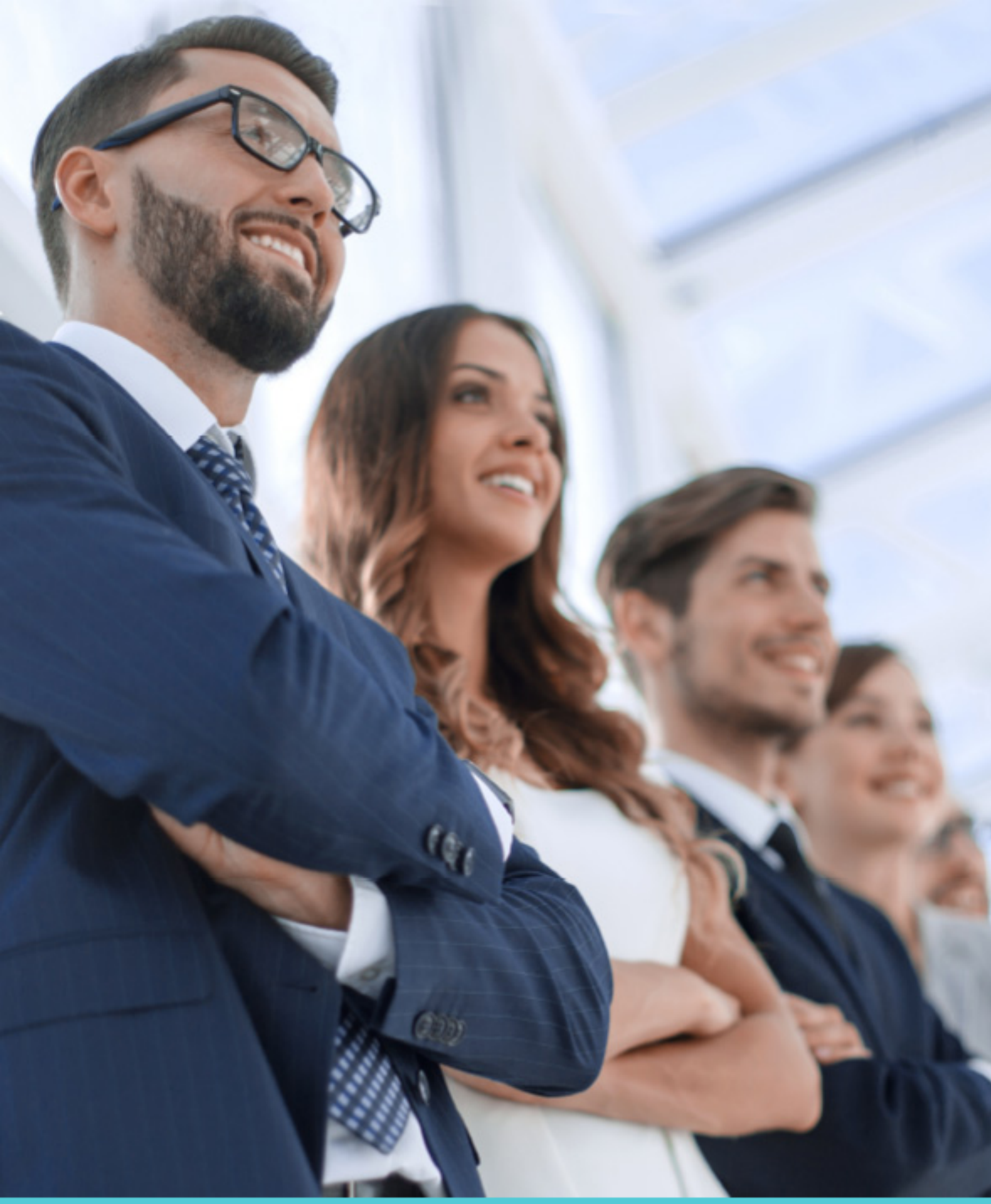
Máster en Ciberseguridad + 60 Créditos ECTS



