unir LA UNIVERSIDAD EN INTERNET

Máster de Formación Permanente en Security Operation Center (SOC)

Máster de Formación Permanente en Security Operation Center (SOC)

Índice

Carta de Presentación

> ***“El Máster tiene como objetivo ayudar a quienes tienen un rol en la ciberseguridad a mejorar su capacidad para encontrar, analizar y responder a las ciber-amenazas de manera proactiva y preventiva”***

El Máster de Formación Permanente en Security Operation center (SOC) está diseñado para todos aquellos que desean ampliar sus habilidades tácticas, estratégicas y operativas para afrontar con conocimiento los **desafíos de seguridad empresarial**.

Los módulos que integran el programa del Máster proporcionarán **una base sólida para diseñar, construir, integrar, ponerlo en producción, operar y mantener un SOC eficiente**.

Para hacerlo, reunimos experiencia, modelos y enfoques contrastados en casos prácticos y reales, combinando personas, procesos y tecnología clave para entregar servicios gestionados de seguridad TIC, criptografía, análisis de arquitectura de seguridad corporativa, etc.

Los alumnos aprenderán a mantenerse actualizados sobre la tecnología que cambia rápidamente, **adaptarse y controlar la creciente generación de nuevas amenazas y comenzar una carrera exitosa en ciberseguridad**.

Este programa presenta una descripción general de cómo organizar y considerar las muchas funciones en los centros de operaciones de seguridad (SOC).

Discutiremos **estrategias que se podrán aplicar a SOC de cualquier tamaño y misión**; desde un SOC con dos personas hasta un CSCC (Cyber Security Command Center) nacional con cientos de personas.

Está orientado a todos los profesionales cuyo desempeño es vinculante a un centro de operaciones de seguridad, desde los nuevos profesionales que recién comienzan a interesarse en la seguridad digital, a los **actuales operadores en un SOC**, a los gerentes que consideran la expansión de la capacidad del SOC, o a aquellos que quieran **orientar su carrera profesional al mundo de la consultoría de ciberseguridad**.

Comenzando con un módulo de Fundamentos que resume las categorías y áreas funcionales, el programa de maestría en SOC propone a los ciber-profesionales la aplicación de estrategias y conceptos clave para respaldar la misión de un SOC de clase mundial.

El Máster en Formación Permanente en Security Operation Center (SOC) tiene como objetivo **ayudar a quienes tienen un rol en la ciberseguridad a mejorar su capacidad para encontrar, analizar y responder a las ciber-amenazas de manera proactiva y preventiva**.

La estructura de este programa incluye módulos estratégicos, módulos tácticos, y módulos técnicos que, cuando se unifican, conducen a una mayor capacidad y eficiencia de operaciones de seguridad.

unir LA UNIVERSIDAD EN INTERNET

Datos Clave

8 MESES / 60 ECTS

DOCENCIA 100% ONLINE

CLAUSTRO ESPECIALIZADO FORMADO POR PROFESIONALES EN ACTIVO

CONOCIMIENTOS APLICABLES DESDE EL PRIMER MÓDULO

EN COLABORACIÓN CON SOC ACADEMY INSTITUTE

TUTOR PERSONAL

MENTOR PROFESIONAL

LABORATORIO VIRTUAL PARA CONSTRUIR UN SOC BASADO EN CASOS REALES.

Por qué UNIR recomienda este programa

Con el **Máster de Formación Permanente en Security Operation Center (SOC)** obtendrás las competencias necesarias para:

- **Detectar y conocer todo tipo de intrusiones**: malware, ransomware, fake news, swarm-as-a-service, troyanos, doxing, phishing, ataque DDOS, espionajes, ataque de fuerza bruta, entre otros.
- Dominar la principal herramienta de un SOC, el **sistema de gestión de eventos e información de seguridad SIEM** (Security Information Event Management)
- **Ampliar tu perspectiva y enfoque** para detectar, analizar y establecer soluciones conociendo todos los aspectos que influyen en la ciberseguridad: seguridad de la red, de las bases de datos y de su almacenamiento, de hardware y de software, de privacidad, de sistemas, de las tecnologías, de las aplicaciones.
- Comprender y corregir todos los incidentes de ciberseguridad posibles, realizando **análisis avanzados, criptoanálisis, ingeniería inversa de malware, vulnerabilidades de red, control de identidades, biométrica, esteganografía, evidencias digitales**.
- **Comunicarte eficazmente** para obtener el apoyo de los otros departamentos y de la dirección, siendo capaz de **involucrar en el proyecto SOC a todos los tomadores de decisión**.

