unir LA UNIVERSIDAD EN INTERNET

# Programa de Formación Universitaria en Hacking e IA aplicados a la Ciberseguridad

Un programa pensado y diseñado para alumnos de Ciclos Formativos de Grado Superior que deseen complementar su formación ampliando conocimientos relacionados con la ciberseguridad.

## Principales aportaciones para un alumno de FP

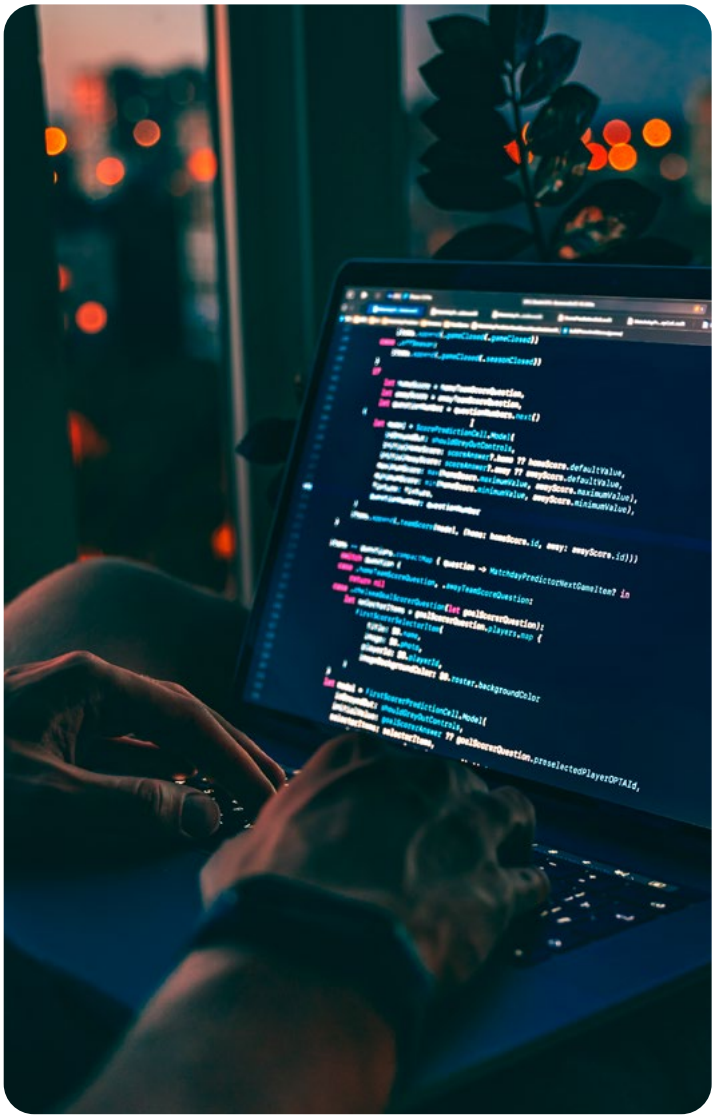
Este programa está diseñado para los alumnos de los **Ciclos Formativos de Grado Superior en Desarrollo de Aplicaciones Web (DAM), Desarrollo de Aplicaciones Multiplataforma (DAM), Administración de Sistemas Informáticas en Red (ASIR), Sistemas de Telecomunicaciones e Informáticas y Automatización y Robótica Industrial** entre otros.

Al finalizar esta formación el estudiante estará preparado para entender las técnicas utilizadas tanto por los hackers éticos como por los profesionales de la auditoría de sistemas para identificar y proteger contra vulnerabilidades en sistemas informáticos.

Estos contenidos formativos pertenecen a un nivel de Grado Universitario en Ciberseguridad, lo cual facilitará el reconocimiento de estos créditos si más adelante deciden iniciar el estudio de este grado.

El Programa de Formación Universitaria en Hacking e IA aplicados a la Ciberseguridad surge como respuesta a la creciente demanda de profesionales con conocimientos de hacking para analizar y auditar las deficiencias y riesgos de seguridad a las que se enfrentan los usuarios, las empresas y las instituciones en aspectos como la arquitectura, el sistema operativo o la comunicación.

Este curso busca fomentar la continuidad formativa de los estudiantes al proporcionar una estructura de aprendizaje modular, que permite la convalidación de asignaturas al Grado en Ciberseguridad. De este modo, se facilita una transición fluida entre la Formación Profesional (FP) y la educación universitaria.