Elige aprender en la escuela
líder en formación para profesionales

ÍNDICE

Ver en la web

inesem formación continua

SOMOS INESEM

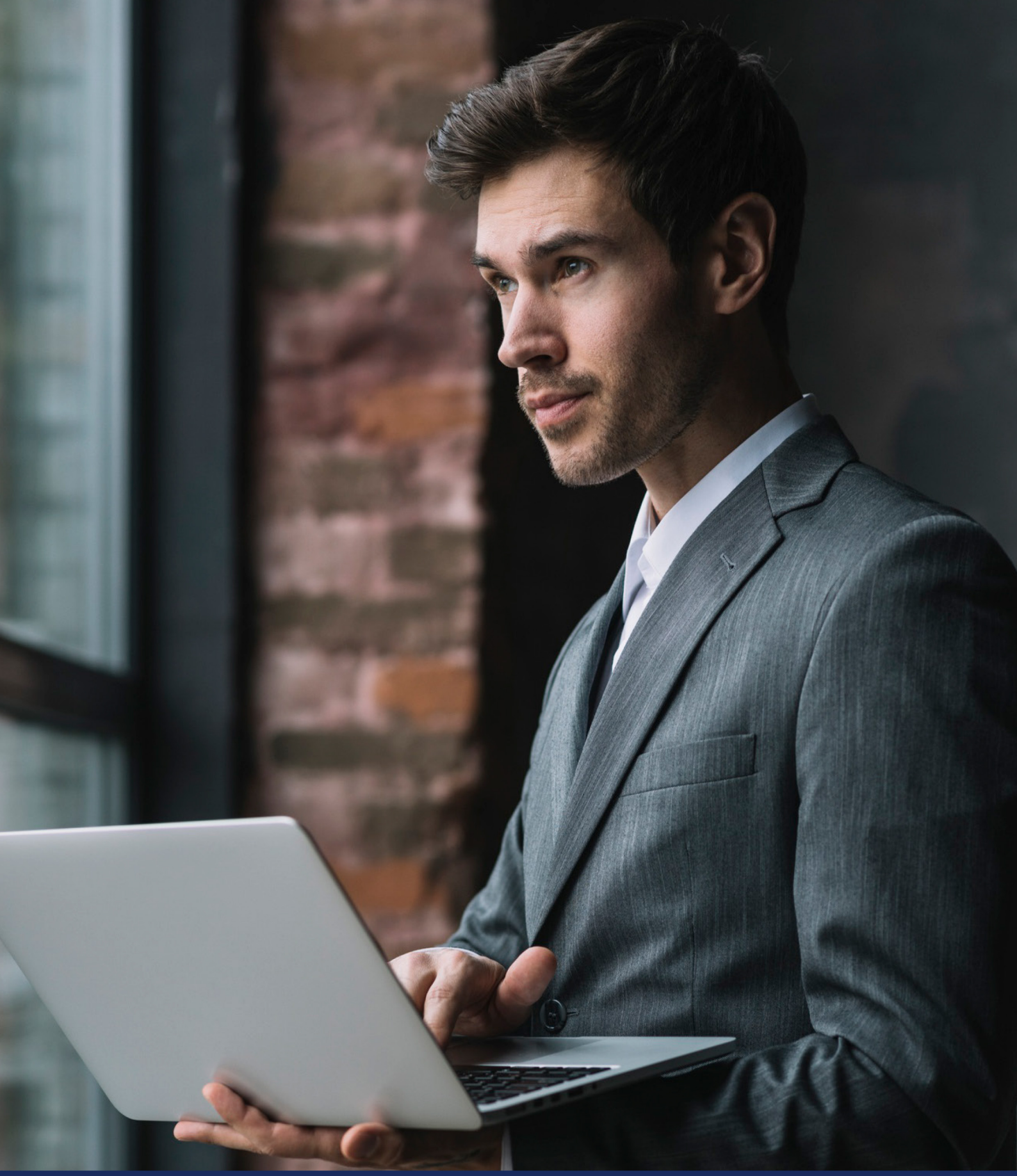
INESEM es una **Business School online** especializada con un fuerte sentido transformacional. En un mundo cambiante donde la tecnología se desarrolla a un ritmo vertiginoso nosotros somos activos, evolucionamos y damos respuestas a estas situaciones.