A QUIÉN VA DIRIGIDO

- Profesionales técnicos o expertos de la seguridad informática que necesitan comprender los conceptos de gestión de proyectos y utilizar múltiples enfoques de desarrollo.
- Miembros de los equipos de operaciones de seguridad informática o personas que van a acceder a estos equipos.
- Mandos intermedios o cargos de gerencia o dirección que desean comprender las áreas críticas para que las iniciativas de ciberseguridad sean exitosas.
- Cualquier persona en un puesto clave o principal de ingeniería/diseño que trabaje regularmente con el personal de gestión de proyectos del área de la seguridad informática.
- Cualquier persona involucrada en la planificación, implementación o mantenimiento de un programa de educación, capacitación o comunicaciones de seguridad informática.
- Líderes de seguridad recientemente ascendidos que desean construir una base de seguridad para liderar y formar equipos.
- Roles de trabajo del marco NICE (Iniciativa Nacional de Educación en Seguridad Cibernética).

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

NETWORKING INTERNACIONAL

Podrás conocer al resto de participantes de España y Latinoamérica con los que te pondremos en contacto de forma presencial y/o virtual a lo largo del curso.

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** de cualquier parte del mundo. 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

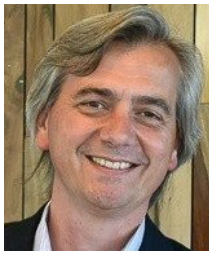
La Universidad Internacional de La Rioja, universidad con docencia 100% online, se ha consolidado como solución educativa adaptada a los nuevos tiempos y a la sociedad actual. El **innovador modelo pedagógico de UNIR** ha conseguido crear un nuevo concepto de universidad en el que se integran aspectos 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.

Claustro

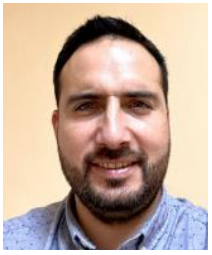
Emilio González
Profesor

Licenciado en Seguridad y Defensa. Máster en Ciberseguridad. Especializado en el área de seguridad informática. Con más de 10 años de experiencia en el sector desarrollando y dirigiendo proyectosvinculados a la ciberseguridad, ciberinteligencia y SOC de diferentes organizaciones.



Daniel Vénere Minoli
Profesor

Licenciado en Informática. Postgrado en Dirección de Empresas y Master en Telecomunicaciones. Con más de 25 años de experiencia en el desarrollo, implementación e integración de modelos de gobierno de riesgo, sistemas de gestión de seguridad de la información y protección de datos personales en instituciones financieras, aseguradoras, retail, telecomunicaciones.



Hernán Villaroel
Profesor

Licenciado en Ingeniería naval con mención en Telecomunicaciones Navales. De la Academia Politecnica Naval (APN), Viña del mar. Experiencia en entornos de transformación digital y en implantación de proyectos TI para la defensa. Se desempeña como analista de Ciberseguridad del departamento de ciberoperaciones de la Armada.

Pilar de Miguel Veira
Profesora

Titulada en Ingeniería de Minas por la Universidad Politécnica de Madrid, PDM por Instituto de Empresa de Madrid. Cuenta con más de 20 años de experiencia en consultoría estratégica y tecnológica en empresas como Accenture, Ey y KPMG. Tiene una amplia experiencia en el ámbito de transformación digital y de negocio, ayudando a las organizaciones en distintos sectores.

Programa

ASIGNATURA 1

La estrategia del diseño y dimensionamiento del SOC

- Tema 1. Definición y tipos de SOC
- Tema 2. Equilibrar los elementos básicos del SOC
- Personas y sus competencias
- Procesos y procedimientos
- Tecnologías de operación y de provisión
- Tema 3. Marco legal y regulatorio
- Actividad práctica: análisis y evaluación de requerimientos SOC
- **Test asignatura 1**

ASIGNATURA 2

El Equilibrio del SOC (dimension vs. servicios)

