Curso Superior en Ciberseguridad desde el Punto de Vista Empresarial y Técnico + 16 Créditos ECTS

Elige aprender en la escuela
líder en formación para profesionales

ÍNDICE

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.**

Curso Superior en Ciberseguridad desde el Punto de Vista Empresarial y Técnico + 16 Créditos ECTS

DURACIÓN
400 horas

MODALIDAD
ONLINE

ACOMPAÑAMIENTO
PERSONALIZADO

CREDITOS
16 ECTS

Titulación

Titulación de Curso Superior en Ciberseguridad desde el Punto de Vista Empresarial y Técnico con 400 horas y 16 ECTS expedida por UTAMED - Universidad Tecnológica Atlántico Mediterráneo.

Ver en la web

inesem formación continua

Descripción

La creciente presencia de la tecnología en nuestro entorno es un hecho indiscutible, ante esta situación surge la necesidad de mantener seguros todos los activos informáticos en las empresas y organizaciones. La seguridad informática se ha convertido en una de las principales preocupaciones de las empresas. Con este Curso de Ciberseguridad desde el punto de vista empresarial y técnico te convertirás el profesional que las empresas necesitan, conocerás las infraestructuras de protección contra incidentes de seguridad y aprenderás gestionarlas de la manera más eficaz, también conocer los ataques más comunes y como proteger un sistema ante estos ataques. Además, contarás con un equipo de profesionales especializados en la materia.

Objetivos

- Comprender los principios básicos de la seguridad informática.
- Asimilar la normativa de aplicación sobre el SGSI.
- Reconocer las vulnerabilidades y los posibles ataques a las redes y a los sistemas libres.
- Conocer los principales sistemas para la protección de la información en las redes y sistemas telemáticos.
- Dominar el proceso de notificación y gestión de intentos de intrusión.
- Saber cómo llevar a cabo un análisis forense informático.

Ver en la web

Para qué te prepara

El Curso de Ciberseguridad desde el punto de vista empresarial y técnico está dirigido a titulados y estudiantes en informática, telecomunicaciones, ingeniería de las tecnologías o cualquier profesional que quieran reforzar sus conocimientos en el área de la Ciberseguridad. También para quien quiera empezar en Ciberseguridad porque empieza desde las nociones básicas.

A quién va dirigido

El Curso de Ciberseguridad desde el punto de vista empresarial y técnico te prepara para proteger a las empresas de los problemas de seguridad que no paran de aparecer en la sociedad que nos encontramos ahora, con lo que crearás medidas de seguridad y usarás herramientas IPS/IDS para proteger los sistemas de las empresas además de tener en cuenta las metodologías recomendadas para trabajar de la forma más eficaz

Salidas laborales

Una vez finalizado este Curso de Ciberseguridad desde el punto de vista empresarial y técnico podrás desempeñarte en el área de la ciberseguridad como Auditor en ciberseguridad, consultor especializado en ciberseguridad, director en ciberseguridad. En general para las empresas que requieran servicios para proteger sus sistemas o tener en cuenta la normativa.

TEMARIO

MÓDULO 1. CIBERSEGURIDAD: GESTIÓN Y HERRAMIENTAS

UNIDAD DIDÁCTICA 1. GESTIÓN Y HERRAMIENTAS DE CIBERSEGURIDAD: INTRODUCCIÓN Y CONCEPTOS BÁSICOS

1. La sociedad de la información
    1. - ¿Qué es la seguridad de la información?
    2. - Importancia de la seguridad de la información
2. Seguridad de la información: Diseño, desarrollo e implantación
    1. - Descripción de los riesgos de la seguridad
    2. - Selección de controles
3. Factores de éxito en la seguridad de la información
4. Vídeo tutorial: relación entre la ciberseguridad y el Big Data

UNIDAD DIDÁCTICA 2. NORMATIVA SOBRE EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