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

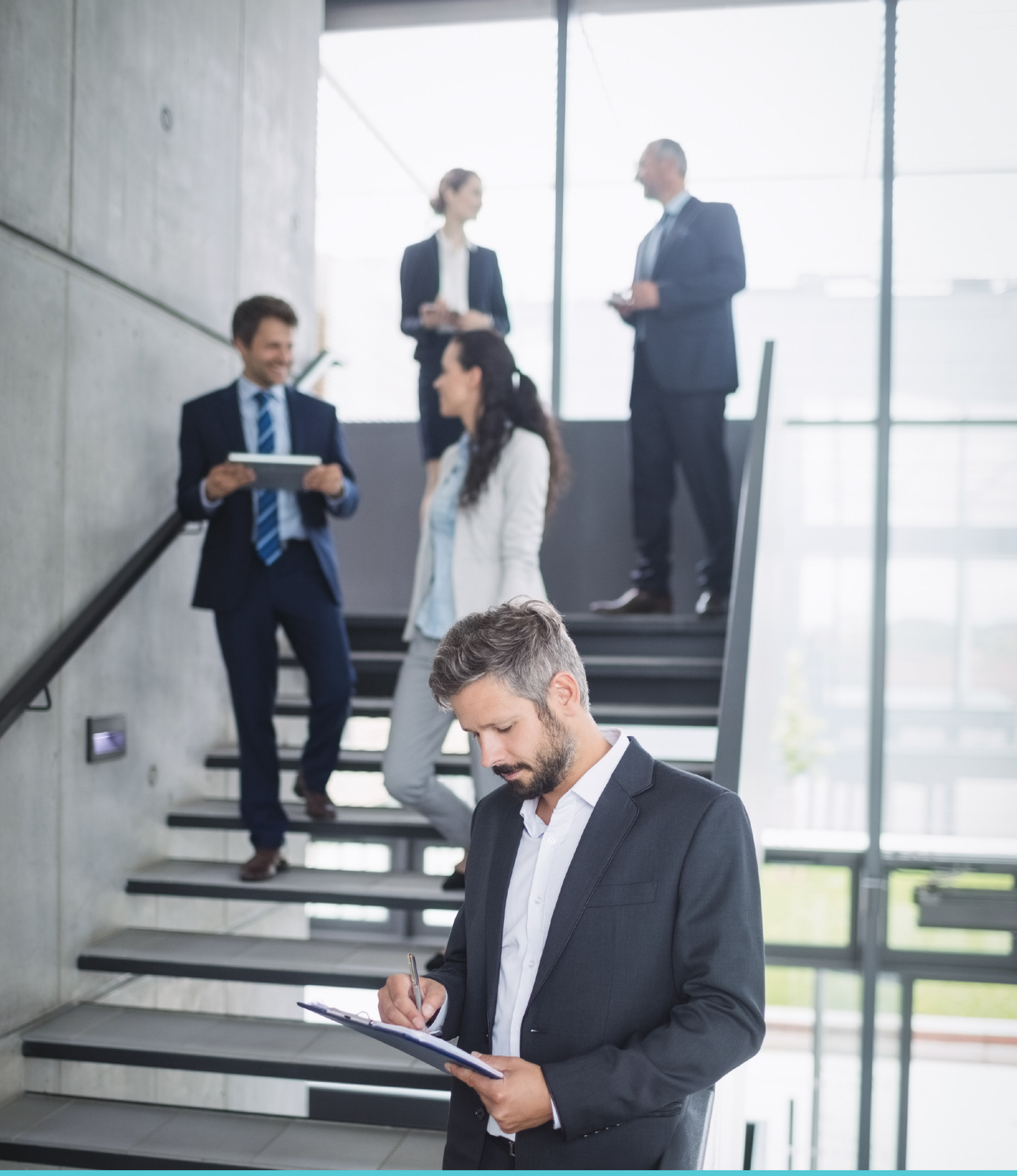
Ver en la web

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

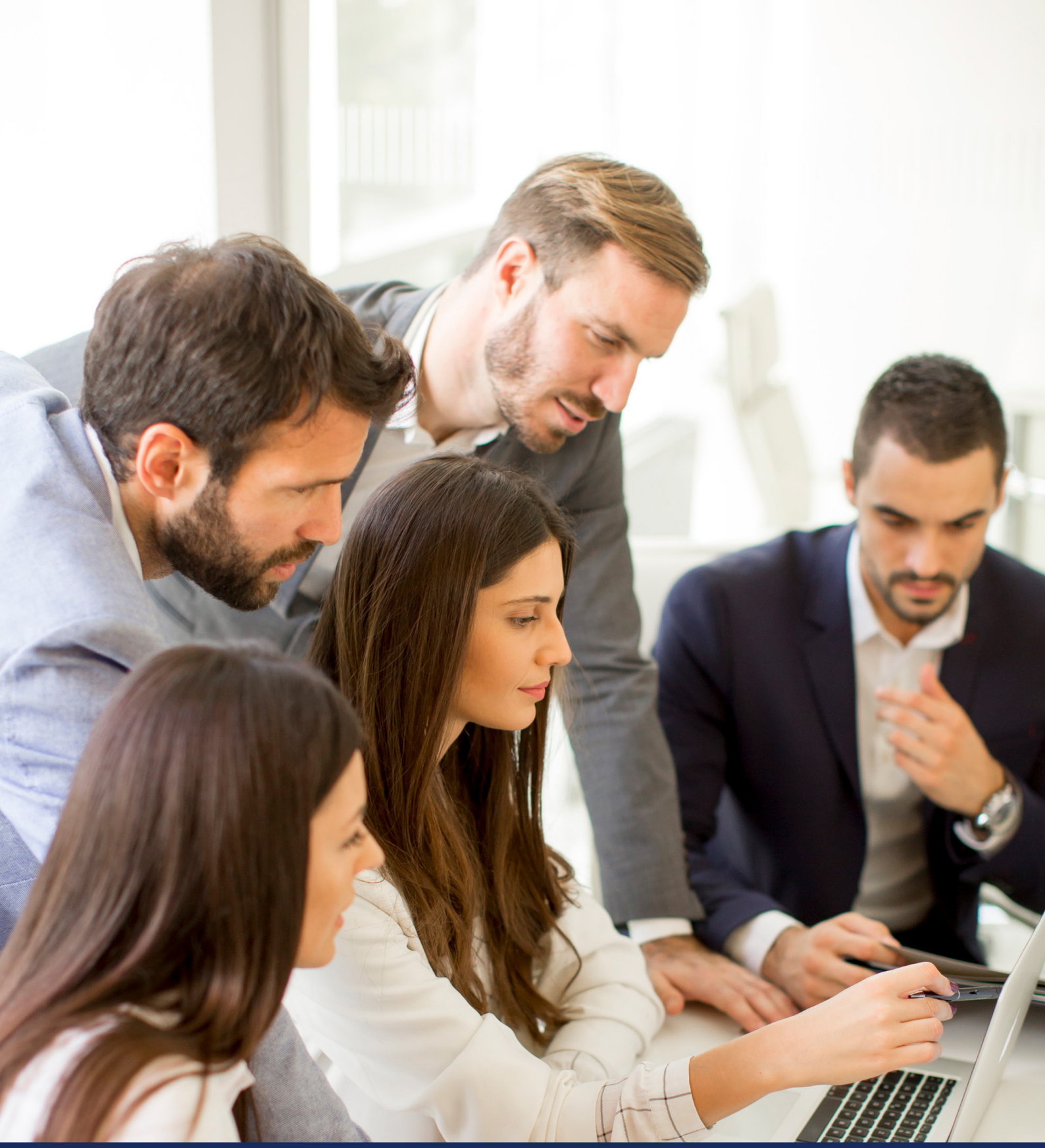
Orientación académica por parte de un equipo docente especialista en su área de conocimiento, que aboga por la calidad educativa adaptando los procesos a las necesidades del mercado laboral.

