unir LA UNIVERSIDAD EN INTERNET

Programa Profesional en Ciberseguridad

Programa Profesional en Ciberseguridad

Índice

Carta de Presentación

En todos los sectores es necesario establecer mecanismos y medidas para proteger los sistemas de información y las redes de comunicaciones. El mundo requiere cada día más expertos en ciberseguridad para salvaguardar la información que se genera y se procesa a través de ordenadores, servidores, dispositivos móviles, redes y sistemas electrónicos.

¿Sabías que, según el último informe de Burning Glass Technologies, la demanda de profesionales ha aumentado un 94% en los últimos seis años?

Las vacantes en ciberseguridad suponen el 13% de la demanda global de empleos en el sector tecnológico.

Según se afirma desde el Foro Económico Mundial, las organizaciones deben comprender los riesgos cibernéticos y planificar los retos del mañana, ya que los piratas informáticos buscan vulnerabilidades para acceder a grandes flujos comerciales o a cualquier información que presente una brecha y suponga un potencial beneficio para ellos.

La ciberseguridad es una de las grandes preocupaciones de todos los Estados. Así se evidenció en la conferencia de Davos 2023, donde se llegó a afirmar que la próxima pandemia podría ser la ciberpandemia. En un mundo digital que evoluciona a gran velocidad, gobiernos y organizaciones de todos los sectores deben anticiparse y abordar los retos de ciberseguridad para poder detectar las operaciones cibernéticas maliciosas.

Las áreas de aplicación son diversas y se necesitan perfiles capaces de desempeñar empleos como los siguientes:

- Expertos en ciberseguridad capaces de asumir distintos roles para compañías de todo tipo y tamaño, e instituciones públicas y privadas.
- Auditores de ciberseguridad que comprueben que las medidas de seguridad establecidas por una organización se ajustan a la normativa de protección de datos, y sepan identificar deficiencias o vulnerabilidades.
- Consultores de ciberseguridad capacitados para implementar las medidas correctoras o complementarias necesarias para mejorar el flujo de las organizaciones y para evitar posibles brechas de seguridad informáticas.
- Hackers éticos que puedan diseñar y lanzar ataques informáticos con los que poder detectar debilidades y evitar así riesgos futuros.

El Curso en Ciberseguridad de UNIR es una oportunidad única para dotarte de más herramientas con las que perfeccionar tu desempeño en el mundo de la ciberseguridad. Podrás obtener mejores resultados ante la creciente complejidad de las situaciones que se plantean en todo tipo de organizaciones.

Objetivos

El objetivo de este curso es aprender, definir e implementar estrategias de seguridad en los sistemas de información mediante diagnósticos de ciberseguridad, la identificación de vulnerabilidades y la puesta en marcha de las medidas necesarias para mitigarlas bajo la normativa vigente y los principales estándares del sector. Todo ello conforme a los protocolos de calidad, de prevención de riesgos laborales y de respeto ambiental.

Por qué UNIR recomienda este programa

Con el Curso en Ciberseguridad aprenderás a:

- Prevenir riesgos, realizar diagnósticos, identificar vulnerabilidades y diseñar e implementar estrategias de seguridad en los sistemas de información y redes de comunicaciones.
- Aplicar las principales técnicas de **protección ante amenazas informáticas** e **incidentes de ciberseguridad**.
- Realizar auditorías de ciberseguridad y diseñar planes de prevención.
- Definir y poner en marcha **estrategias de seguridad** en organizaciones de todo tipo conforme a la normativa vigente en cada caso.
- Hacer frente a los **ataques informáticos**.

Una propuesta innovadora con 5 valores diferenciales

Profesores **especialistas con una amplia experiencia profesional**.

Formación en **entornos reales de trabajo**: aplicaciones online, laboratorios, nuevas tecnologías...

Empleabilidad: aumenta tus posibilidades de encontrar trabajo gracias a la adaptación continua de los temarios del curso a las necesidades de las empresas. Realiza prácticas en las mejores compañías del mercado.

Garantía de **calidad de UNIR**, la Universidad en internet.

Herramientas más demandadas: utiliza como cualquier profesional del sector las aplicaciones más empleadas por las empresas.

Requisitos de acceso

El Programa Profesional en Ciberseguridad, no requiere de ningún requisito de acceso, pero está dirigido a perfiles técnicos con conocimientos de las principales técnicas de protección frente a las amenazas externas y ciberataques, deseo de avanzar en su formación técnica dentro del área de sistemas de forma analítica y metódica o a quienes tengan interés por orientarse hacia la auditoría.

Datos Clave

DURACIÓN: 9 MESES / 42 ECTS

DOCENCIA 100% ONLINE

CLASES PRESENCIALES VIRTUALES

Interactúa con el profesor y el resto de los estudiantes. Si no puedes asistir en directo, puedes verlas en diferido siempre que quieras.

