



Masters Profesionales

Master en Ciberseguridad



INESEM
BUSINESS SCHOOL

INESEM BUSINESS SCHOOL

Índice

Master en Ciberseguridad

1. Sobre Inesem

2. Master en Ciberseguridad

[Descripción](#) / [Para que te prepara](#) / [Salidas Laborales](#) / [Resumen](#) / [A quién va dirigido](#) /

[Objetivos](#)

3. Programa académico

4. Metodología de Enseñanza

5. ¿Porqué elegir Inesem?

6. Orientacion

7. Financiación y Becas

SOBRE INESEM BUSINESS SCHOOL



INESEM Business School como Escuela de Negocios Online tiene por objetivo desde su nacimiento trabajar para fomentar y contribuir al desarrollo profesional y personal de sus alumnos. Promovemos ***una enseñanza multidisciplinar e integrada***, mediante la aplicación de ***metodologías innovadoras de aprendizaje*** que faciliten la interiorización de conocimientos para una aplicación práctica orientada al cumplimiento de los objetivos de nuestros itinerarios formativos.

En definitiva, en INESEM queremos ser el lugar donde te gustaría desarrollar y mejorar tu carrera profesional. ***Porque sabemos que la clave del éxito en el mercado es la "Formación Práctica" que permita superar los retos que deben de afrontar los profesionales del futuro.***

Master en Ciberseguridad



DURACIÓN	1500
PRECIO	1795 €
MODALIDAD	Online

Entidad impartidora:



INESEM
BUSINESS SCHOOL

Programa de Becas / Financiación 100% Sin Intereses

Titulación Masters Profesionales

- 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.”

Resumen

En torno a esta nueva era donde el Cloud Computing y la continua transmisión de datos en red es algo más que habitual en las empresas, no es raro encontrar noticias de ataques cibernéticos, generando la importancia de la seguridad de la información que exige profesionales informáticos con conocimientos actualizados. Con esta acción formativa se cubren los objetivos y técnicas de ciberseguridad que debe manejar un buen profesional de la seguridad informática, teniendo en cuenta cuestiones como la normativa, protocolos y herramientas para salvaguardar la información de una entidad. En INESEM podrás trabajar en un Entorno Personal de Aprendizaje donde el alumno es el protagonista, avalado por un amplio grupo de tutores especialistas en el sector y respaldado por entidades de prestigio.

