



**EUROINNOVA**  
INTERNATIONAL ONLINE EDUCATION



**ESIBE** ESCUELA  
IBEROAMERICANA  
DE POSTGRADO

## Maestría en Ciberseguridad





Elige aprender en la escuela  
**líder en formación online**

# ÍNDICE

1 | Somos **ESIBE**

2 | Rankings

3 | Alianzas y acreditaciones

4 | By **EDUCA**  
**EDTECH**  
Group

5 | Metodología  
LXP

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

7 | Financiación y **Becas**

8 | Métodos de pago

9 | Programa Formativo

10 | Temario

11 | Contacto

## SOMOS ESIBE

---

**ESIBE** es una **institución Iberoamericana de formación en línea** que tiene como finalidad potenciar el futuro empresarial de los profesionales de Europa y América a través de masters profesionales, universitarios y titulaciones oficiales. La especialización que se alcanza con nuestra nueva **oferta formativa** se sustenta en una metodología en línea innovadora y unos contenidos de gran calidad.

Ofrecemos a nuestro alumnado una **formación de calidad sin barreras físicas**, flexible y adaptada a sus necesidades con el fin de garantizar su satisfacción y que logre sus metas de aprendizaje más ambiciosas. Nuestro modelo pedagógico se ha llevado a miles de alumnos en toda Europa, enriqueciendo este recorrido de la mano de **universidades de prestigio**, con quienes se han alcanzado alianzas.

Más de

**18**

años de  
experiencia

Más de

**300k**

estudiantes  
formados

Hasta un

**98%**

tasa  
empleabilidad

Hasta un

**100%**

de financiación

Hasta un

**50%**

de los estudiantes  
repite

Hasta un

**25%**

de estudiantes  
internacionales

[Ver en la web](#)



Conectamos continentes,  
**Impulsamos conocimiento**



**QS, sello de excelencia académica**

ESIBE: 5 estrellas en educación online

## RANKINGS DE ESIBE

---

**ESIBE** ha conseguido el reconocimiento de diferentes rankings a nivel nacional e internacional, gracias a sus programas de Master profesionales y titulaciones oficiales.

Para la elaboración de estos rankings, se emplean indicadores como la excelencia académica, la calidad de la institución, el perfil de los profesionales.



Ranking Educativo  
**Innovatec**



[Ver en la web](#)

## ALIANZAS Y ACREDITACIONES

---



Ver en la web

## BY EDUCA EDTECH

ESIBE es una marca avalada por **EDUCA EDTECH Group**, que está compuesto por un conjunto de experimentadas y reconocidas **instituciones educativas de formación online**. Todas las entidades que lo forman comparten la misión de **democratizar el acceso a la educación** y apuestan por la transferencia de conocimiento, por el desarrollo tecnológico y por la investigación.



### ONLINE EDUCATION



Ver en la web



# METODOLOGÍA LXP

---

La metodología **EDUCA LXP** permite una experiencia mejorada de aprendizaje integrando la AI en los procesos de e-learning, a través de modelos predictivos altamente personalizados, derivados del estudio de necesidades detectadas en la interacción del alumnado con sus entornos virtuales.

EDUCA LXP es fruto de la **Transferencia de Resultados de Investigación** de varios proyectos multidisciplinarios 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 ESIBE

### 1. Formación Online Especializada

Nuestros alumnos acceden a un modelo pedagógico innovador de **más de 20 años de experiencia educativa** con Calidad Europea.



### 2. Metodología de Educación Flexible



#### 100% ONLINE

Con nuestra metodología estudiarán **100% online**



#### PLATAFORMA EDUCATIVA

Nuestros alumnos tendrán **acceso los 365 días del año** a la plataforma educativa.



### 3. Campus Virtual de Última Tecnología

Contamos con una plataforma avanzada con **material adaptado a la realidad empresarial**, que fomenta la participación, interacción y comunicación on alumnos de distintos países.

### 4. Docentes de Primer Nivel

Nuestros docentes están acreditados y formados en **Universidades de alto prestigio en Europa**, todos en activo y con amplia experiencia profesional.



Ver en la web



## 5. Tutoría Permanente

Contamos con un **Centro de Atención al Estudiante CAE**, que brinda atención personalizada y acompañamiento durante todo el proceso formativo.

## 6. Bolsa de Empleo y Prácticas

Nuestros alumnos tienen acceso a **ofertas de empleo y prácticas**, así como el **acompañamiento durante su proceso de incorporación al mercado laboral** en nuestro ámbito nacional.

## 7. Comunidad Alumni

Nuestros alumnos tienen acceso automático a servicios complementarios gracias a una **Networking formada con alumnos en los cinco continentes**.



