDÁCTICA 6. HACK THIS SITE

1. ¿Qué es Hack This Suite?
2. Desafíos Hack This Site

UNIDAD DIDÁCTICA 7. GOOGLE XSS GAME

1. ¿Qué es Google XSS Game?
2. Niveles de Google XSS game

UNIDAD DIDÁCTICA 8. HACKTHIS

1. ¿Qué es HackThis?
2. Tutorial HackThis
3. Basic+

MÓDULO 8. IA EN LA CIBERSEGURIDAD

UNIDAD DIDÁCTICA 1. FUNDAMENTOS DE IA APLICADA A LA CIBERSEGURIDAD

1. Revisión de arquitecturas clave de IA en el contexto de la seguridad digital
2. Desafíos y oportunidades de la IA en la protección de sistemas y datos
3. Fuentes de datos y preprocesamiento para modelos de ciberseguridad
4. Google Cloud AI como plataforma y herramienta para el desarrollo de IA en ciberseguridad

UNIDAD DIDÁCTICA 2. DETECCIÓN INTELIGENTE DE AMENAZAS Y ANOMALÍAS

1. Modelos de machine learning para la detección de malware y virus
2. Análisis de comportamiento de red y usuario (UEBA) con ia
3. Detección de intrusiones basada en anomalías mediante redes neuronales
4. Identificación de ataques de día cero y amenazas persistentes avanzadas (APTS)
5. Técnicas de aprendizaje no supervisado para el descubrimiento de amenazas desconocidas

UNIDAD DIDÁCTICA 3. IA PARA LA GESTIÓN DE VULNERABILIDADES Y PARCHES

1. Priorización de vulnerabilidades utilizando modelos predictivos
2. Automatización de la identificación y clasificación de fallos de seguridad
3. Predicción de exploits y superficies de ataque con IA
4. Optimización de estrategias de parcheo basadas en riesgo
5. Análisis de código estático y dinámico asistido por IA

UNIDAD DIDÁCTICA 4. SEGURIDAD CIUDADANA Y RESPUESTA A EMERGENCIAS CON IA

1. Generación de ataques adversarios para pruebas de resistencia
2. Automatización de pruebas de penetración y escaneo de vulnerabilidades
3. Desarrollo de honeypots inteligentes para engañar a atacantes
4. Respuesta automatizada a incidentes y contención de amenazas
5. Modelos de aprendizaje por refuerzo para estrategias de ciberdefensa

UNIDAD DIDÁCTICA 5. PROTECCIÓN DE LA PRIVACIDAD Y DATOS CON IA

1. Anonimización y desidentificación de datos sensibles utilizando IA
2. Detección y prevención de fugas de datos (DLP) asistida por IA
3. Seguridad en el tratamiento de datos personales con técnicas de IA
4. Privacidad diferencial y criptografía homomórfica aplicadas con IA
5. Gestión de identidad y acceso (IAM) inteligente

UNIDAD DIDÁCTICA 6. IA EN LA CIBERSEGURIDAD CLOUD Y DE INFRAESTRUCTURAS

1. Monitoreo y detección de amenazas en entornos de nube
2. Seguridad de contenedores y microservicios con IA
3. Protección de infraestructuras críticas y sistemas de control industrial (ICS/SCADA)
4. Análisis de riesgos y cumplimiento en entornos multicloud
5. Implementación de IA para la seguridad de la cadena de suministro de software

UNIDAD DIDÁCTICA 7. RESILIENCIA CIBERNÉTICA Y RECUPERACIÓN ASISTIDA POR IA

1. Evaluación de la resiliencia de sistemas frente a ciberataques
2. Planificación y simulación de escenarios de crisis con IA
3. Recuperación automatizada de desastres y restauración de sistemas
4. Análisis forense digital y detección de persistencia con IA
5. Optimización de planes de continuidad de negocio post-ataque

UNIDAD DIDÁCTICA 8. EL FUTURO DE LA IA EN CIBERSEGURIDAD

1. IA explicable (XAI) en la toma de decisiones de seguridad
2. Ataques adversarios contra modelos de IA y contramedidas
3. El papel de la computación cuántica en la ciberseguridad
4. Tendencias emergentes en la intersección IA-Ciberseguridad
5. Colaboración humano-IA en los equipos de ciberseguridad (Google Security Operations)

MÓDULO 9. PROYECTO FIN DE MÁSTER

Solicita información sin compromiso

¡Matricularme ya!

Teléfonos de contacto

+34 958 050 240

!Encuéntranos aquí!

Edificio Educa Edtech

Camino de la Torrecilla N.º 30 EDIFICIO EDUCA EDTECH,
Oficina 34, C.P. 18200, Maracena (Granada)

formacion.continua@inesem.es

www.formacioncontinua.eu

Horario atención al cliente

Lunes a Jueves: 09:00 a 20:00

Viernes: 9:00 a 14:00

Ver en la web

inesem
formación continua


inesem
formación continua


By
EDUCA EDTECH
Group