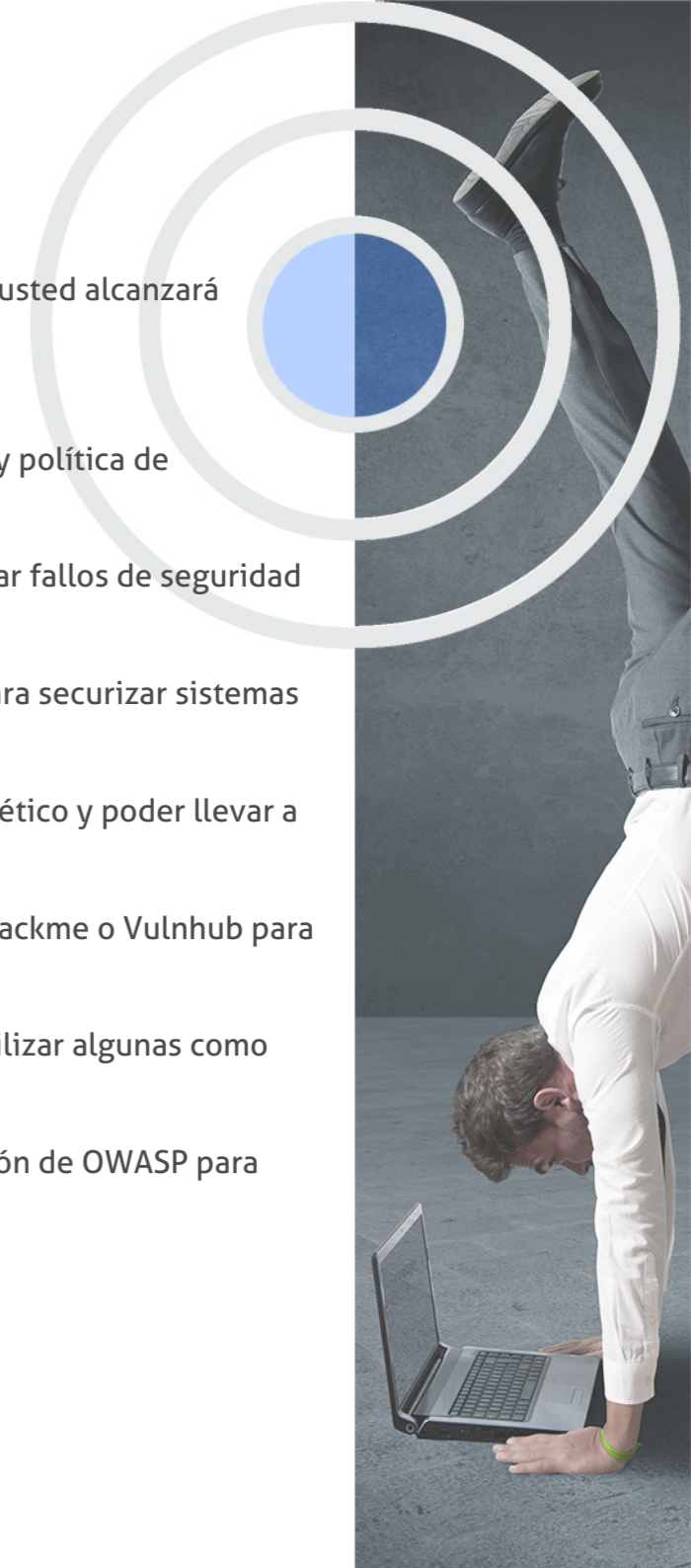
A quién va dirigido

El principal objetivo de este Master en Ciberseguridad es dotar de las habilidades necesarias para evitar ciberataques, intentos de intrusión e incidentes de seguridad a ingenieros informáticos, administradores de sistemas o profesionales del campo informático utilizando las principales herramientas, técnicas, normativa y políticas de seguridad dentro de este sector.

Objetivos

Con el Masters Profesionales **Master en Ciberseguridad** usted alcanzará los siguientes objetivos:

- Implantar SGSI aplicando la legislación, normativa y política de seguridad necesaria.
- Establecer comunicaciones seguras y poder detectar fallos de seguridad con sistemas IDS/IPS y sistemas SIEM.
- Aprender los principales modelos criptográficos para securizar sistemas y saber utilizar la ingeniería inversa.
- Conocer el funcionamiento y las fases del Hacking ético y poder llevar a cabo auditorías informáticas.
- Utilizar plataformas como Hack the Box (HTB), Tryhackme o Vulnhub para entrenar las habilidades de hacker ético.
- Saber cómo funcionan las herramientas OSINT y utilizar algunas como Shodan, Maltego, Google Dork, Creepy o Foca.
- Seguir las guías de desarrollo, testing y code revisión de OWASP para crear desarrollos web seguros.





¿Y, después?

Para qué te prepara

Gracias a este Master en Ciberseguridad descubrirás que protocolos de red, estándares de comunicación y herramientas se usan para garantizar la seguridad informática. Te anticiparás a ciberataques utilizando técnicas de ingeniería inversa, herramientas OSINT y análisis de malware. Conocerás el Hacking ético y practicarás en plataformas como Hack the Box (HTB), Tryhackme o Vulnhub. Además, podrás desarrollar sitios web de forma segura con OWASP.

Salidas Laborales

Existe una gran demanda de expertos en ciberseguridad ya que todas las empresas buscan personal cualificado para cubrir estos puestos. Gracias a este Master en Ciberseguridad podrás optar a trabajar en puestos como Chief Security Officer (CSO), Data Protection Officer (DPO), Auditor de sistemas, Consultor de ciberseguridad, Hacker ético o Experto en desarrollo web seguro.

¿Por qué elegir INESEM?



PROGRAMA ACADÉMICO

Master en Ciberseguridad

Módulo 1. **Legislación, política de seguridad y ciberinteligencia**

Módulo 2. **Herramientas, técnicas de ciberseguridad y sistemas siem**

Módulo 3. **Hacking ético y auditoría informática**

Módulo 4. **Gestión de incidentes y análisis forense**

Módulo 5. **Cracking o ingeniería inversa**

Módulo 6. **Herramientas de ciberseguridad osint**

Módulo 7. **Hacking training platforms**

Módulo 8. **Seguridad en desarrollo web**

Módulo 9. **Ciberseguridad aplicada a inteligencia artificial (ia), smartphones, internet de las cosas (iot) e industria 40**

Módulo 10. **Proyecto fin de máster**

Módulo 1.

Legislación, política de seguridad y ciberinteligencia

Unidad didáctica 1.

Introducción y conceptos básicos

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

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 27001
2. Legislación: Leyes aplicables a los SGSI (RGPD)

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.

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 5.

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

Unidad didáctica 1.

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 2.

Criptografía

1. Perspectiva histórica y objetivos de la criptografía
2. Teoría de la información
3. Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía
4. Criptografía de clave privada o simétrica
5. Criptografía de clave pública o asimétrica
6. Algoritmos criptográficos más utilizados
7. Funciones hash y los criterios para su utilización
8. Protocolos de intercambio de claves
9. Herramientas de cifrado

Unidad didáctica 3.

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 4.

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 5.

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 6.

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 7.

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.