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.**

Máster en Ciberseguridad + 60 Créditos ECTS

DURACIÓN
1500 horas

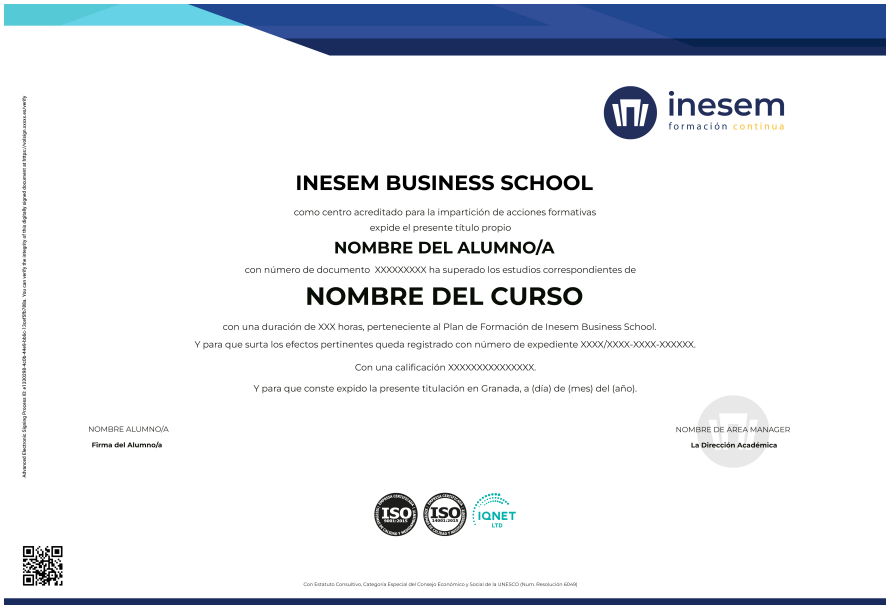
MODALIDAD
ONLINE

ACOMPAÑAMIENTO
PERSONALIZADO

CREDITOS
60 ECTS

Titulación

Titulación de Máster de Formación Permanente en Ciberseguridad con 1500 horas y 60 ECTS expedida por UTAMED - Universidad Tecnológica Atlántico Mediterráneo.



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 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 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

La ciberseguridad es una prioridad para las empresas y en la vida privada de las personas debido al aumento exponencial de datos en internet y ciberataques cada vez más avanzados. Con este Máster en Ciberseguridad aprenderás los principales estándares, protocolos y herramientas utilizados para securizar sistemas. Podrás detectar, analizar y anticiparte a ciberataques y realizar auditorías informáticas. Utilizarás las principales herramientas OSINT y sabrás aplicar ingeniería inversa. Aprenderás las principales técnicas y fases del hacking ético y entrenarás en plataformas como Hack the Box (HTB), Tryhackme o Vulnhub. Contarás con un equipo de profesionales especializados en la materia. Además, gracias a las prácticas garantizadas, podrás acceder a un mercado laboral en plena expansión.

