EUROINNOVA
INTERNATIONAL ONLINE EDUCATION

inesem business school UTAMED

Curso Superior en Gestión de Incidentes de Ciberseguridad y Análisis Malware + 16 Créditos ECTS

Elige aprender en la escuela
líder en formación online

ÍNDICE

Ver en la web

inesem business school

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 business school

Leaders driving change

Elige Inesem

ALIANZA INESEM Y UTAMED

NESEM y **UTAMED** se unen para liderar la transformación de la educación superior online.

INESEM Business School destaca como business school de referencia en formación online para profesionales, con especial énfasis en áreas como empresa, marketing, recursos humanos, tecnología y gestión empresarial. Su modelo formativo combina accesibilidad, innovación y un fuerte enfoque en el desarrollo de competencias.

UTAMED, desde su origen digital y su mirada Atlántico-Mediterránea, comparte esa visión orientada al futuro. Como universidad 100% online, apuesta por programas actualizados, multidisciplinares y adaptados a las demandas de un mercado global.

Esta alianza refuerza el puente entre la formación profesional y la formación universitaria, creando itinerarios integrados que permiten a los estudiantes avanzar en sus carreras con titulaciones avaladas académicamente y conectadas con el entorno laboral.

Ambas instituciones coinciden en ofrecer una experiencia educativa ágil, práctica y con fuerte base tecnológica, gracias a la novedosa metodología EDUCA LXP.

UTAMED

inesem business school

Ver en la web

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.

QS STARS RATING SYSTEM
Online Learning

Financial Magazine
Actualidad Económica & Centros de Formación

Ranking Educativo Innovatec

LOS MEJORES MASTERS EN CIBERSEGURIDAD
CyberEOP

FSO RANKING

Webometrics
RANKING WEB OF UNIVERSITIES

NOSOLOMASTER
RANKING Y OPINIONES SOBRE MASTER

webempresa

EL MUNDO

Ver en la web

inesem
business school

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 business school

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 business school

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.**

MÉTODOS DE PAGO

Con la Garantía de:

educapay

Fracciona el pago de tu curso en cómodos plazos y sin interéres de forma segura.

mastercard maestro VISA PayPal

bizum amazon pay Pay G Pay

Nos adaptamos a todos los métodos de pago internacionales:

OXXO mercado pago DISCOVER efecty Diners Club INTERNATIONAL CMR Falabella

y muchos más...

Protección al Comprador

Ver en la web

inesem business school

Curso Superior en Gestión de Incidentes de Ciberseguridad y Análisis Malware + 16 Créditos ECTS

DURACIÓN
400 horas

MODALIDAD
ONLINE

ACOMPAÑAMIENTO
PERSONALIZADO

CREDITOS
16 ECTS

Titulación

Titulación de Curso Superior en Gestión de Incidentes de Ciberseguridad y Análisis Malware con 400 horas y 16 ECTS expedida por UTAMED - Universidad Tecnológica Atlántico Mediterráneo.

Ver en la web

inesem business school


UTAMED

inesem business school

INESEM BUSINESS SCHOOL
UNIVERSIDAD TECNOLÓGIC ALTÁNTICO - MEDITERRÁNEO

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 UTAMED.
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX/XXXX-XXXX-XXXXXX.
Con una calificación XXXXXXXXXXXXXX.
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 ÁREA MANAGER
La Dirección Académica

Descripción

Con este Curso en Gestión de Incidentes de Ciberseguridad y Análisis Malware tendrás una formación completa sobre sistemas de detección y prevención de intrusiones, control de malware, respuesta a incidentes de seguridad, gestión de intentos de intrusión y análisis forense informático. Además de dominar las técnicas de implementación y las mejores prácticas en ciberseguridad. En cuanto a análisis de malware podrás identificar los tipos de malware, como se comportan y podrás analizar diferentes tipos de archivos para detectar los malware, confinarlos para su análisis posterior utilizando ingeniería inversa y luego crear planes para defenderse de estos malware. Además, contarás con un equipo docente especializado en la materia.

Objetivos

- Comprender los fundamentos de gestión de incidentes, detección de intrusiones y prevención.
- Conocer las diferentes arquitecturas y tipos de IDS/IPS, y establecer criterios de seguridad para su ubicación.
- Implementar y gestionar sistemas IDS/IPS.
- Controlar y proteger eficazmente contra el malware.
- Responder y gestionar incidentes de seguridad.
- Establecer procesos para la notificación, gestión y resolución de intentos de intrusión.
- Desarrollar habilidades en análisis forense informático.

Ver en la web

Para qué te prepara

Este Curso en Gestión de Incidentes de Ciberseguridad y Análisis Malware dirigido a estudiantes y profesionales informáticos que quieran adquirir conocimientos en ciberseguridad, más específicamente en gestión de riesgos y análisis de malware. También para todo aquel que esté interesado en aprender sobre ciberseguridad.

