

Curso Superior en Seguridad Informática y en Elaboración de Informes Periciales
+ 16 Créditos ECTS





**Elige aprender en la escuela
líder en formación para profesionales**

ÍNDICE

1 | Somos INESEM

**4 | By EDUCA
EDTECH
Group**

**7 | Programa
Formativo**

2 | Rankings

**5 | Metodología
LXP**

8 | Temario

**3 | Alianzas y
acreditaciones**

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

9 | Contacto

[Ver en la web](#)

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](#)



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.



ONLINE EDUCATION



[Ver en la web](#)



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](#)

4. Calidad AENOR

- ✓ Somos Agencia de Colaboración N°99000000169 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**.

[Ver en la web](#)

Curso Superior en Seguridad Informática y en Elaboración de Informes Periciales + 16 Créditos ECTS



DURACIÓN

400 horas



MODALIDAD

ONLINE



ACOMPAÑAMIENTO

PERSONALIZADO



CREDITOS

16 ECTS

Titulación

Titulación de Curso Superior en Seguridad Informática y en Elaboración de Informes Periciales con 400 horas y 16 ECTS expedida por UTAMED - Universidad Tecnológica Atlántico Mediterráneo.

[Ver en la web](#)



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 XXXXX/XXXX-XXXX-XXXXXX.

Con una calificación XXXXXXXXXXXXXXXX.

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

NOMBRE ALUMNO/A
Firma del Alumno/s

NOMBRE DE ÁREA MANAGER
La Dirección Académica



Con Estatuto Consultivo, Categoría Especial del Consejo Económico y Social de la UNESCO (Nº resolución 604/94)

Descripción

Hoy en día la seguridad informática es un tema muy importante y sensible, que abarca un gran conjunto de aspectos en continuo cambio y constante evolución, que exige que los profesionales informáticos posean conocimientos actualizados. Con la realización del Curso en Seguridad Informática y en Elaboración de Informes Periciales el alumno aprenderá los conocimientos necesarios para actuar como Perito Judicial en los ámbitos de Seguridad Informática y contiene todo lo necesario para poder ejercer como Perito Judicial, desarrollando con éxito esta actividad, una vez obtenido el diploma va a poder tramitar el alta en los Juzgados que el designe e incluye toda la legislación actual en el mundo del Peritaje. También, contarás con un equipo de profesionales especializados en la materia.

Objetivos

- Conocer los ámbitos de actuación de un Perito Judicial en Seguridad Informática.
- Proteger sistemas informáticos.
- Auditarse redes de comunicación y sistemas informáticos.
- Detectar y responder ante incidentes de seguridad.
- Diseñar e implementar sistemas seguros de acceso y transmisión de datos.
- Gestionar servicios en el sistema informático.

[Ver en la web](#)

Para qué te prepara

Este Curso en Seguridad Informática y en Elaboración de Informes Periciales va dirigido a todas aquellas personas que quieran orientar su futuro laboral en el mundo de la peritación judicial en seguridad informática, desempeñando tareas propias de un perito judicial y conociendo aspectos dentro de la informática como las tareas de auditoría.

A quién va dirigido

Este Curso en Seguridad Informática y en Elaboración de Informes Periciales te dotará de competencias profesionales para ejercer como Perito Judicial. Además de garantizar la seguridad de los accesos y usos de la información registrada en equipos informáticos, así como del propio sistema, asegurándolos de los posibles ataques, identificando vulnerabilidades y aplicando estrategias de protección contra estos.

Salidas laborales

Al finalizar este Curso en Seguridad Informática y en Elaboración de Informes Periciales, podrás optar por una trayectoria profesional dedicada a la ciberseguridad como perito informático forense que podrás ejercer en diferentes procesos judiciales que se den lugar en los Juzgados y Tribunales. Tendrás que defender tu informe pericial siguiendo los procedimientos necesarios.