## 8. Programa de Orientación Laboral

Los alumnos cuentan con **asesoramiento personalizado** para mejorar sus skills y afrontar con excelencia sus procesos de selección y promoción profesional.



## 9. Becas y Financiación

Nuestra Escuela ofrece **Becas para profesionales latinoamericanos y financiación sin intereses y a la medida**, de modo que el factor económico no sea un impedimento para que los profesionales tengan acceso a una formación internacional de alto nivel.

## FINANCIACIÓN Y BECAS

---

Financia tu cursos o máster y disfruta de las becas disponibles. ¡Contacta con nuestro equipo experto para saber cuál se adapta más a tu perfil!

**25%** Beca  
ALUMNI

**20%** Beca  
DESEMPLEO

**15%** Beca  
EMPRENDE

**15%** Beca  
RECOMIENDA

**15%** Beca  
GRUPO

**20%** Beca  
FAMILIA  
NUMEROSA

**20%** Beca  
DIVERSIDAD  
FUNCIONAL

**20%** Beca  
PARA PROFESIONALES,  
SANITARIOS,  
COLEGIADOS/AS



[Solicitar información](#)

## MÉTODOS DE PAGO

---

Con la Garantía de:



Fracciona el pago de tu curso en cómodos plazos y sin intereses de forma segura.



Nos adaptamos a todos los métodos de pago internacionales:



y muchos más...



[Ver en la web](#)

## Maestría en Ciberseguridad



**DURACIÓN**  
1500 horas



**MODALIDAD  
ONLINE**



**ACOMPañAMIENTO  
PERSONALIZADO**

## Titulación

Titulación de Maestría en Ciberseguridad con 1500 horas expedida por ESIBE (ESCUELA IBEROAMERICANA DE POSTGRADO).



Ver en la web

## Descripción

---

La ciberseguridad siempre ha sido importante, pero de un tiempo a esta parte se ha convertido en el eje central a seguir tanto para el mundo empresarial como en nuestro día a día. Con esta Maestría en Ciberseguridad podrás defenderte de ciberataques y aplicar estrategias para mejorar la ciberseguridad de sistemas, procesos o entornos. Conocerás la legislación y normativa que hay que cumplir. Utilizarás sistemas IDS/IPS, SIEM y herramientas OSINT como Shodan o Maltego. Aprenderás cómo funciona el hacking ético y entrenarás en plataformas como Hack the Box, Tryhackme o Vulnhub y por último desarrollarás webs de forma segura. 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 y normativa aplicable para los Sistemas de Gestión de la Seguridad de la Información (SGSI).
- Utilizar herramientas OSINT como Google Dork, Shodan, Maltego, The Harvester o Foca.
- Saber cómo establecer comunicaciones seguras, cómo encriptar información e implantar sistemas IDS/IPS.
- Entender en qué consiste el hacking ético y como se aplica en diferentes entornos y ataques.
- Descubrir los principales aspectos y herramientas para llevar a cabo auditorías informáticas.
- Entrenar las técnicas de hacking en plataformas como Hack the Box (HTB), Tryhackme, Hacker101 o Vulnhub.
- Aprender a utilizar las guías OWASP para poder llevar a cabo desarrollos web seguros, testing y revisión de código.

## A quién va dirigido

---

La ciberseguridad es utilizada en todas las áreas, pero para su desarrollo los perfiles más adecuados para llevar a cabo esta Maestría en Ciberseguridad serían los de Ingenieros informáticos o estudiantes en Grados de informática que quieran especializarse en las principales técnicas y herramientas para garantizar la ciberseguridad siguiendo la legislación y normativa vigente.

## Para qué te prepara

---

Con esta Maestría en Ciberseguridad podrás defenderte de ciberataques y aplicar estrategias para mejorar la ciberseguridad de sistemas, procesos o entornos. Conocerás la legislación y normativa que hay que cumplir. Utilizarás sistemas IDS/IPS, SIEM y herramientas OSINT como Shodan o Maltego. Aprenderás cómo funciona el hacking ético y entrenarás en plataformas como Hack the Box,

[Ver en la web](#)

Tryhackme o Vulnhub y por último desarrollarás webs de forma segura.

## Salidas laborales

---

Los Expertos en Ciberseguridad son de los perfiles más demandados en el mundo laboral debido a la gran cantidad de empresas que necesitan expertos en esta materia. Por ello, gracias a esta Maestría en Ciberseguridad optarás a puestos como Experto en Ciberseguridad empresarial, Hacker ético, Responsable de seguridad en aplicaciones web, Ingeniero social o Auditor informático.