1. Estándares y Normas Internacionales sobre los SGSI
    1. - Familia de Normas ISO 27000
    2. - La Norma UNE-EN-ISO/IEC 27001:2014
    3. - Buenas prácticas en seguridad de la información, Norma ISO/IEC 27002
2. Normativa aplicable a los SGSI
    1. - Normativa comunitaria sobre seguridad de la información
    2. - Legislación Española sobre seguridad de la información
    3. - El Instituto Nacional de Ciberseguridad (INCIBE)

UNIDAD DIDÁCTICA 3. POLÍTICA DE SEGURIDAD: ANÁLISIS Y GESTIÓN DE RIESGOS

1. Plan de implantación del SGSI
2. Análisis de riesgos
    1. - Análisis de riesgos: Aproximación
    2. - Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su 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
    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 800-30
18. - Exposición de la metodología Magerit

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. AUDITORÍA DE CIBERSEGURIDAD

1. Criterios Generales en la Auditoría de Seguridad de la Informática
    1. - Código deontológico de la función de auditoría
    2. - Relación de los distintos tipos de auditoría en el marco de los sistemas de información
    3. - Criterios a seguir para la composición del equipo auditor
    4. - Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
    5. - Tipos de muestreo a aplicar durante el proceso de auditoría
    6. - Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
    7. - Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
    8. - Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
    9. - Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas
2. Aplicación de la normativa de protección de datos de carácter personal
    1. - Normativa de referencia: Reglamento General de Protección de Datos y Ley Orgánica de Protección de Datos 3/2018
    2. - Principios generales de la protección de datos de carácter personal
    3. - Legitimación para el tratamiento de datos personales
    4. - Medidas de responsabilidad proactiva
    5. - Los derechos de los interesados
    6. - Delegado de Protección de Datos
3. 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.
4. Descripción de los aspectos sobre cortafuego en auditorías de sistemas de información
    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. Guías para la ejecución de las distintas fases de la auditoría de sistemas de información
    1. - Normas para la implantación de la auditoría de la documentación
    2. - Instrucciones para la elaboración del plan de auditoría
    3. - Pruebas de auditoría
    4. - Instrucciones para la elaboración del informe de auditoría

UNIDAD DIDÁCTICA 5. COMUNICACIONES SEGURAS: SEGURIDAD POR NIVELES

1. Seguridad a nivel físico
    1. - Tipos de ataques
    2. - Servicios de Seguridad
    3. - Medidas de seguridad a adoptar
2. Seguridad a nivel de enlace
    1. - Tipos de ataques
    2. - Medidas de seguridad a adoptar
3. Seguridad a nivel de red
    1. - Datagrama IP
    2. - Protocolo IP
    3. - Protocolo ICMP
    4. - Protocolo IGMP
    5. - Tipos de Ataques
    6. - Medidas de seguridad a adopta
4. Seguridad a nivel de transporte
    1. - Protocolo TCP
    2. - Protocolo UDP
    3. - Tipos de Ataques
    4. - Medidas de seguridad a adoptar
5. Seguridad a nivel de aplicación
    1. - Protocolo DNS
    2. - Protocolo Telnet
    3. - Protocolo FTP
    4. - Protocolo SSH
    5. - Protocolo SMTP
    6. - Protocolo POP
    7. - Protocolo IMAP
    8. - Protocolo SNMP
    9. - Protocolo HTTP
    10. - Tipos de Ataques
    11. - Medidas de seguridad a adoptar

MÓDULO 2. CIBERSEGURIDAD: 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
    1. - Respaldo y recuperación de los datos
    2. - Actualización del Plan de Recuperación
    3. - Errores comunes al formular un DRP
6. Proceso para la comunicación del incidente a terceros

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE INFORMÁTICO

1. Conceptos generales y objetivos del análisis forense
    1. - Tipos de análisis forense
2. Exposición del Principio de Lockard
3. Guía para la recogida de evidencias electrónicas

1. - Evidencias volátiles y no volátiles
2. - Etiquetado de evidencias
3. - Cadena de custodia
4. - Ficheros y directorios ocultos
5. - Información oculta del sistema
6. - Recuperación de ficheros borrados

4. Guía para el análisis de las evidencias electrónicas recogidas
5. Guía para la selección de las herramientas de análisis forense

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