Hacking ético y auditoría informática

Unidad didáctica 1.

Introducción y conceptos previos

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.

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 4.

Gestión de incidentes y 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

Módulo 5.

Cracking o ingeniería inversa

Unidad didáctica 1.

Introducción y definiciones básicas

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

Unidad didáctica 2.

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 3.

Herramientas de cracking

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

Módulo 6.

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 7.

Hacking training platforms

Unidad didáctica 1.

Introducción a hacking training platforms

1. ¿Qué es el hacking ético?
2. - Diferencias entre hacker ético y malicioso
3. - Tipos de hacking ético
4. - Tipos de trabajos de hacking ético
5. Máquinas virtuales
6. - Instalar VirtualBox
7. - Instalar Kali Linux
8. 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. - Requisitos para utilizar Vulnhub
3. Interfaz de Vulnhub
4. Tutoriales
5. - Ripper: 1 CTF, Vulnhub
6. - Symfonos2 VulnHub
7. - VulnHub - Zico 2 Walkthrough
8. - DC-1:1 Vulnhub

Unidad didáctica 6.

Hack this site

1. ¿Qué es Hack This Suite?
2. Desafíos Hack This Site
3. - Misiones básicas
4. - Misiones realistas

Unidad didáctica 7.

Google xss game

1. ¿Qué es Google XSS Game?
2. Niveles de Google XSS game
3. - Nivel 1
4. - Nivel 2
5. - Nivel 3
6. - Nivel 4
7. - Nivel 5
8. - Nivel 6

Unidad didáctica 8.

Hackthis

1. ¿Qué es HackThis?
2. - Primer desafío
3. Tutorial HackThis
4. Basic+

Módulo 8.

Seguridad en desarrollo web

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. A1:2017 Inyección
2. A2:2017 Autenticación rota
3. A3:2017 Exposición de datos sensibles
4. A4:2017 Entidades externas XML (XXE)
5. A5:2017 Control de acceso roto
6. A6:2017 Mala configuración de seguridad
7. A7:2017 Cross-Site Scripting (XSS)
8. A8:2017 Deserialización insegura
9. A9:2017 Uso de componentes con vulnerabilidades conocidas
10. A10:2017 Insuficiente registro y monitoreo

Módulo 9.

Ciberseguridad aplicada a inteligencia artificial (ia), smartphones, internet de las cosas (iot) e industria 40

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 40

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

Módulo 10.
Proyecto fin de máster

metodología de aprendizaje

La configuración del modelo pedagógico por el que apuesta INESEM, requiere del uso de herramientas que favorezcan la colaboración y divulgación de ideas, opiniones y la creación de redes de conocimiento más colaborativo y social donde los alumnos complementan la formación recibida a través de los canales formales establecidos.



Con nuestra metodología de aprendizaje online, el alumno comienza su andadura en INESEM Business School a través de un campus virtual diseñado exclusivamente para desarrollar el itinerario formativo con el objetivo de mejorar su perfil profesional. El alumno debe avanzar de manera autónoma a lo largo de las diferentes unidades didácticas así como realizar las actividades y autoevaluaciones correspondientes.

El equipo docente y un tutor especializado harán un *seguimiento exhaustivo*, evaluando todos los progresos del alumno así como estableciendo una línea abierta para la resolución de consultas.

Nuestro sistema de aprendizaje se fundamenta en *cinco pilares* que facilitan el estudio y el desarrollo de competencias y aptitudes de nuestros alumnos a través de los siguientes entornos:

Secretaría

Sistema que comunica al alumno directamente con nuestro asistente virtual permitiendo realizar un seguimiento personal de todos sus trámites administrativos.

Campus Virtual

Entorno Personal de Aprendizaje que permite gestionar al alumno su itinerario formativo, accediendo a multitud de recursos complementarios que enriquecen el proceso formativo así como la interiorización de conocimientos gracias a una formación práctica, social y colaborativa.

Revista Digital

Espacio de actualidad donde encontrar publicaciones relacionadas con su área de formación. Un excelente grupo de colaboradores y redactores, tanto internos como externos, que aportan una dosis de su conocimiento y experiencia a esta red colaborativa de información.

Revista Digital

Secretaría

5

pilares del método

Webinars

Campus Virtual

Comunidad

Comunidad

Espacio de encuentro que permite el contacto de alumnos del mismo campo para la creación de vínculos profesionales. Un punto de intercambio de información, sugerencias y experiencias de miles de usuarios.