[Ver en la web](#)

## TEMARIO

---

### MÓDULO 1. 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. Diagnóstico 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 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 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 2. 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 3. HACKING ÉTICO, CRACKING E INGENIERÍA INVERSA

#### 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. INTRODUCCIÓN A LA INGENIERÍA INVERSA

1. Concepto de Ingeniería Inversa
2. Características de la Ingeniería Inversa

3. Ventajas del uso de Ingeniería Inversa

UNIDAD DIDÁCTICA 6. 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 7. HERRAMIENTAS DE CRACKING

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

MÓDULO 4. 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 5. PERITAJE INFORMÁTICO FORENSE

##### UNIDAD DIDÁCTICA 1. INFORMÁTICA, CONECTIVIDAD E INTERNET

1. La informática
2. Componentes de un sistema informático
3. Estructura básica de un sistema informático
4. Unidad central de proceso en un sistema informático
5. Periféricos más usuales: conexión
6. Sistema operativo
7. Internet
8. Conectividad a Internet

##### UNIDAD DIDÁCTICA 2. FUNDAMENTOS DE LA INFORMÁTICA Y ELECTRÓNICA FORENSE

1. Concepto de informática forense
2. Objetivos de la informática forense
3. Usos de la informática forense
4. El papel del perito informático
5. El laboratorio informático forense
6. Evidencia digital
7. Cadena de custodia

##### UNIDAD DIDÁCTICA 3. CIBERCRIMINALIDAD

1. Delito informático
2. Tipos de delito informático
3. Cibercriminalidad

##### UNIDAD DIDÁCTICA 4. HACKING ÉTICO

1. ¿Qué es el hacking ético?
2. Aspectos legales del hacking ético
3. Perfiles del hacker
4. Test de vulnerabilidades
5. Sniffing

6. Tipos de test de seguridad en entornos web

UNIDAD DIDÁCTICA 5. ANÁLISIS FORENSE

1. El análisis forense
2. Etapas de un análisis forense
3. Tipos de análisis forense
4. Requisitos para el análisis forense
5. Principales problemas

UNIDAD DIDÁCTICA 6. 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 7. SISTEMA DE GESTIÓN DE SEGURIDAD EN LA INFORMACIÓN SGSI

1. La sociedad de la información
2. ¿Qué es la seguridad de la información?
3. Importancia de la seguridad de la información
4. Principios básicos de seguridad de la información: confidencialidad, integridad y disponibilidad
5. Descripción de los riesgos de la seguridad
6. Selección de controles
7. Factores de éxito en la seguridad de la información
8. Beneficios aportados por un sistema de seguridad de la información

MÓDULO 6. ANÁLISIS FORENSE Y HERRAMIENTAS PARA PERITAJE INFORMÁTICO

UNIDAD DIDÁCTICA 1. ANÁLISIS FORENSE DE DISPOSITIVOS FÍSICOS INFORMÁTICOS

UNIDAD DIDÁCTICA 2. ANÁLISIS FORENSE EN WINDOWS

UNIDAD DIDÁCTICA 3. ANÁLISIS FORENSE EN GNU/LINUX

UNIDAD DIDÁCTICA 4. ANÁLISIS FORENSE EN MAC OS

UNIDAD DIDÁCTICA 5. ANÁLISIS FORENSE EN ANDROID

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE EN IOS

UNIDAD DIDÁCTICA 7. ANÁLISIS FORENSE DE EMAILS, WHATSAPPS Y OTRAS COMUNICACIONES

UNIDAD DIDÁCTICA 8. INFORME PERICIAL

## Solicita información sin compromiso

**¡Matricularme ya!**

### Telefonos de contacto

España		+34 900 831 200	Argentina		54-(11)52391339
Bolivia		+591 50154035	Estados Unidos		1-(2)022220068
Chile		56-(2)25652888	Guatemala		+502 22681261
Colombia		+57 601 50885563	Mexico		+52-(55)11689600
Costa Rica		+506 40014497	Panamá		+507 8355891
Ecuador		+593 24016142	Perú		+51 1 17075761
El Salvador		+503 21130481	República Dominicana		+1 8299463963

### !Encuétranos aquí!

#### Edificio Educa Edtech

Camino de la Torrecilla N.º 30 EDIFICIO EDUCA EDTECH,  
C.P. 18.200, Maracena (Granada)

 [formacion@euroinnova.com](mailto:formacion@euroinnova.com)

 [www.euroinnova.com](http://www.euroinnova.com)

#### Horario atención al cliente

Lunes a viernes: 9:00 a 20:00h Horario España

¡Síguenos para estar al tanto de todas nuestras novedades!

España       
Latino America    
Reública Dominicana  

Ver en la web



By  
**EDUCA EDTECH**  
Group