Objetivos

- Conocer la legislación, normativa y políticas aplicables a los Sistemas de gestión de la seguridad de la información.
- Descubrir posibles fallos de seguridad en cada uno de los niveles de comunicación y utilizar sistemas IDS/IPS y SIEM.
- Entender para qué sirve el cracking y la criptografía y cómo se puede realizar la ingeniería inversa.
- Saber qué es el Hacking ético, cuáles son sus diferentes fases y poder realizar auditorías informáticas.
- Entrenar las habilidades y técnicas de hacker ético en plataformas como Hack the Box (HTB), Tryhackme o Vulnhub.
- Utilizar herramientas OSINT como Google Dork, Shodan, Maltego, The Harvester, Creepy o Foca.
- Aplicar las guías de desarrollo, testing y revisión de código de OWASP para garantizar la seguridad en desarrollo web.

Para qué te prepara

El Máster en Ciberseguridad está especialmente enfocado a ingenieros informáticos, administradores de sistemas o en general profesionales del sector informático que busquen una formación actualizada en las técnicas, herramientas, políticas y normativas más utilizadas para garantizar la seguridad de los sistemas informáticos y evitar ciberataques e incidentes de seguridad.

A quién va dirigido

Con este Máster en Ciberseguridad aprenderás los principales estándares, protocolos y herramientas utilizados para securizar sistemas. Podrás detectar, analizar y anticiparte a ciberataques y realizar auditorías informáticas. Utilizarás las principales herramientas OSINT y sabrás aplicar ingeniería inversa. Aprenderás las principales técnicas y fases del hacking ético y entrenarás en plataformas

como Hack the Box (HTB), Tryhackme o Vulnhub.

Salidas laborales

La ciberseguridad es un campo profesional con gran demanda laboral, con multitud de perfiles profesionales a cubrir y que conlleva una gran responsabilidad. Gracias a este Máster en Ciberseguridad optarás a puestos como Chief Security Officer (CSO), Data Protection Officer (DPO), Auditor de sistemas, Consultor de ciberseguridad, Hacker ético o Experto en desarrollo web seguro.

TEMARIO

MÓDULO 1. CIBERSEGURIDAD: NORMATIVA, POLÍTICA DE SEGURIDAD Y CIBERINTELIGENCIA

UNIDAD DIDÁCTICA 1. CIBERSEGURIDAD Y SOCIEDAD DE LA INFORMACIÓN

1. ¿Qué es la ciberseguridad?
2. La sociedad de la información
3. Diseño, desarrollo e implantación
4. Factores de éxito en la seguridad de la información
5. Soluciones de Ciberseguridad y Ciberinteligencia CCN-CERT

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

1. Estándares y Normas Internacionales sobre los SGSI. ISO 2. Legislación: Leyes aplicables a los SGSI

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

1. Plan de implantación del SGSI
2. Análisis de riesgos
3. Gestión de riesgos

UNIDAD DIDÁCTICA 4. 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 a Phising
7. Phising
8. Man In The Middle

UNIDAD DIDÁCTICA 5. CIBERINTELIGENCIA Y CIBERSEGURIDAD

1. Ciberinteligencia
2. Herramientas y técnicas de ciberinteligencia
3. Diferencias entre ciberinteligencia y ciberseguridad
4. Amenazas de ciberseguridad

UNIDAD DIDÁCTICA 6. MÉTODOS DE INTELIGENCIA DE OBTENCIÓN DE INFORMACIÓN

1. Contextualización
2. OSINT
3. HUMINT
4. IMINT

5. Otros métodos de inteligencia para la obtención de información

UNIDAD DIDÁCTICA 7. CIBERINTELIGENCIA Y TECNOLOGÍAS EMERGENTES

1. Tecnologías emergentes
2. Desafíos y oportunidades de la ciberinteligencia en las tecnologías emergentes
3. Análisis de amenazas avanzado
4. Usos de las tecnologías emergentes en la ciberinteligencia

MÓDULO 2. REDES INFORMÁTICAS: ARQUITECTURA, PROTOCOLOS Y CIBERSEGURIDAD

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LA RED

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

UNIDAD DIDÁCTICA 2. ESTANDARIZACIÓN DE PROTOCOLOS

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

UNIDAD DIDÁCTICA 3. 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 4. 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 5. 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 6. 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 7. REDES MAN Y WAN, PROTOCOLOS

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

UNIDAD DIDÁCTICA 8. 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 9. PROTECCIÓN DE UNA RED

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

UNIDAD DIDÁCTICA 10. REPARACIÓN DE RED

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

UNIDAD DIDÁCTICA 11. COMUNICACIONES SEGURAS: SEGURIDAD POR NIVELES

1. Seguridad a Nivel Físico
2. Seguridad a Nivel de Enlace
3. Seguridad a Nivel de Red
4. Seguridad a Nivel de Transporte
5. Seguridad a Nivel de Aplicación

UNIDAD DIDÁCTICA 12. APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

1. Identificación de los componente de una PKI y sus modelos de relaciones
2. Autoridad de certificación y sus elementos
3. Política de certificado y declaración de prácticas de certificación (CPS)
4. Lista de certificados revocados (CRL)
5. Funcionamiento de las solicitudes de firma de certificados (CSR)
6. Infraestructuras de gestión de privilegios (PMI)

