eip
ESCUELA INTERNACIONAL POSGRADOS

Máster en

DIRECCIÓN DE CIBERSEGURIDAD, HACKING ÉTICO & SEGURIDAD OFENSIVA

C|EH CERTIFIED ETHICAL HACKER

OFFENSIVE SECURITY OSCP

UEMC Universidad Europea Miguel de Cervantes

GRUPO MAINJOBS

Índice

I. Escuela Internacional de Posgrados

Somos una **Escuela Superior de Posgrados** con actividad docente e investigadora **a nivel internacional** cuyo objetivo es ser **puente entre jóvenes profesionales y empresas lideres** en sus sectores.

Todo el equipo de la Escuela trabaja con un objetivo común: convertirte en el/la profesional que demandan las empresas.

La **metodología de trabajo** es **100% práctica y flexible**, para fomentar activamente la participación y que puedas compatibilizar el estudio con otras actividades paralelas.

eip
ESCUELA INTERNACIONAL POSGRADOS

Especializarse no es una opción, es una necesidad.

» En un mundo cada vez más digitalizado donde se procesa la mayor parte de la información a través de la red es primordial garantizar la protección de los datos, pues empresas y particulares pueden ser vulnerables a una gran cantidad de amenazas, tanto internas como externas, que podrían llegar a causar daños considerables.

» De esta necesidad nace, en materia de Seguridad Informática, la figura del **experto** en **Ciberseguridad** que asume la responsabilidad de diseñar e implementar las estrategias encaminadas a prevenir los incidentes de seguridad.

» En el ámbito de la Ciberseguridad habrá dos ramas diferenciadas, el **especialista en seguridad defensiva** encargado de organizar un plan de seguridad para la infraestructura de la red de la organización, o bien como experto ofensivo, buscando las vulnerabilidades para determinar la seguridad del sistema en lo que se conoce como **hacking ético.**

Perfil del alumnado

Jóvenes recién titulados/as o que estén finalizando sus estudios en Ingenierías de Informática, Telecomunicaciones, Física, Matemáticas y afines, interesados/as en completar su formación, especializándose en el sector de la Ciberseguridad, Hacking Ética y la Seguridad Ofensiva.

Profesionales motivados/as por la especialización en el sector de la ciberseguridad con titulación universitaria en Ingeniería Informática, Telecomunicaciones, Física, Matemáticas y afines.

Jóvenes recién titulados/as o que estén finalizando el ciclo superior de técnico Superior en Desarrollo de Aplicaciones Web o técnico Superior en Desarrollo de Aplicaciones Multiplataforma interesados/as en completar su formación, especializándose en el sector de la Ciberseguridad, Hacking Ética y la Seguridad Ofensiva.

Lo que más valoran l@s alumn@s de EIP:

Luís Ramón Gavilán. Programa Superior en Ciberseguridad

«El profesor es perfecto, muy participativo y solidario con aportación de material adicional muy complet**o**».

José Martínez Velasco. Programa Superior en Ciberseguridad

«El profesor nos ayuda a entender cualquier concepto por simple o complejo que sea».

Alberto Cañete Carpintero. Programa Superior en Ciberseguridad

«Conocimiento de recursos interesantes para mi profesión. El poder hacerlo online permite ver las clases cuando mejor te venga».

Gerardo Rodriguez De la Hoz. Curso de Especialización en Machine Learning y Python

«Me ha enseñado un nuevo campo que desconocía y sobre el que poder seguir aprendiendo».

Lo que más valoran l@s alumn@s de EIP:

Buenaventura Caballero Palacio. Curso de Tecnologías aplicadas a la Industria 4.0

«El curso está proporcionando material teórico de calidad con un seguimiento a través de las actividades a realizar que hace que se tome aún más interés en él».

Alberto Rodríguez Oria. Curso de Tecnologías aplicadas a la Industria 4.0

«Se descubren tecnologías interesantes que antes no las conocía. Estoy descubriendo un mundo bastante novedoso y curioso. Me gustaría seguir formándome sobre ello».

Gloria Catllá. Curso de Tecnologías aplicadas a la Industria 4.0

«Con este curso estamos adquiriendo conocimientos que están actualizados al mercado laboral en el que estamos compitiendo por formar parte».

Beatriz Díaz. Curso de Tecnologías aplicadas a la Industria 4.0

«Variabilidad de contenidos, experiencias personales de los profesionales».