- Tema 1. Cyber seguridad reactiva, proactiva y preventiva
- Tema 2. Diseño del SOC alineado a las capacidades vs requerimientos
- Tema 3. Consolidar tecnologías, servicios y soluciones
- Tema 4. Definir el CMM (modelo de madurez)
- Actividad práctica: proyectar (ecosistema tecnológico y arquitectura) del SOC
- **Test asignatura 2**

ASIGNATURA 3

La autoridad del SOC

- Tema 1. Obtener el apoyo del Directorio
- Tema 2. Establecer gobierno, estrategia y políticas
- Tema 3. Implementar marco legal y regulatorio
- Actividad práctica: presentación y defensa del proyecto SOC a los tomadores de decisión
- **Test asignatura 3**

ASIGNATURA 4

Las mejores prácticas como táctica operativa

- Tema 1. Equilibrar servicios vs capacidades
- Tema 2. Plan de evolución de capacidades
- Tema 3. Programa de mejora continua:
- Medir rendimiento
- Proceso de ajustes y control de cambios
- Actividad práctica: definir el plan de evolución de madurez SOC
- **Test asignatura 4**

ASIGNATURA 5

El capital humano (talento vs cantidad)

- Tema 1. Dimensión del equipo humano SOC
- Tema 2. Gestión del talento
- Tema 3. Plan de carrera SOC
- Tema 4. Plan de entrenamiento (laboratorios y simulación de cyber escenarios)
- Actividad práctica: diseñar el plan de captación y retención del talento
- **Test asignatura**

ASIGNATURA 6

La estrategia operacional

- Tema 1. Modelo de relación interna
- Tema 2. Modelo de organización jerárquica

- Tema 3. Procesos operativos de seguridad:
- Procesos de operación rutinaria
- Procesos de delivery de servicios
- Indicadores y métricas (KPIs, KRIs y KDIs)
- Tema 4. Seguridad del ecosistema de Soporte operacional del SOC
- Actividad práctica: definir el BCP & DRP
- **Test asignatura 6**

ASIGNATURA 7

La importancia de la calidad del dato

- Tema 1. Selección de fuentes de colección:
- Clasificación del dato de valor
- Tema 2. Definición de casos de uso:
- Alerta temprana
- Tema 3. Indicadores y métricas de calidad
- Actividad práctica: análisis y evaluación de requerimientos del SIEM
- **Test asignatura 7**

ASIGNATURA 8

El ciclo de vida del SOC

- Tema 1. Plan de mejora continua
- Tema 2. Plan de evolución tecnológica
- Tema 3. Plan de capacitación y entrenamiento
- Tema 4. Alianzas con otros SOC´s
- Actividad práctica: definir y establecer alianzas con otros SOC´s y/o fuentes externas de inteligencia de amenazas
- **Test asignatura 8**

ASIGNATURA 9

Ciberinteligencia de amenazas (consumidor vs productor)

- Tema 1. Técnicas tradicionales vs inteligencia aplicada
- Tema 2. Capacidad y estrategia basada en la cyber amenaza
- Tema 3. Consumir, fusionar y producir inteligencia de amenaza
- Tema 4. Desarrollo y uso de inteligencia de amenaza
- Actividad práctica: detección proactiva y automatización de respuesta
- **Test asignatura 9**

ASIGNATURA 10

Poner en producción un SOC (Trabajo Fin de Máster)

Talleres de diseño, despliegue, configuración y puesta en producción del SOC por medio de las etapas a seguir.