7. Campos de certificados de atributos
8. Aplicaciones que se apoyan en la existencia de una PKI

UNIDAD DIDÁCTICA 13. 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 14. 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 15. INTRODUCCIÓN A LOS SISTEMAS SIEM

1. ¿Qué es un SIEM?
2. Evolución de los sistemas SIEM: SIM, SEM y SIEM
3. Arquitectura de un sistema SIEM

UNIDAD DIDÁCTICA 16. CAPACIDADES DE LOS SISTEMAS SIEM

1. Problemas a solventar
2. Administración de logs
3. Regulaciones IT
4. Correlación de eventos
5. Soluciones SIEM en el mercado

MÓDULO 3. CRIPTOGRAFÍA Y REDES PRIVADAS VIRTUALES (VPN)

UNIDAD DIDÁCTICA 1. HISTORIA Y EVOLUCIÓN DE LA CRIPTOGRAFÍA

1. La criptografía a lo largo de la historia
2. El nacimiento del criptoanálisis
3. La criptografía en nuestros tiempos
4. Criptografía en el futuro

UNIDAD DIDÁCTICA 2. SEGURIDAD INFORMÁTICA Y CRIPTOGRAFÍA

1. Seguridad Informática
2. Uso de seguridad informática y criptografía
3. Tipo de amenazas
4. Respuesta ante un ataque
5. Amenazas del futuro

UNIDAD DIDÁCTICA 3. CRIPTOGRAFÍA SIMÉTRICA Y CRIPTOGRAFÍA ASIMÉTRICA

1. Criptografía simétrica
2. Criptografía asimétrica
3. Criptografía híbrida
4. Criptografía y seguridad informática: El Ciclo de vida de las claves y contraseñas

UNIDAD DIDÁCTICA 4. CRIPTOGRAFÍA DE CLAVE PRIVADA

1. Cifrado de clave privada
2. Cifrado DES
3. Función F

UNIDAD DIDÁCTICA 5. CRIPTOGRAFÍA DE CLAVE PÚBLICA

1. Cifrado de clave pública
2. PKC como herramienta de cifrado
3. Uso en Generación de Firmas Dígitales
4. Aplicaciones de la criptografía pública y privada
5. Certificado dígital
6. DNI Electrónico
7. Bitcoin

UNIDAD DIDÁCTICA 6. PROTOCOLOS CRIPTOGRÁFICOS Y FIRMAS DIGITALES

1. Protocolo criptográfico
2. Protocolo criptográfico avanzado
3. Firma segura hacia delante

UNIDAD DIDÁCTICA 7. APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

1. Identificación de los componentes de una PKI y sus modelos de relaciones
2. Autoridad de certificación y sus elementos
3. Política de certificado y declaración de prácticas de certificación (CPS)
4. Lista de certificados revocados (CRL)
5. Funcionamiento de las solicitudes de firma de certificados (CSR)
6. Infraestructuras de gestión de privilegios (PMI)
7. Campos de certificados de atributos
8. Aplicaciones que se apoyan en la existencia de una PKI

UNIDAD DIDÁCTICA 8. HASHING

UNIDAD DIDÁCTICA 9. TIPOS DE ALGORITMOS Y CIFRADOS CRIPTOGRÁFICOS

1. Métodos criptográficos históricos
2. Challenge Handshake Authentication Protocol (CHAP)
3. Federal Information Processing Standards (FIPS)
4. Private Communication Technology (PCT)
5. Secure Electronic Transaction (SET)
6. Secure Sockets Layer (SSL)

7. Simple Key Management for Internet Protocol (SKIP)
8. IP Security Protocol (IPSec)

UNIDAD DIDÁCTICA 10. HERRAMIENTAS CRIPTOGRÁFICAS Y EJEMPLOS DE USO

1. Herramientas Criptográficas de Microsoft
2. CrypTool-Online (CTO)
3. Java Cryptographic Architecture (JCA)
4. GNU Privacy Guard
5. Whisply
6. DiskCryptor
7. AES Crypt
8. Ejemplos criptográficos en Python

UNIDAD DIDÁCTICA 11. INTRODUCCIÓN A LAS REDES PRIVADAS VIRTUALES (VPN)

1. ¿Qué son las redes privadas virtuales o VPN?
2. Bloques de construcción de VPN
3. Tecnologías VPN, Topología y Protocolos
4. VPN vs IP móvil

UNIDAD DIDÁCTICA 12. ARQUITECTURAS VPN

1. Requisitos y arquitecturas VPN
2. Arquitecturas VPN basadas en seguridad y en capas
3. VPN de acceso remoto y extranet