- Claustro formado por especialistas y profesionales en activo.
- Conocimientos aplicables desde el primer módulo.
- Tutor personal.

Salidas profesionales:

Los alumnos que superen el programa formativo podrán ejercer su actividad en entidades de los sectores donde sea necesario establecer mecanismos y medidas para la protección de los sistemas de información y redes de comunicaciones. Las ocupaciones y puestos de trabajo más relevantes son los siguientes:

- Experto en ciberseguridad.
- Auditor de ciberseguridad.
- Consultor de ciberseguridad.
- Hacker ético.

Claustro

Wiktor Nykiel

Ingeniero de Ciberseguridad, es cofundador de Ginseg, Comunidad de Ciberinteligencia Colectiva y del Congreso IntelCon. Anteriormente fue responsable de la línea de servicio de ciberinteligencia enfocada en entidades financieras en el Centro de Excelencia EMEIA de EY. También ha sido responsable del Servicio Global de Ciberinteligencia de Prosegur.

Miguel Ángel Ortega

Ingeniero informático de formación con amplia experiencia en el mundo TIC ha liderado proyectos de ciberseguridad en el sector gubernamental relacionados con la seguridad de la información en entornos protegidos y multidominio, así como en el diseño e implantación de capacidades de protección, detección y repuesta en SOC.

Raúl Ramírez

Autodidacta, graduado en Telecomunicaciones y máster en Seguridad de la Información. Trabaja como investigador forense en el equipo DFIR Global de Santander, desde donde se responde ante cualquier incidente y se automatizan las tareas de recolección y respuesta. Habitual Blue Team CTF player y entusiasta de la seguridad defensiva.

Manuel Sánchez Rubio

Doctor por la Universidad de Alcalá e Ingeniero en Informática. Investigador científico en el Ministerio de Defensa. Manuel Sánchez Rubio es director asociado del Máster en Seguridad Informática en UNIR y profesor de la Universidad de Alcalá, de la Complutense de Madrid y de la de Huelva, así como en universidades en Chile y Colombia en áreas relacionadas con las redes, la seguridad informática y los delitos informáticos en distintos grados y másteres.

Daniel Echeverri

Formador e investigador de seguridad informática y hacking. Autor del blog thehackerway.com y de los libros “Python para Pentesters”, “Hacking con Python” y “Deep web – Privacidad y anonimato en TOR, I2P y Freenet” publicados por la editorial 0xWORD, así como el libro «25 Técnicas aplicadas a campañas de red team y hacking» de edición propia. Desde hace más de 15 años desarrolla actividades de desarrollo y arquitectura de software, administración de servidores, pentesting, hardening de sistemas y formaciones tanto para organizaciones públicas como privadas.

Carlos Galán

Ha trabajado como consultor legal en la Agencia de Tecnología Legal (ATL) y como técnico jurídico en el Instituto Nacional de Ciberseguridad (INCIBE) sobre amenazas híbridas, la desinformación, la privacidad y la ciberseguridad. Miembro del equipo de investigación del Parlamento Europeo para el proyecto “Las comunicaciones estratégicas como factor clave para contrarrestar las amenazas híbridas”.

Programa

MÓDULO 1

Gestión y operación de la ciberseguridad

- Tema 1. Desarrollo de planes de prevención y concienciación en ciberseguridad.
- Tema 2. Auditoría de incidentes de ciberseguridad.
- Tema 3. Investigación de los incidentes de ciberseguridad.
- Tema 4. Implementación de medidas de ciberseguridad.
- Tema 5. Detección y documentación de incidentes de ciberseguridad.

MÓDULO 2

Aspectos legales de la ciberseguridad

- Tema 1. Puntos principales de aplicación para un correcto cumplimiento normativo.
- Tema 2. Diseño de sistemas de cumplimiento normativo.
- Tema 3. Legislación para el cumplimiento de la responsabilidad penal.
- Tema 4. Legislación y jurisprudencia en materia de protección de datos.
- Tema 5. Normativa vigente de ciberseguridad de ámbito nacional e internacional.
- Tema 6. Esquema Nacional de Seguridad (ENS).
- Tema 7. Ley PIC (Protección de Infraestructuras Críticas).

MÓDULO 3

Mecanismos de seguridad y defensa del perímetro

- Tema 1. Diseño de planes de segurización.
- Tema 2. Configuración de sistemas de control de acceso y autenticación de personas.
- Tema 3. Administración de credenciales de acceso a sistemas informáticos.
- Tema 4. Diseño de redes de computadores seguras.
- Tema 5. Configuración de dispositivos y sistemas informáticos.
- Tema 6. Configuración de dispositivos para la instalación de sistemas informáticos.
- Tema 7. Configuración de los sistemas informáticos.