Sistema de evaluación

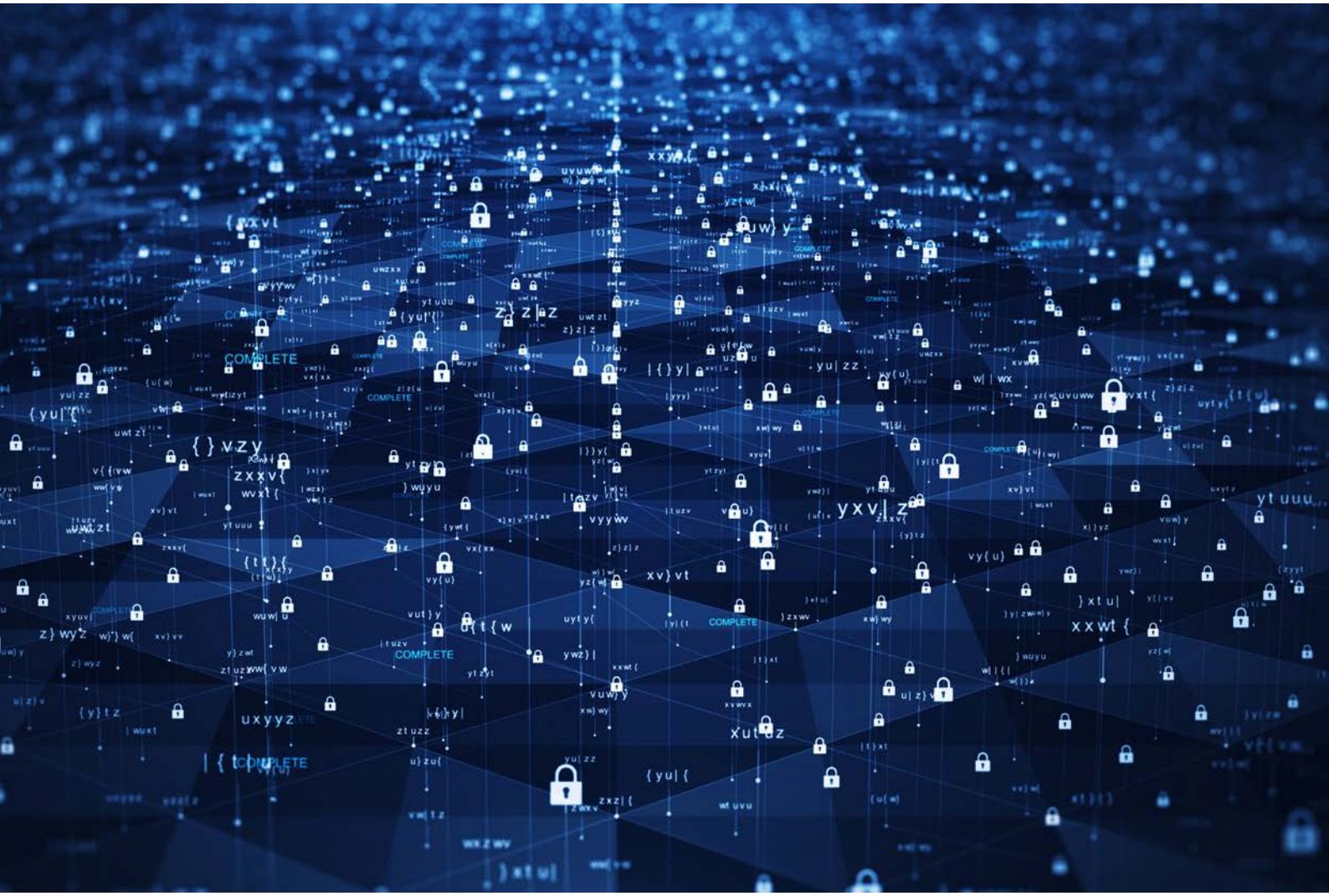
Para superar este máster el alumno deberá superar:

- Realización de las actividades asignadas en cada módulo.
- Exámenes tipo test que tendrán lugar al final de cada módulo. Será necesario responder correctamente al menos al 60% de las preguntas para obtener el aprobado.
- Entrega y superación proyecto final

Requisitos de acceso

Estar en posesión de un título universitario oficial* español u otro expedido por una institución de Educación Superior del Espacio Europeo de Educación Superior que facultan en el país expedidor del título para el acceso de enseñanzas de Máster.

*Esto implica título oficial de graduado, diplomado, arquitecto técnico, ingeniero técnico, licenciado, arquitecto o ingeniero.