[Ver en la web](#)

TEMARIO

MÓDULO 1. PERITO JUDICIAL

UNIDAD DIDÁCTICA 1. PERITACIÓN Y TASACIÓN

1. Delimitación de los términos peritaje y tasación
2. La peritación
3. La tasación pericial

UNIDAD DIDÁCTICA 2. NORMATIVA BÁSICA NACIONAL

1. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial
2. Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil
3. Ley de Enjuiciamiento Criminal, de 1882
4. Ley 1/1996, de 10 de enero, de Asistencia Jurídica Gratuita

UNIDAD DIDÁCTICA 3. LOS PERITOS

1. Concepto
2. Clases de perito judicial
3. Procedimiento para la designación de peritos
4. Condiciones que debe reunir un perito
5. Control de la imparcialidad de peritos
6. Honorarios de los peritos

UNIDAD DIDÁCTICA 4. EL RECONOCIMIENTO PERICIAL

1. El reconocimiento pericial
2. El examen pericial
3. Los dictámenes e informes periciales judiciales
4. Valoración de la prueba pericial
5. Actuación de los peritos en el juicio o vista

UNIDAD DIDÁCTICA 5. LEGISLACIÓN REFERENTE A LA PRÁCTICA DE LA PROFESIÓN EN LOS TRIBUNALES

1. Funcionamiento y legislación
2. El código deontológico del Perito Judicial

UNIDAD DIDÁCTICA 6. LA RESPONSABILIDAD

1. La responsabilidad
2. Distintos tipos de responsabilidad
 1. - Responsabilidad civil
 2. - Responsabilidad penal
 3. - Responsabilidad disciplinaria
3. El seguro de responsabilidad civil

[Ver en la web](#)

UNIDAD DIDÁCTICA 7. PERITACIONES

1. La peritación médico-legal
 1. - Daño corporal
 2. - Secuelas
2. Peritaciones psicológicas
 1. - Informe pericial del peritaje psicológico
3. Peritajes informáticos
4. Peritaciones inmobiliarias

MÓDULO 2. ELABORACIÓN DE INFORMES PERICIALES

UNIDAD DIDÁCTICA 1. PERITO, INFORME PERICIAL Y ATESTADO POLICIAL

1. Concepto de perito
2. Atestado policial
3. Informe pericial

UNIDAD DIDÁCTICA 2. TIPOS DE INFORMES PERICIALES

1. Informes periciales por cláusulas de suelo
2. Informes periciales para justificación de despidos

UNIDAD DIDÁCTICA 3. TIPOS DE INFORMES PERICIALES

1. Informes periciales de carácter económico, contable y financiero
2. Informes especiales de carácter pericial

UNIDAD DIDÁCTICA 4. LAS PRUEBAS JUDICIALES Y EXTRAJUDICIALES

1. Concepto de prueba
2. Medios de prueba
3. Clases de pruebas
4. Principales ámbitos de actuación
5. Momento en que se solicita la prueba pericial
6. Práctica de la prueba

UNIDAD DIDÁCTICA 5. ELABORACIÓN DEL INFORME TÉCNICO

1. ¿Qué es el informe técnico?
2. Diferencia entre informe técnico y dictamen pericial
3. Objetivos del informe pericial
4. Estructura del informe técnico

UNIDAD DIDÁCTICA 6. ELABORACIÓN DEL DICTAMEN PERICIAL

1. Características generales y estructura básica
2. Las exigencias del dictamen pericial
3. Orientaciones para la presentación del dictamen pericial

[Ver en la web](#)

UNIDAD DIDÁCTICA 7. VALORACIÓN DE LA PRUEBA PERICIAL

1. Valoración de la prueba judicial
2. Valoración de la prueba pericial por Jueces y Tribunales

MÓDULO 3. SEGURIDAD INFORMATICA

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
2. Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
3. Salvaguardas y tecnologías de seguridad más habituales
4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