Máster en
Dirección de Ciberseguridad,
Hacking Ético y Seguridad Ofensiva

(60 ECTS – 1500h)

II. Información del Máster

MÁSTER EN DIRECCIÓN DE CIBERSEGURIDAD, HACKING ÉTICO Y SEGURIDAD OFENSIVA

UEMC Universidad Europea Miguel de Cervantes

eip ESCUELA INTERNACIONAL POSGRADOS

ESTRUCTURA DEL PROGRAMA FORMATIVO

MÁSTER DUAL

CRÉDITOS ECTS 60

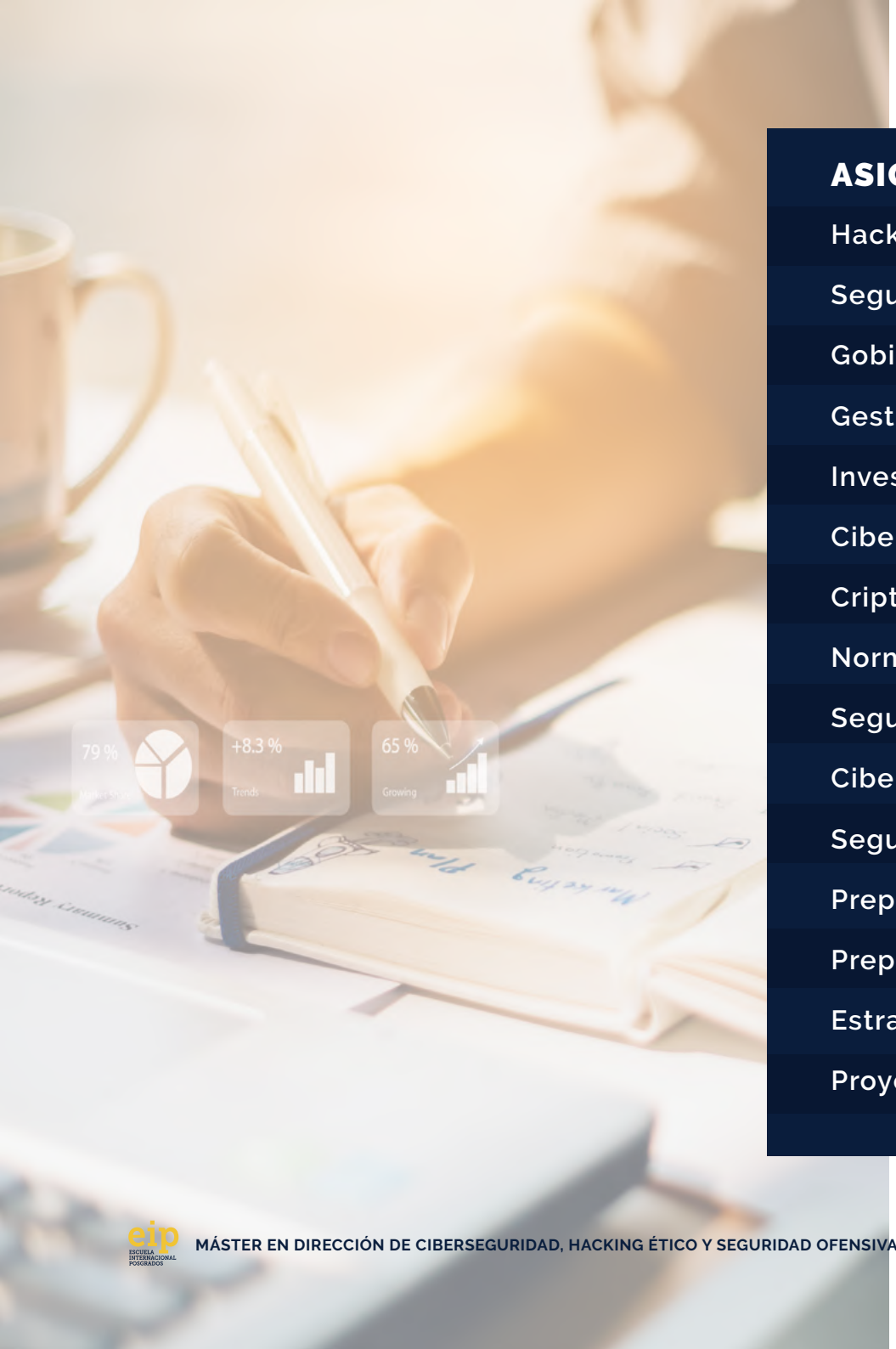
DURACIÓN 1500 horas

MODALIDAD FLEXIBLE
Online con clases en directo y grabadas

IDIOMA Español

PRÁCTICAS PROFESIONALES

Dentro de tu Plan de Desarrollo Profesional, a partir del tercer mes podrás comenzar tus prácticas extracurriculares en puestos técnicos de ciberseguridad y hacking ético, en las que iniciarás una experiencia de Master Dual que te permitirá "aprender haciendo".