# Programa

## Cuatrimestre 1

Octubre - Febrero

## Asignatura 1: Amenazas en el Ciberespacio

### Principales competencias y resultado de aprendizaje

Esta asignatura se centra en el estudio de los peligros y riesgos inherentes al uso de las tecnologías de la información y la comunicación, particularmente en Internet.

El objetivo principal de la asignatura es proporcionar a los estudiantes una comprensión profunda de las diversas amenazas que existen en el ciberespacio, así como las técnicas y herramientas para mitigarlas. Se abordarán conceptos fundamentales como la clasificación de amenazas y la motivación de los atacantes, la gestión del riesgo y la inteligencia de amenazas, aspectos esenciales para cualquier profesional de la ciberseguridad.

En cuanto al contenido, la asignatura está estructurada en varios temas:

- **Introducción a las amenazas y riesgos**: este módulo cubre la tipología y clasificación de amenazas, así como la gestión del riesgo y la inteligencia de amenazas.
- **La Internet oscura**: se exploran las redes Darknet y Deep Web, con un enfoque especial en tecnologías como Tor, ZeroNet, I2P y Freenet.
- **Tor**: se profundiza en la red TOR, diferenciando entre diferentes tipos de redes y su funcionamiento.
- **Criptomonedas**: este tema aborda el concepto de «blockchain», su historia y funcionamiento, además de discutir la legalidad y ejemplos de criptomonedas en diversos países.

- **Inteligencia en fuentes abiertas (OSINT)**: se estudian las técnicas de recolección de información a partir de fuentes abiertas y su importancia en la ciberseguridad.
- **Ataques a IoT**: se analiza la seguridad en dispositivos conectados a Internet, incluyendo el uso de herramientas como Shodan para la detección de vulnerabilidades.
- **Fraudes en la red**: se examinan diversos tipos de estafas en línea, desde la carta nigeriana hasta la sextorsión.
- **Fraudes en medios de pago**: se exploran las vulnerabilidades en métodos de pago electrónicos, tarjetas EMV NFC y billeteras electrónicas.
- **Defensa en redes**: se discuten técnicas de seguridad en operaciones, recursos y controles, y sistemas de detección de intrusión.
- **Detección y respuesta ante amenazas**: se enseñan los fundamentos de la monitorización de amenazas y la respuesta proactiva a incidentes, incluyendo el uso de herramientas de SIEM y SOAR.

## Cuatrimestre 2

Marzo – Julio

## Asignatura 2: Técnicas de Hacking y Auditoría de Sistemas

### Principales competencias y resultado de aprendizaje

Esta asignatura tiene como **objetivo principal** proporcionar a los estudiantes un entendimiento profundo de las técnicas utilizadas tanto por los hackers éticos como por los profesionales de la auditoría de sistemas para identificar y proteger contra vulnerabilidades en sistemas informáticos.

Al finalizar esta asignatura, los estudiantes estarán preparados para comprender y enfrentarse a los desafíos de seguridad informática en un mundo digital en constante evolución. Con un enfoque en la ética y la legalidad, se espera que los estudiantes se conviertan en profesionales capaces de proteger y fortalecer la seguridad de los sistemas informáticos en sus futuras carreras.

El **hacking ético**, a diferencia de las prácticas ilegales de hacking, se enfoca en identificar y corregir vulnerabilidades en sistemas informáticos de manera ética y legal. Implica comprender cómo piensan los atacantes y emplear técnicas similares para fortalecer la seguridad de los sistemas. Por otro lado, la auditoría de sistemas se centra en evaluar la efectividad de los controles de seguridad implementados en una organización, identificar posibles puntos débiles y recomendar acciones correctivas.

En el panorama actual de la informática, la seguridad de los sistemas juega un papel crucial. Los avances tecnológicos han traído consigo un aumento en la complejidad de las **infraestructuras** informáticas, pero también han abierto nuevas puertas a **amenazas cibernéticas** cada vez más sofisticadas.

Por ello, exploraremos en detalle tanto

las **metodologías y técnicas** utilizadas por los hackers éticos para **identificar vulnerabilidades**, como las herramientas y prácticas empleadas en la auditoría de sistemas. Abordaremos temas que van desde la **recolección de información** y el escaneo de redes hasta la explotación de vulnerabilidades y la **mitigación de riesgos**. Además, analizaremos la importancia de la **ética** y la **legalidad** en el contexto del hacking ético y la auditoría de sistemas, al preparar a los estudiantes para enfrentar los desafíos de seguridad informática en un entorno cada vez más complejo y dinámico.