MÓDULO 4

Desarrollo y despliegue seguro de aplicaciones

- Tema 1. Prueba de aplicaciones web y para dispositivos móviles.
- Tema 2. Determinación del nivel de seguridad requerido por aplicaciones.
- Tema 3. Detección y corrección de vulnerabilidades en aplicaciones web.
- Tema 4. Detección de problemas de seguridad en aplicaciones para dispositivos móviles.
- Tema 5. Implantación de sistemas seguros de desplegado de software.

MÓDULO 5

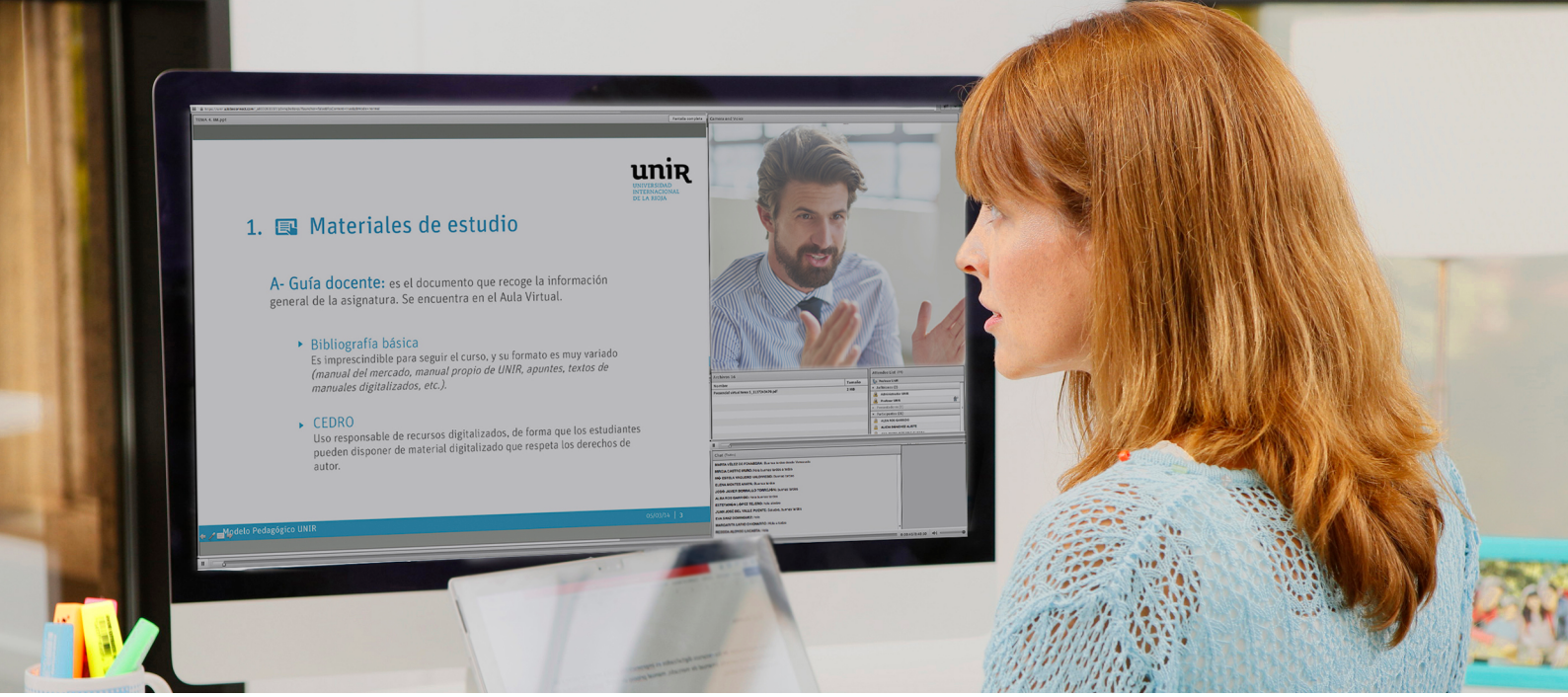
Digital Forensics and incident response

- Tema 1. Aplicación de metodologías de análisis forense.
- Tema 2. Realización de análisis forenses en dispositivos móviles.
- Tema 3. Realización de análisis forenses en cloud.
- Tema 4. Realización de análisis forenses en IoT.
- Tema 5. Documentación y elaboración de informes de análisis forenses. Apartados de los que se compone el informe.