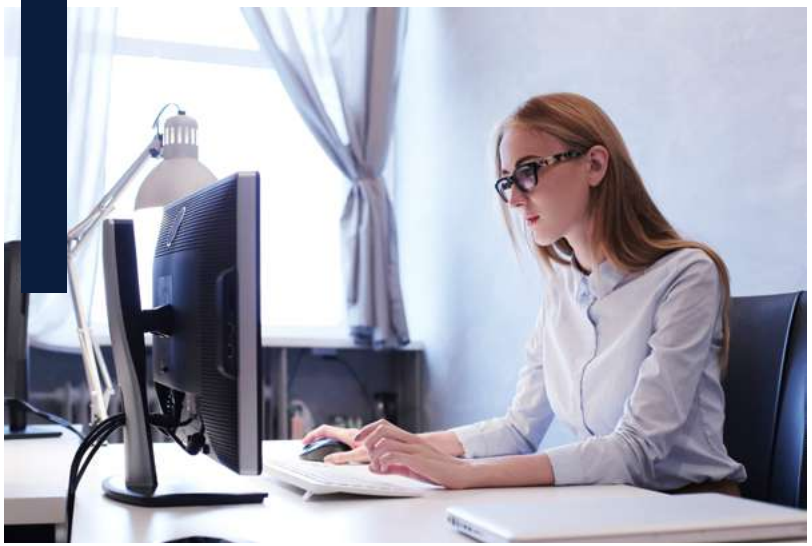


ASIGNATURAS	CRÉDITOS ECTS	HORAS
Hacking ético.	6	150
Seguridad ofensiva.	6	150
Gobierno y gestión de seguridad TI.	6	150
Gestión de riesgos e incidentes.	6	150
Investigación en DeepWeb y DarkWeb.	2,5	62,5
Ciberinteligencia.	2,5	62,5
Criptología.	2,5	62,5
Normativa y legislación.	2,5	62,5
Seguridad en Infraestructuras críticas.	2,5	62,5
Ciberseguridad y tecnologías disruptivas.	3	75
Seguridad en desarrollo software.	2,5	62,5
Preparación para la certificación CEH.	4	100
Preparación para la certificación OSCP.	4	100
Estrategia para una Marca Personal de éxito.	2	50
Proyecto Fin de Máster.	8	200

Hacking ético.

- Te enseñaremos a pensar como un hacker: "Para vencer a un hacker, necesitas pensar como un hacker".
- Aplica **Técnicas de hacking** usadas por hackers y profesionales de seguridad para poder entrar una empresa u organización.
- écnicas para la recopilación de información que te servirá para acometer un ataque (**footprinting**).
- Escanea redes de posibles objetivos de ataques (**scanning**).
- Enumera e identifica de los nombres de los equipos, usuarios, y recursos compartidos que pueden ser atacados (**enumeration**).
- Analiza las vulnerabilidades por donde será posible realizar un ataque (**vulnerability analysis**).
- Explota las vulnerabilidades encontradas y llevar a cabo el ataque (**system hacking**).
- Analiza las amenazadas de **malware** existentes.
- Aprende a "escuchar" y capturar información que circula por una red (**sniffing**).
- Aplica **técnicas de ingeniería social** para obtener información confidencial a través de la manipulación de usuarios legítimos.
- Ejecuta ataques de denegación de servicio para saturar un servidor y dejarlo sin servicio (**DoS**).
- Aprende a secuestrar sesiones de usuario (**Session Hijacking**).
- Evade sistemas de detección de intrusos, cortafuegos y sistemas trampa o señuelos (**IDS, firewall, honeypot**).
- Inyecta código en una aplicación para poder atacarla (**sql injection, cross site scripting**).
- Hackea servidores, todo tipo de redes, aplicaciones web y móviles, dispositivos y objetos interconectados a través de una red (IoT), servidores y aplicaciones en la nube (cloud computing), etc.
- Aprende a ponérselo difícil a posibles atacantes mediante técnicas de **hardering**.
- **Analiza las contramedidas** para prevenir todos los ataques que has aprendido a realizar.

Seguridad ofensiva.