UNIDAD DIDÁCTICA 2. ANÁLISIS DE IMPACTO DE NEGOCIO

1. Identificación de procesos de negocio soportados por sistemas de información
2. Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
3. Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

UNIDAD DIDÁCTICA 3. GESTIÓN DE RIESGOS

1. Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
2. Metodologías comúnmente aceptadas de identificación y análisis de riesgos
3. Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

UNIDAD DIDÁCTICA 4. PLAN DE IMPLANTACIÓN DE SEGURIDAD

1. Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio
2. Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
3. Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

UNIDAD DIDÁCTICA 5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. Principios generales de protección de datos de carácter personal
2. Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
3. Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
4. Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

UNIDAD DIDÁCTICA 6. SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE SISTEMAS

1. Determinación de los perímetros de seguridad física
2. Sistemas de control de acceso físico más frecuentes a las instalaciones de la organización y a las áreas en las que estén ubicados los sistemas informáticos
3. Criterios de seguridad para el emplazamiento físico de los sistemas informáticos
4. Exposición de elementos más frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos
5. Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos
6. Elaboración de la normativa de seguridad física e industrial para la organización
7. Sistemas de ficheros más frecuentemente utilizados
8. Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización
9. Configuración de políticas y directivas del directorio de usuarios
10. Establecimiento de las listas de control de acceso (ACLs) a ficheros
11. Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados
12. Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo
13. Sistemas de autenticación de usuarios débiles, fuertes y biométricos
14. Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos
15. Elaboración de la normativa de control de accesos a los sistemas informáticos

UNIDAD DIDÁCTICA 7. IDENTIFICACIÓN DE SERVICIOS

1. Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
2. Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
3. Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

UNIDAD DIDÁCTICA 8. IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

1. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
2. Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ
3. Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones
4. Definición de reglas de corte en los cortafuegos
5. Relación de los registros de auditoría del cortafuegos necesario para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
6. Establecimiento de la monitorización y pruebas de los cortafuegos

UNIDAD DIDÁCTICA 9. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

1. Introducción al análisis de riesgos
2. Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su

[Ver en la web](#)

- actualización permanente, así como criterios de programación segura
- 3. Particularidades de los distintos tipos de código malicioso
 - 4. Principales elementos del análisis de riesgos y sus modelos de relaciones
 - 5. Metodologías cualitativas y cuantitativas de análisis de riesgos
 - 6. Identificación de los activos involucrados en el análisis de riesgos y su valoración
 - 7. Identificación de las amenazas que pueden afectar a los activos identificados previamente
 - 8. Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
 - 9. Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
 - 10. Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
 - 11. Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
 - 12. Determinación de la probabilidad e impacto de materialización de los escenarios
 - 13. Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
 - 14. Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
 - 15. Relación de las distintas alternativas de gestión de riesgos
 - 16. Guía para la elaboración del plan de gestión de riesgos
 - 17. Exposición de la metodología NIST SP 800
 - 18. Exposición de la metodología Magerit

UNIDAD DIDÁCTICA 10. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

- 1. Herramientas del sistema operativo tipo Ping, Traceroute, etc
- 2. Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc
- 3. Herramientas de análisis de vulnerabilidades tipo Nessus
- 4. Analizadores de protocolos tipo Wireshark, DSniff, Cain & Abel, etc
- 5. Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc
- 6. Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc

UNIDAD DIDÁCTICA 11. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS

- 1. Principios generales de cortafuegos
- 2. Componentes de un cortafuegos de red
- 3. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
- 4. Arquitecturas de cortafuegos de red
- 5. Otras arquitecturas de cortafuegos de red

UNIDAD DIDÁCTICA 12. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

- 1. Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada
- 2. Guía para la elaboración del plan de auditoría
- 3. Guía para las pruebas de auditoría
- 4. Guía para la elaboración del informe de auditoría

MÓDULO 4. LEGISLACIÓN NACIONAL APLICABLE AL SECTOR DEL PERITAJE

[Ver en la web](#)

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

