Masters Oficiales

Master Oficial Universitario en Ciberseguridad + 60 Créditos ECTS

INESEM BUSINESS SCHOOL

Índice

Master Oficial Universitario en Ciberseguridad + 60 Créditos ECTS

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 Oficial Universitario en Ciberseguridad + 60 Créditos ECTS

DURACIÓN	1500
PRECIO	3495 €
CRÉDITOS ECTS	60
MODALIDAD	Online

Entidad impartidora:

INESEM BUSINESS SCHOOL

eCAMPUS UNIVERSITY

Programa de Becas / Financiación 100% Sin Intereses

Titulación Masters Oficiales

- Doble Titulación: - Título Oficial de Master Oficial Universitario en Ciberseguridad expedida por la Universidad e-Campus acreditado con 60 ECTS Universitarios. Su superación dará derecho a la obtención del correspondiente Título Oficial de Máster, el cual puede habilitar para la realización de la Tesis Doctoral y obtención del título de Doctor/a. - Titulación de Master en Ciberseguridad con 1500 horas expedida por EUROINNOVA INTERNATIONAL ONLINE EDUCATION, miembro de la AEEN (Asociación Española de Escuelas de Negocios) y CLADEA (Consejo Latinoamericano de Escuelas de Administración)

Resumen

La demanda de expertos en ciberseguridad por las empresas es cada vez mayor ya que proteger el valor más importante para ellas, la información, es clave.Gracias al Master Oficial Universitario en Ciberseguridad usarás los principales estándares y protocolos en sistemas informáticos aplicando la legislación y normativa vigente. Te anticiparás a las amenazas con mecanismos de detección y análisis y realizarás auditorías informáticas. Descubrirás técnicas criptográficas y de ingeniería inversa aplicando el hacking ético. Además, usarás las principales herramientas de ciberseguridad OSINT.En INESEM 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.

A quién va dirigido

El Master Oficial en Ciberseguridad está orientado tanto para profesionales como a estudiantes del sector informático que quieran aprender a gestionar la ciberseguridad y utilizar sus principales técnicas y herramientas de una manera profesional y, por tanto, convertirse en experto en uno de los sectores con más demanda laboral en la actualidad.

Objetivos

Con el Masters Oficiales **Master Oficial Universitario en Ciberseguridad + 60 Créditos ECTS** usted alcanzará los siguientes objetivos:

- Gestionar la ciberseguridad de cualquier empresa aplicando la legislación y normativa vigente.
- Establecer los protocolos y estándares más adecuados para cualquier tipo de red empresarial.
- Saber aplicar las principales técnicas criptográficas y de ingeniería inversa.
- Aprender qué es el hacking ético y cómo aplicarlo en sus diferentes fases.
- Descubrir las principales técnicas de desarrollo web seguro mediante las guías OWASP.
- Utilizar las herramientas OSINT más interesantes para la ciberseguridad.

¿Y, después?

Para qué te prepara

Mediante el Master Oficial en Ciberseguridad sabrás gestionar los estándares y protocolos más utilizados en los sistemas informáticos y aplicarás las leyes y normativas vigentes. Además, gestionarás amenazas y serás capaz de realizar auditorías informáticas. Todo ello gracias al aprendizaje de técnicas criptográficas, ingeniería inversa, la aplicación del hacking ético y el uso de las principales herramientas de ciberseguridad OSINT.

Salidas Laborales

Actualmente, existe una gran demanda de profesionales expertos en ciberseguridad. Por tanto, obtener esta titulación oficial te abrirá las puertas del mundo laboral y podrás optar a puestos tan demandados e interesantes como Analista de Ciberseguridad empresarial, Consultor/Gestor de seguridad informático, Hacker ético o Auditor de sistemas informáticos.

¿Por qué elegir INESEM?

El alumno es el protagonista

01

Nuestro modelo de aprendizaje se adapta a las necesidades del alumno, quién decide cómo realizar el proceso de aprendizaje a través de itinerarios formativos que permiten trabajar de forma autónoma y flexible.

Innovación y Calidad

Ofrecemos un servicio de orientación profesional y programas de entrenamiento de competencias con el que ayudamos a nuestros alumnos a crear y optimizar su perfil profesional.

02

Empleabilidad y desarrollo profesional

03

Ofrecemos el contenido más actual y novedoso, respondiendo a la realidad empresarial y al entorno cambiante con una alta rigurosidad académica combinada con formación práctica.

INESEM Orienta

Ofrecemos una asistencia complementaria y personalizada que impulsa la carrera de nuestros alumnos a través de nuestro Servicio de Orientación de Carrera Profesional permitiendo la mejora de competencias profesionales mediante programas específicos.

04

Facilidades Económicas y Financieras

05

Ofrecemos a nuestros alumnos facilidades para la realización del pago de matrículas 100% sin intereses así como un sistema de Becas para facilitar el acceso a nuestra formación.