- Aprende a penetrar en sistemas informáticos.
- Conoce **métodos y técnicas de evasión** para evitar ser rastreado y/o poder evadir firewalls y antivirus para llevar a cabo el ataque con éxito.
- Crea diccionarios personalizados y enfocados a cada circunstancia para intentar acceder a los sistemas a través de **técnicas de cracking, guessing,** etc.
- Realiza ataques de suplantación de identidad, ataques de denegación de servicio para tirar servidores, capturar credenciales, levantar servidores y honeypots, etc.
- Analiza las técnicas de **acceso a redes WiFi**.
- Hackea y accede a dispositivos englobados dentro de la denominación Internet of Things como webcams, cámaras de vigilancia infantiles, Alexa, Google Home, Smart TVs, etc.
- Aprende a atacar dispositivos móviles y crear apps maliciosas.
- Conoce los diferentes métodos y técnicas para hackear aplicaciones web como las técnicas de **inyección de código, subidas de ficheros y WebShells**.

Gobierno y gestión de seguridad TI

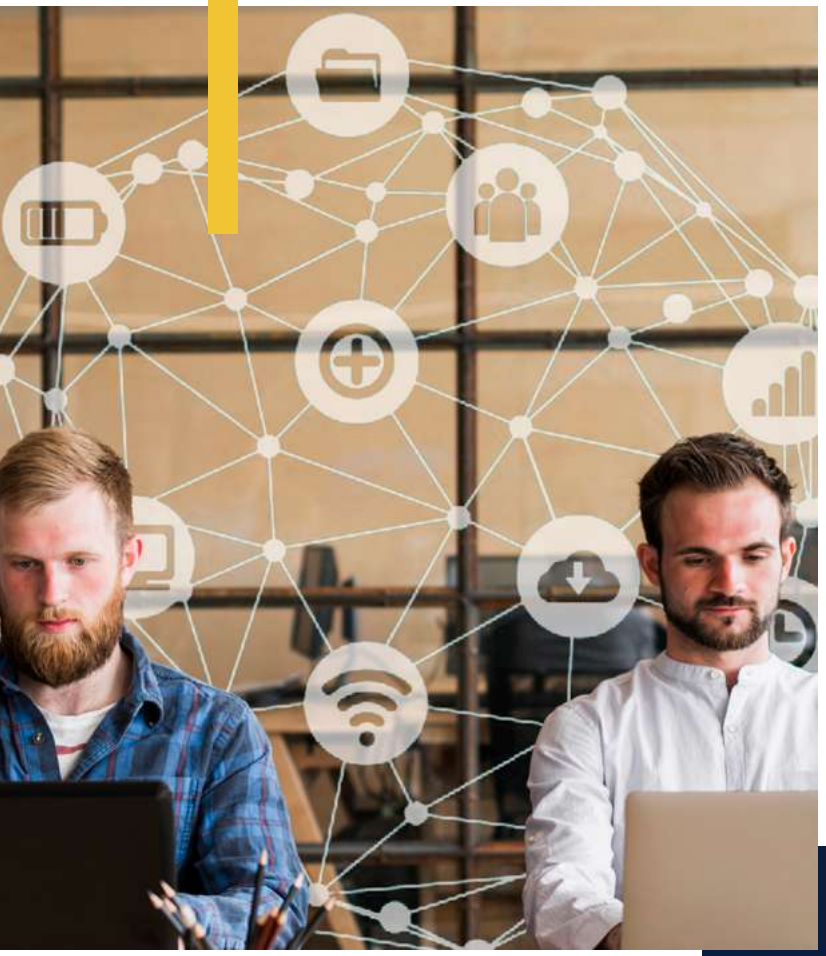
- Adquiere la capacitación para elaborar la guía corporativa para la implantación del **plan de seguridad** de una organización.
- Genera e **implanta políticas de seguridad** de la información.
- Aprende a garantizar la seguridad y privacidad de los datos de empresa y usuarios.
- Supervisa la administración del control de acceso a la información.
- Supervisa el **cumplimiento normativo** de la seguridad de la información.
- Se el responsable del equipo de respuesta ante incidentes de seguridad de la información de la organización.
- Supervisa la **arquitectura de seguridad** de la información de la empresa.
- Diseña el plan de continuidad de negocio y el plan de concienciación y formación en seguridad informática de una organización.
- Construye un **sistema de clasificación de la información** de una organización.
- Gestiona la seguridad de la información mediante un enfoque orientado a la **gestión del servicio con ITIL**.