OTROS PROGRAMAS RECOMENDADOS

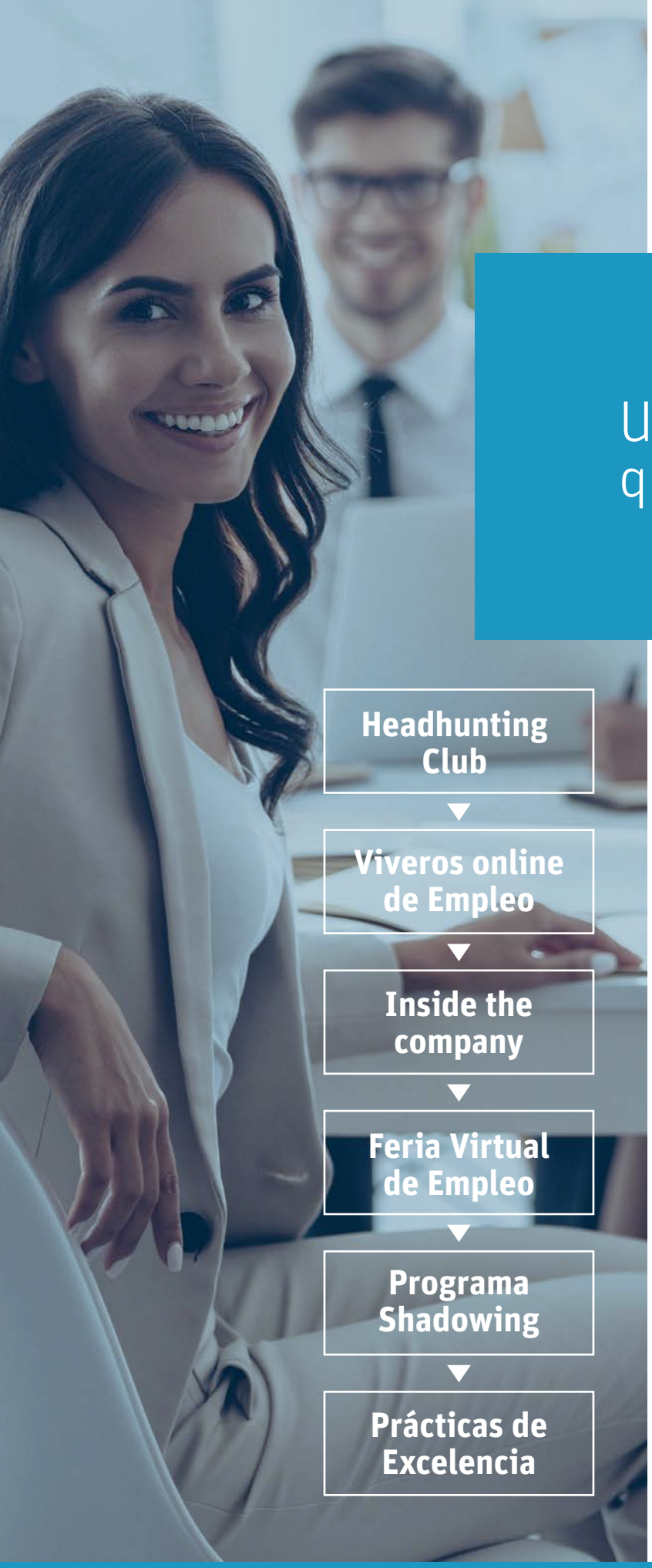
- Máster en Ciberseguridad
- Experto Universitario en Peritaje informático.

CÓMO MATRICULARSE

- Completa el formulario de preinscripción.
- Recibe la llamada de un asesor personal, que verifique que cumples los requisitos exigidos y te ayude a elaborar tu plan de estudios personalizado.
- Cumplimenta la matrícula* con la forma de pago más adecuada a tus necesidades.
- Recibe tu clave de acceso al AULA VIRTUAL y comienza el curso organizándote a tu manera.

** Un asesor te facilitará el acceso al formulario de matrícula.*

unir LA UNIVERSIDAD EN INTERNET



UNIR, mucho más que una universidad

Headhunting Club

Viveros online de Empleo

Inside the company

Feria Virtual de Empleo

Programa Shadowing

Prácticas de Excelencia

CONVIÉRTETE EN EL PROFESIONAL QUE LAS EMPRESAS NECESITAN

A través de nuestro **Dpto. de Salidas Profesionales y Empleabilidad**, podrás encontrar multitud de oportunidades, programas de apoyo y contacto con las mejores empresas de tu sector. Estas empresas ya forman parte de nuestra Red de Partners UNIR y te están buscando.

accenture · indra · Deloitte. · Hewlett Packard Enterprise · Telefónica · CEPSA · Microsoft · GARRIGUES · Heineken · Baker McKenzie. · IBM · EY · gasNatural fenosa · AIRBUS · CONVERSE · ferrovial · FCC · pwc · MELIÁ · zeppelin · Sacyr

Más información - 941 209 743

empleoypracticas.unir.net | info@unir.net

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) 3683 3800

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