PROGRAMA ACADÉMICO

Master Oficial Universitario en Ciberseguridad + 60 Créditos ECTS

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

Módulo 2. **Redes informáticas: arquitectura, protocolos y ciberseguridad**

Módulo 3. **Cracking, ingeniería inversa y criptografía**

Módulo 4. **Hacking ético y auditoría informática**

Módulo 5. **Gestión de incidentes y análisis forense**

Módulo 6. **Seguridad en desarrollo web**

Módulo 7. **Ciberseguridad aplicada a inteligencia artificial (ia), smartphones, internet de las cosas (iot) e industria 40**

Módulo 8. **Ciberseguridad aplicada al comercio electrónico (e-commerce) y el cloud computing**

Módulo 9. **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 27001:2017
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

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.
Cracking, ingeniería inversa y criptografía

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

Unidad didáctica 4.
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 5.
Diferentes aplicaciones de la criptografía de clave pública

1. Aplicaciones de la criptografía pública y privada
2. Certificado dígital
3. DNI Electrónico
4. Bitcoin

Módulo 4.
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 5.
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 6.
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 7.

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 móvil

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 8.

Ciberseguridad aplicada al comercio electrónico (e-commerce) y el cloud computing

Unidad didáctica 1.

Reglamento general de protección de datos (rgpd) en proyectos de comercio electrónico

1. Determinación de los aspectos clave del comercio electrónico (e-commerce)
2. Identificación de los elementos necesarios para afrontar con garantías la adaptación al Reglamento General de Protección de Datos en proyectos de ecommerce
3. Comprensión de los aspectos legales básicos que tienen que ser respetados por un servicio de venta online
4. Exposición de las obligaciones en materia de consumidores y usuarios

Unidad didáctica 2.

Ciberseguridad en el comercio electrónico

1. Identificación de las ciberamenazas y formas de fomentar la ciberseguridad en el comercio electrónico
2. Determinación de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado
3. Actuación ante un incidente de seguridad

Unidad didáctica 3.

Aspectos introductorios de cloud computing

1. Orígenes del cloud computing
2. Qué es cloud computing
3. Características del cloud computing
4. La nube y los negocios
5. Modelos básicos en la nube

Unidad didáctica 4.

Hardware cloud

1. Virtualización
2. Categorías de virtualización
3. Cloud storage
4. Proveedores fiables de cloud storage

Unidad didáctica 5.

Servicios cloud

1. Servicios cloud para el usuario
2. Escritorio virtual o VDI
3. Servicio de centro de datos remoto

Unidad didáctica 6.

Seguridad, auditoría y cumplimiento en la nube

1. Introducción
2. Gestión de riesgos en el negocio
3. Cuestiones legales básicas. eDiscovery
4. Las auditorías de seguridad y calidad en cloud computing
5. El ciclo de vida de la información

Unidad didáctica 7.

Conceptos avanzados de cloud computing

1. Interoperabilidad en la nube
2. Centro de procesamiento de datos y operaciones
3. Cifrado y gestión de claves
4. Gestión de identidades

Unidad didáctica 8.

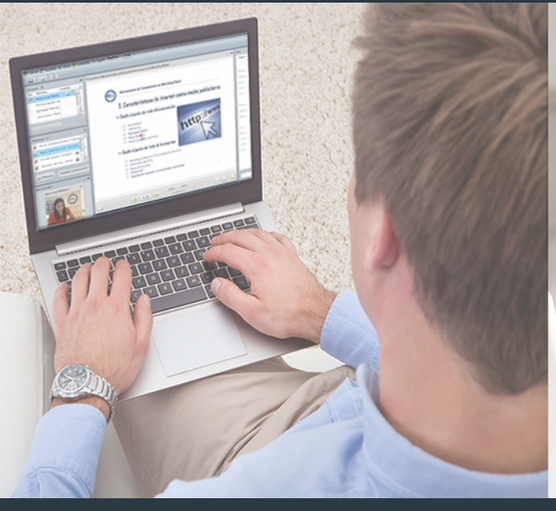
Seguridad y aspectos legales del cloud computing

1. (LOPD) Ley de Protección de Datos
2. Propiedad intelectual
3. Relaciones laborales
4. Los retos del Cloud Computing
5. Implementación de la seguridad en el Cloud Computing
6. Análisis forense en el Cloud Computing
7. Cloud Security Alliance (CSA)

Módulo 9.
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 colabradores y redactores, tanto internos como externos, que aportan una dosis de su conocimiento y experiencia a esta red colaborativa de información.

Comunidad

Espacio de encuentro que pemite el contacto de alumnos del mismo campo para la creación de vínculos profesionales. Un punto de intercambio de información, sugerecias 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.

Masters Oficiales

Master Oficial Universitario en Ciberseguridad + 60 Créditos ECTS