Los **objetivos** para el estudiante son:

- Comprender los principios fundamentales del hacking ético y la auditoría de sistemas.
- Aprender las metodologías y técnicas utilizadas en el hacking ético.
- Familiarizarse con las herramientas necesarias para llevar a cabo una auditoría de sistemas efectiva.
- Desarrollar habilidades para identificar, explotar y mitigar vulnerabilidades en sistemas informáticos.
- Entender la importancia de la ética y la legalidad en el contexto del hacking ético y la auditoría de sistemas.

## Asignatura 3: Inteligencia Artificial Aplicada a la Ciberseguridad

### Principales competencias y resultado de aprendizaje

La asignatura Inteligencia Artificial Aplicada a la Ciberseguridad se erige como un pilar fundamental para el profesional de la seguridad en la era digital. Su objetivo principal es dotar al estudiante de las competencias teóricas y, sobre todo, prácticas, para diseñar, implementar y gestionar sistemas de ciberdefensa potenciados por inteligencia artificial (IA) y machine learning (ML).

En un panorama donde los ciberataques son cada vez más sofisticados y automatizados, la capacidad de respuesta tradicional resulta insuficiente. La IA emerge no como una opción, sino como una necesidad para analizar ingentes, volúmenes de datos, detectar anomalías imperceptibles para el ser humano y automatizar la respuesta ante incidentes en tiempo real.

Esta materia conecta los fundamentos de la seguridad informática con las técnicas más vanguardistas en ciencia de datos. Su contenido traza una ruta lógica que parte de la comprensión del ciclo de vida de un proyecto de machine learning, profundizando en los algoritmos defensivos clave para la detección de malware o intrusiones. Sin embargo, no se detiene ahí; aborda una perspectiva de 360 grados al estudiar también cómo la IA puede ser atacada (adversarial machine learning) y, consecuentemente, cómo proteger nuestros modelos. Finalmente, la asignatura culmina con la operacionalización de estas soluciones (MLOps), su interpretabilidad (XAI) y su integración en una estrategia de defensa adaptativa y continua, preparando al alumno para los desafíos reales del sector.

- **Bloque 1**: Fundamentos y aplicaciones clásicas de IA en ciberseguridad
- **Bloque 2**: IA Generativa (LLM) y su doble uso en ciberseguridad
- **Bloque 3**: Ciberseguridad de los sistemas de IA

## Un nuevo concepto de universidad online

La Universidad Internacional de La Rioja, universidad con docencia 100% online, se ha consolidado como solución educativa adaptada a los nuevos tiempos y a la sociedad actual. El innovador modelo pedagógico de UNIR ha conseguido crear un nuevo concepto de universidad en el que se integran aspectos tecnológicos de última generación al servicio de una enseñanza cercana y de calidad. La metodología 100% online permite a los alumnos estudiar estén donde estén, interactuando, relacionándose y compartiendo experiencias con sus compañeros y profesores. Actualmente UNIR cuenta con:

- Más de 41.000 alumnos.
- Más de 10.000 alumnos internacionales.
- Presencia en 90 países de los 5 continentes.
- Más de 130 títulos de Grado y Postgrado.
- Más de 4.000 convenios de colaboración firmados para dar cobertura de prácticas a nuestros estudiantes.

* Los temas pueden sufrir alguna variación antes del inicio del curso.

## Dirección y profesorado

El claustro está compuesto por profesionales y profesores de reconocido prestigio y con una dilatada experiencia en el ámbito empresarial y docente de la Informática. Esto nos permite ofrecer a nuestros alumnos una formación sólida y completa a través de un programa académico riguroso y eminentemente práctico en la Ingeniería Informática y eminentemente práctico en la matemática computacional.

### Elisa Alises Núñez

Offensive Security Engineer en Minery Report | Directora Académica Grado Ciberseguridad UNIR | Ingeniera Informática | Máster Ciberseguridad | Certificaciones como CSIO, CSCE, CEHv12 Master... | Experto Universitario en Peritaje Informático

**Formación**

Ingeniera informática con máster en **ciberseguridad**. Profesional de ciberseguridad con cerca de **4 años de experiencia en el ámbito técnico, con especial foco en pentesting** y experiencia adicional en otras áreas como análisis forense y scripting.

**Experiencia**

Cuenta con casi **3 años de experiencia en la dirección de un grado oficial**, reglado y con reconocimiento internacional, **liderando a más de 500 personas** y coordinando distintos departamentos, con responsabilidad en la toma de decisiones estratégicas y operativas.

Además, dispone de casi **3 años de experiencia en docencia**, impartiendo formación especializada en ciberseguridad. **Dirección de más de 25 TFG y TFM en ciberseguridad**, con calificaciones mayoritariamente de notable y sobresaliente.