UNIDAD DIDÁCTICA 13. PROTOCOLOS DE TUNELIZACIÓN VPN

1. PPTP
2. L2TP
3. L2F
4. IPSec
5. MPLS

UNIDAD DIDÁCTICA 14. AUTENTICACIÓN Y CONTROL DE ACCESO EN VPN

1. Autenticación PPP
2. RADIO y Kerberos
3. Autenticación de VPN
4. Control de acceso en VPN

UNIDAD DIDÁCTICA 15. GESTIÓN DE SERVICIOS Y REDES VPN

1. Protocolos y arquitectura de gestión de red
2. Gestión de servicios VPN
3. Centros de operaciones de red (NOC)
4. Redundancia y equilibrio de carga

MÓDULO 4. MALWARE E INGENIERÍA INVERSA

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN AL ANÁLISIS DE MALWARE

UNIDAD DIDÁCTICA 2. TÉCNICAS Y HERRAMIENTAS PARA ANÁLISIS DE MALWARE

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. FUNDAMENTOS DE LA INGENIERÍA INVERSA

1. Concepto de Ingeniería Inversa
2. Características de la Ingeniería Inversa
3. Ventajas del uso de Ingeniería Inversa

UNIDAD DIDÁCTICA 5. TIPOS DE INGENIERÍA INVERSA

1. Ingeniería inversa de datos
2. Ingeniería inversa de lógica o proceso
3. Ingeniería inversa de interfaces de usuario

UNIDAD DIDÁCTICA 6. HERRAMIENTAS DE INGENIERÍA INVERSA

1. Ghidra
2. IDA
3. Winhex
4. Hiew
5. x64dbg
6. Radare2
7. Cutter

UNIDAD DIDÁCTICA 7. INTRODUCCIÓN AL CRACKING

UNIDAD DIDÁCTICA 8. HERRAMIENTAS DE CRACKING

1. Depuradores
2. Desensambladores
3. Compiladores Inversos o Decompiladores

MÓDULO 5. HERRAMIENTAS DE CIBERSEGURIDAD OSINT

UNIDAD DIDÁCTICA 1. QUÉ SON LAS HERRAMIENTAS OSINT

1. Introducción

UNIDAD DIDÁCTICA 2. GOOGLE DORK

1. Qué es Google Dork
2. Uso y aplicación de Google Dork

UNIDAD DIDÁCTICA 3. SHODAN

1. Qué es Shodan
2. Uso y aplicación de Shodan

UNIDAD DIDÁCTICA 4. MALTEGO

1. Qué es Maltego
2. Uso y aplicación de Maltego

UNIDAD DIDÁCTICA 5. THE HARVESTER

1. Qué es The Harvester
2. Uso y aplicación de The Harvester

UNIDAD DIDÁCTICA 6. RECON-NG

1. Qué es Recon-ng
2. Uso y aplicación de Recon-ng

UNIDAD DIDÁCTICA 7. CREEPY

1. Qué es Creepy
2. Uso y aplicación de Creepy

UNIDAD DIDÁCTICA 8. FOCA

1. Qué es Foca
2. Uso y aplicación de Foca

MÓDULO 6. PENTESTING Y HACKING TOOLS

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN AL HACKING ÉTICO

1. ¿Qué es el hacking ético?
2. Aspectos legales del hacking ético
3. Perfiles del hacker ético

UNIDAD DIDÁCTICA 2. FASES DEL HACKING ÉTICO EN LOS ATAQUES A SISTEMAS Y REDES

1. Tipos de ataques
2. Herramientas de hacking ético
3. Tests de vulnerabilidades

UNIDAD DIDÁCTICA 3. FASES DEL HACKING ÉTICO EN LOS ATAQUES A REDES WIFI

1. Tipos de ataques
2. Herramientas de hacking ético
3. Tipos de seguridad WiFi
4. Sniffing

UNIDAD DIDÁCTICA 4. FASES DEL HACKING ÉTICO EN LOS ATAQUES WEB

1. Tipos de ataques
2. Herramientas de hacking ético
3. Tipos de seguridad web
4. Tipo de test de seguridad en entornos web

UNIDAD DIDÁCTICA 5. KALI LINUX

UNIDAD DIDÁCTICA 6. NMAP

UNIDAD DIDÁCTICA 7. METASPLOIT

UNIDAD DIDÁCTICA 8. WIRESHARK

UNIDAD DIDÁCTICA 9. JOHN THE RIPPER

UNIDAD DIDÁCTICA 10. HASHCAT

UNIDAD DIDÁCTICA 11. HYDRA

UNIDAD DIDÁCTICA 12. BURP SUITE

UNIDAD DIDÁCTICA 13. ZED ATTACK PROXY

UNIDAD DIDÁCTICA 14. SQLMAP

UNIDAD DIDÁCTICA 15. AIRCRACK-NG

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. ANÁLISIS FORENSE

UNIDAD DIDÁCTICA 1. 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 2. 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 3. 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