A quién va dirigido

Este Curso en Gestión de Incidentes de Ciberseguridad y Análisis Malware te prepara para enfrentarte a los desafíos actuales de la ciberseguridad y de las amenazas del malware, capacidad para responder y gestionar incidentes de seguridad. Establecer procesos de notificación y gestión de intentos de intrusión y realizar análisis forense informático. Al finalizar este curso, estarás capacitado para proteger los sistemas y datos frente a ataques cibernéticos.

Salidas laborales

Al finalizar este Curso en Gestión de Incidentes de Ciberseguridad y Análisis Malware, estarás preparado para desempeñarte como especialista en ciberseguridad, analista de seguridad de la información, consultor de seguridad, administrador de sistemas, perito informático forense o analista de malware. Podrás trabajar en empresas de seguridad informática.

TEMARIO

MÓDULO 1. CIBERSEGURIDAD: GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES

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 2. ANÁLISIS DE MALWARE

UNIDAD DIDÁCTICA 1. ESCENARIO DE INFECCIÓN Y TÉCNICAS DE COMUNICACIÓN

1. Ejecución de un archivo adjunto
2. Clic desafortunado
3. Apertura de un documento infectado
4. Ataques informáticos
5. Ataques físicos: infección por llave USB
6. Introducción a las técnicas de comunicación con el C&C

UNIDAD DIDÁCTICA 2. OBTENCIÓN Y ANÁLISIS DE INFORMACIÓN

1. Analizando datos del registro
2. Analizando datos del registro de eventos
3. Analizando archivos ejecutados durante el arranque
4. Analizando sistema de archivos

UNIDAD DIDÁCTICA 3. FUNCIONALIDADES DE LOS MALWARES. COMO OPERAR ANTE AMENAZAS

1. Técnicas de persistencia
2. Técnicas de ocultación
3. Malware sin archivo
4. Evitar el UAC
5. Fases para operar ante amenazas

UNIDAD DIDÁCTICA 4. ANÁLISIS BÁSICO DE ARCHIVOS

1. Análisis de un archivo PDF
2. Extraer el código JavaScript
3. Desofuscar código JavaScript
4. Análisis de un archivo de Adoble Flash
5. Análisis de un archivo JAR
6. Análisis de un archivo de Microsoft Office

UNIDAD DIDÁCTICA 5. REVERSE ENGINEERING

1. ¿Qué es el Reverse Engineering?
2. Ensamblador x86

3. Ensamblador x64
4. Análisis estático
5. Análisis dinámico

UNIDAD DIDÁCTICA 6. OFUSCACIÓN, INTRODUCCIÓN Y TÉCNICAS

1. ¿Qué es la ofuscación?
2. Ofuscación de cadenas de caracteres
3. Ofuscación mediante la API de Windows
4. Packers
5. Otros tipos de técnicas ofuscación

UNIDAD DIDÁCTICA 7. DETECCIÓN Y CONFINAMIENTO

1. Primeros pasos en la detección y confinamiento
2. Compromiso de red: Indicadores
3. Tips de firmas de archivo
4. Detección y erradicación a través de ClamAV

UNIDAD DIDÁCTICA 8. OPENIOC

1. Introducción a OpenIOC
2. Primeros pasos con
3. Interfaz gráfica de edición
4. Detección

¿Te ha parecido interesante esta información?

Si aún tienes dudas, nuestro equipo de asesoramiento académico estará encantado de resolverlas.

Pregúntanos sobre nuestro método de formación, nuestros profesores, las becas o incluso simplemente conócenos.

Solicita información sin compromiso

Teléfonos de contacto

España	+34 900 831 200	Argentina	54-(11)52391339
Bolivia	+591 50154035	Estados Unidos	1-(2)022220068
Chile	56-(2)25652888	Guatemala	+502 22681261
Colombia	+57 601 50885563	Mexico	+52-(55)11689600
Costa Rica	+506 40014497	Panamá	+507 8355891
Ecuador	+593 24016142	Perú	+51 1 17075761
El Salvador	+503 21130481	República Dominicana	+1 8299463963

!Encuéntranos aquí!

Edificio Educa Edtech

Camino de la Torrecilla N.º 30 EDIFICIO EDUCA EDTECH,
C.P. 18.200, Maracena (Granada)

formacion@euroinnova.com

www.euroinnova.com

Horario atención al cliente

Lunes a viernes: 9:00 a 20:00h Horario España

Ver en la web

inesem business school

¡Síguenos para estar al tanto de todas nuestras novedades!

España 

Latino America 

Reública Dominicana 

Ver en la web

inesem
business school

inesem
business school

By
EDUCA EDTECH
Group