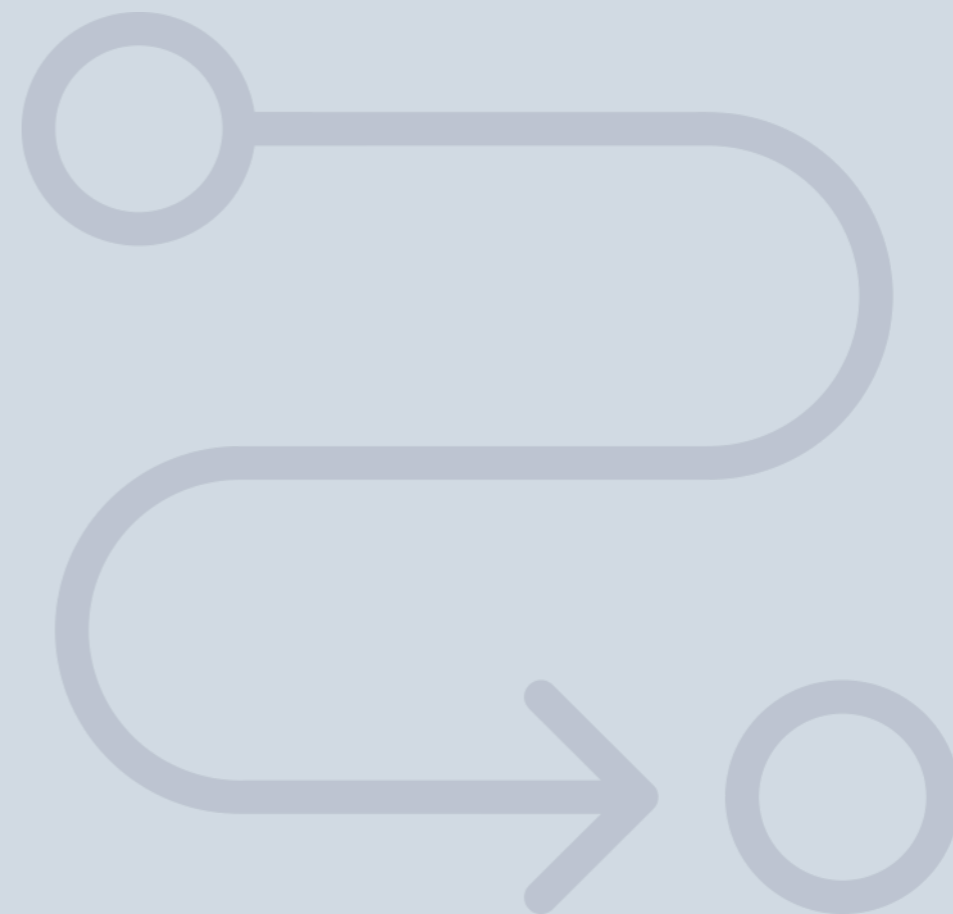
Webinars

Píldoras formativas mediante el formato audiovisual para complementar los itinerarios formativos y una práctica que acerca a nuestros alumnos a la realidad empresarial.



SERVICIO DE **Orientación** de Carrera

Nuestro objetivo es el asesoramiento para el desarrollo de tu carrera profesional. Pretendemos capacitar a nuestros alumnos para su adecuada adaptación al mercado de trabajo facilitándole su integración en el mismo. Somos el aliado ideal para tu crecimiento profesional, aportando las capacidades necesarias con las que afrontar los desafíos que se presenten en tu vida laboral y alcanzar el éxito profesional. Gracias a nuestro Departamento de Orientación de Carrera se gestionan más de 500 convenios con empresas, lo que nos permite contar con una plataforma propia de empleo que avala la continuidad de la formación y donde cada día surgen nuevas oportunidades de empleo. Nuestra bolsa de empleo te abre las puertas hacia tu futuro laboral.



Financiación y becas

En INESEM

Ofrecemos a nuestros alumnos facilidades económicas y financieras para la realización del pago de matrículas,

todo ello
100%
sin intereses.

INESEM continúa ampliando su programa de becas para acercar y posibilitar el aprendizaje continuo al máximo número de personas. Con el fin de adaptarnos a las necesidades de todos los perfiles que componen nuestro alumnado.



20%	Beca desempleo	Para los que atraviesen un periodo de inactividad laboral y decidan que es el momento idóneo para invertir en la mejora de sus posibilidades futuras.
15%	Beca emprende	Nuestra apuesta por el fomento del emprendimiento y capacitación de los profesionales que se han aventurado en su propia iniciativa empresarial.
10%	Beca alumnos	Como premio a la fidelidad y confianza de los alumnos en el método INESEM, ofrecemos una beca a todos aquellos que hayan cursado alguna de nuestras acciones formativas en el pasado.

Masters Profesionales

Master en Ciberseguridad

Impulsamos tu carrera profesional



INESEM
BUSINESS SCHOOL

www.inesem.es



958 05 02 05 formacion@inesem.es

Gestionamos acuerdos con más de 2000 empresas y tramitamos más de 500 ofertas profesionales al año.

Facilitamos la incorporación y el desarrollo de los alumnos en el mercado laboral a lo largo de toda su carrera profesional.