UNIDAD DIDÁCTICA 4. 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 5. AUDITORÍA DE SEGURIDAD INFORMÁTICA

1. Criterios Generales
2. Aplicación de la normativa de protección de datos de carácter personal
3. Herramientas para la auditoría de sistemas
4. Descripción de los aspectos sobre cortafuego en auditorías de sistemas de información
5. Guías para la ejecución de las distintas fases de la auditoría de sistemas de información

MÓDULO 9. DESARROLLO WEB SEGURO

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LA SEGURIDAD WEB

1. ¿Qué es la seguridad web?
2. Amenazas para un sitio web
3. Consejos para mantener un sitio web seguro
4. Otros consejos de seguridad web
5. Proveedores de alojamiento web seguros

UNIDAD DIDÁCTICA 2. OWASP DEVELOPMENT

1. ¿Qué es OWASP? ¿Y OWASP Development?
2. ¿Qué es ASVS?
3. Uso del ASVS
4. Requisitos de arquitectura, diseño y modelado de amenazas
5. Requisitos de verificación de autenticación
6. Requisitos de verificación de gestión de sesión
7. Requisitos de verificación de control de acceso
8. Requisitos de validación, desinfección y verificación de la codificación
9. Requisitos de verificación de criptografía almacenados
10. Requisitos de manejo de verificaciones y registro de errores

11. Requisitos de verificación de protección de datos
12. Requisitos de verificación de comunicaciones
13. Requisitos de verificación de código malicioso
14. Requisitos de verificación de lógica de negocios
15. Requisitos de verificación de archivos y recursos
16. Requisitos de verificación de API y servicio web
17. Requisitos de verificación de configuración
18. Requisitos de verificación de Internet de las Cosas
19. Glosario de términos

UNIDAD DIDÁCTICA 3. OWASP TESTING GUIDE

1. Aspectos introductorios
2. La Guía de Pruebas de OWASP
3. El framework de pruebas de OWASP
4. Pruebas de seguridad de aplicaciones web
5. Reportes de las pruebas

UNIDAD DIDÁCTICA 4. OWASP CODE REVIEW

1. Aspectos introductorios
2. Revisión de código seguro
3. Metodología

UNIDAD DIDÁCTICA 5. OWASP TOP TEN

1. Broken Access Control - Control de acceso roto (A01:2021)
2. Cryptographic Failures - Fallos criptográficos (A02:2021)
3. Injection - Inyección (A03:2021)
4. Insecure Design - Diseño Inseguro (A04:2021)
5. Security Misconfiguration - Configuración incorrecta de seguridad (A05:2021)
6. Vulnerable and Outdated Components - Componentes vulnerables y obsoletos (A06:2021)
7. Identification and Authentication Failures - Fallos de Identificación y Autenticación (A07:2021)
8. Software and Data Integrity Failures - Fallos de integridad de software y datos (A08:2021)
9. Security Logging and Monitoring Failures - Registro de seguridad y fallos de monitoreo (A09:2021)
10. Server-Side Request Forgery (SSRF) - Falsificación de solicitud del lado del servidor (A10:2021)

MÓDULO 10. CIBERSEGURIDAD APLICADA A INTELIGENCIA ARTIFICIAL (IA), SMARTPHONES, INTERNET DE LAS COSAS (IOT) E INDUSTRIA 4.0

UNIDAD DIDÁCTICA 1. CIBERSEGURIDAD EN NUEVAS TECNOLOGÍAS

1. Concepto de seguridad TIC
2. Tipos de seguridad TIC
3. Aplicaciones seguras en Cloud
4. Plataformas de administración de la movilidad empresarial (EMM)
5. Redes WiFi seguras
6. Caso de uso: Seguridad TIC en un sistema de gestión documental

UNIDAD DIDÁCTICA 2. CIBERSEGURIDAD EN SMARTPHONES

1. Buenas prácticas de seguridad móvil
2. Protección de ataques en entornos de red móv

UNIDAD DIDÁCTICA 3. INTELIGENCIA ARTIFICIAL (IA) Y CIBERSEGURIDAD

1. Inteligencia Artificial
2. Tipos de inteligencia artificial
3. Impacto de la Inteligencia Artificial en la ciberseguridad

UNIDAD DIDÁCTICA 4. CIBERSEGURIDAD E INTERNET DE LAS COSAS (IOT)

1. Contexto Internet de las Cosas (IoT)
2. ¿Qué es IoT?
3. Elementos que componen el ecosistema IoT
4. Arquitectura IoT
5. Dispositivos y elementos empleados
6. Ejemplos de uso
7. Retos y líneas de trabajo futuras
8. Vulnerabilidades de IoT
9. Necesidades de seguridad específicas de IoT

UNIDAD DIDÁCTICA 5. SEGURIDAD INFORMÁTICA EN LA INDUSTRIA 4.0

1. Industria 4.0
2. Necesidades en ciberseguridad en la Industria 4.0

MÓDULO 11. 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