MÓDULO 6

Ciberseguridad y hacking

- Tema 1. Determinación de las herramientas de monitorización para detectar vulnerabilidades.
- Tema 2. Ataque y defensa en entorno de pruebas de las comunicaciones inalámbricas.
- Tema 3. Ataque y defensa en entorno de pruebas de redes y sistemas para acceder a sistemas de terceros.
- Tema 4. Consolidación y utilización de sistemas comprometidos.
- Tema 5. Ataque y defensa en entorno de pruebas a aplicaciones web.



Metodología

Este curso está concebido para que pongas en práctica todo lo aprendido conforme avanzas en los distintos temas:

- **Temarios online** a los que podrás acceder en cualquier momento y desde cualquier lugar. Todos los contenidos se pueden descargar para facilitar el estudio sin conexión.
- **Clases en directo** que permanecen grabadas para que puedas verlas tantas veces como quieras.
- Aprendizaje en **entornos reales de trabajo**: aplicaciones online, laboratorios, etc.
- Actividades de desarrollo y test de evaluación para que vayas probando tus nuevas habilidades a medida que avanzas en la formación.

Sistema de evaluación

Para obtener la titulación el alumno deberá

- Realizar y superar la **evaluación continua** de cada uno de los módulos: actividades de desarrollo, ejercicios grupales, test de evaluación y participación en foros.
- Realizar y superar los **exámenes teórico-prácticos** de cada uno de los módulos formativos.

Calificación final del Programa Profesional

Media de los resultados obtenidos en la evaluación continua y en el examen final. Para que se pueda calcular la media entre la evaluación continua y el examen final será necesario tener aprobadas las dos partes.

Al finalizar el Curso en Ciberseguridad de UNIR obtendrás un título propio de UNIR con un reconocimiento de 42 créditos ECTS.

FLEXTIME

Nos adaptamos a tu disponibilidad horaria permitiéndote acceder y participar en directo a las sesiones online, a los foros de discusión, así como a los materiales complementarios. Sin barreras geográficas, en cualquier momento y en cualquier lugar.

CLAUSTRO ESPECIALIZADO

Todos nuestros docentes son profesionales de empresas líderes, que imparten sus sesiones en base a su propia experiencia, lo que aporta una visión real del mercado.

LEARNING BY DOING

Aplicarás todos los conocimientos gracias al aprendizaje adquirido en sesiones prácticas. Trabajarás en grupos dirigidos por especialistas, donde podrás fomentar el Networking e intercambiar experiencias.

SESIONES ONLINE EN DIRECTO

Podrás seguir e intervenir en las sesiones estés donde estés, sin necesidad de desplazamientos. Y si por algún motivo no pudieras asistir, podrás ver el material grabado en cualquier momento.

MENTORING CONSTANTE Y PERSONALIZADO

Desde el primer día se te asignará un tutor que te acompañará y apoyará en todo momento, resolviendo todas las dudas que te puedan surgir y tratando de potenciar tus habilidades para tu desarrollo.

Por qué elegirnos

Porque ponemos a tu disposición todo lo que necesitas para mejorar tu carrera profesional, **sin necesidad de desplazarte**, tan solo requieres de conexión a internet y un dispositivo (PC, Tablet o incluso un Móvil) para seguir el programa.

Porque con nuestro modelo pedagógico, pionero en el mercado, participarás en **clases online en directo impartidas por los mejores profesionales**. Además, podrás verlas **en cualquier momento y desde cualquier lugar**, ideal para compatibilizarlo con tu agenda personal y profesional.

Porque fomentamos el **NETWORKING**, clave en tu desarrollo profesional, poniéndote en contacto con ponentes y participantes de alto nivel, con los que compartirás trabajo y experiencias a través de la plataforma.

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
- Además UNIR es una **universidad responsable con la cultura, la economía y la sociedad.** Este compromiso se materializa a través de la Fundación UNIR.

unir LA UNIVERSIDAD EN INTERNET

RECTORADO LOGROÑO

Avenida de la Paz, 137
26006. La Rioja
España
+34 941 210 211

DELEGACIÓN MADRID

Calle de García Martín, 21
28224. Pozuelo de Alarcón
España
+34 915 674 391

DELEGACIÓN BOGOTÁ

Calle 100 # 19-61. Edificio Centro Empresarial 100. Oficina 801. 11001
Colombia
+571 5169659

DELEGACIÓN CD. DE MÉXICO

Avenida Universidad 472,
Narvarte Poniente. 03600
México
+52 (55) 84210768

DELEGACIÓN QUITO

Avenida República E7-123 y Martín Carrión (esquina). Edificio Pucará
Ecuador
(+593) 3931480

DELEGACIÓN LIMA

José Gabriel Chariarse, 415
San Antonio. Miraflores
Perú
(01) 496 – 8095

unir.net | +34 941 209 743