Gestión de riesgos e incidentes

- Aprende fundamentos en la gestión de riesgos siguiendo la **normativa ISO 31000:2018**.
- Conoce el proceso de la gestión de riesgos e incidentes.
- Conoce **indicadores de riesgo tecnológico (kri´s)**, que te ayudarán a evaluar, analizar riesgos.
- Realiza análisis y toma decisiones para la gestión de riesgos.
- Gestiona los riesgos de una organización acerca de la seguridad de la información siguiendo la **normativa ISO 27001**.
- Aprenderás a gestionar de incidentes y a elaborar el plan de continuidad del negocio.
- Lleva a cabo la investigación de los riesgos que soportan los Sistemas de Información y recomienda las medidas apropiadas que deberían adoptarse para controlar estos riesgos siguiendo la **metodología Magerit**, elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España.

Investigación en DeepWeb y DarkWeb

- Adquiere los conocimientos para identificar las diferencias entre SURFACEWEB, DEEPWEB & DARKWEB.
- Aprende de forma práctica como se aplican las adecuadas **normas de seguridad** para el acceso y navegación en la DEEPWEB & DARKWEB.
- Asimila los potenciales riesgos en el acceso inseguro a DEEPWEB & DARKWEB.
- Utiliza la DEEPWEB & DARKWEB como herramientas para la obtención de información relevante en desarrollo de investigaciones relacionadas con **persecución criminal y delincuencia informática**.



Ciberinteligencia

- Conoce las características del **cibercrimen, ciberterrorismo y hacktivismo** para mitigar su impacto y mejorar así la toma de decisiones en el ámbito de la ciberseguridad.
- Adquiere conocimientos que te permitirán disponer de un **sistema predictivo de alertas tempranas** relativas al cibercrimen, al ciberterrorismo y al hacktivismo.
- **Identifica, rastrea y predice las capacidades, intenciones y actividades cibernéticas malintencionadas** que apoyarán la toma de decisiones.

Criptología

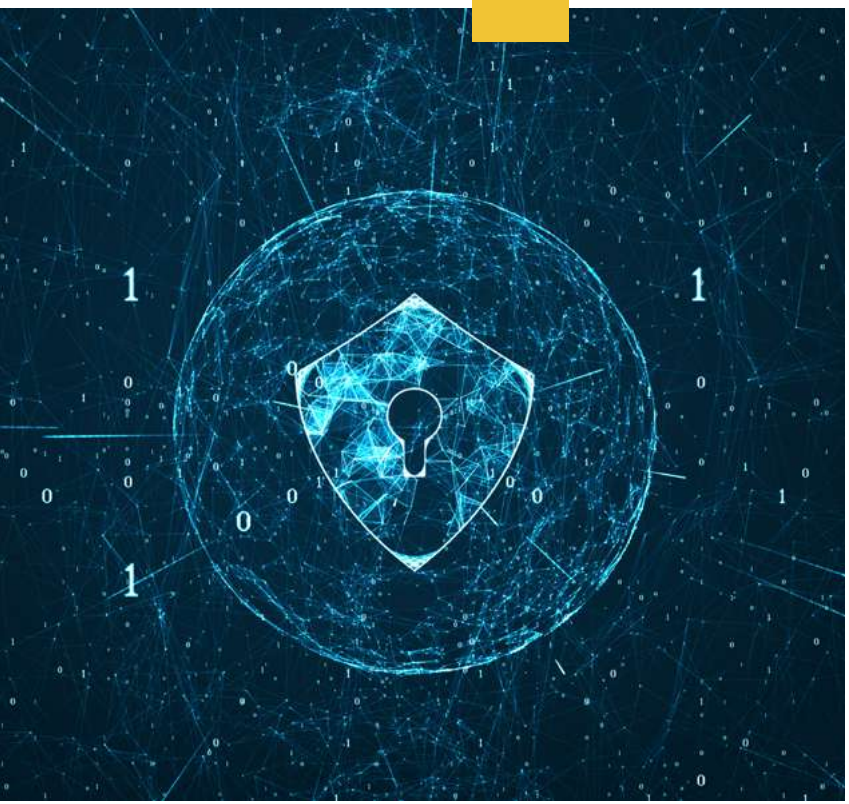
- Comprende y aplica **técnicas criptográficas avanzadas** para encriptar y proteger la información.
- Aprende a recuperar información encriptada mediante **criptoanálisis**.
- Estudia sistemas criptográficos con el fin de encontrar debilidades en los sistemas y romper su seguridad.
- Adéntrate en el **estudio de la esteganografía**, mediante la aplicación de técnicas que permiten ocultar mensajes u objetos.
- Conoce cuáles son los protocolos criptográficos más utilizados y estándares.
- Adquiere conocimientos acerca del futuro de la criptografía: Criptografía basada en retículos. **Criptografía sobre curvas hiperelípticas. Criptografía cuántica.**

Normativa

- Conoce la legislación en materia de ciberseguridad y las consecuencias de su incumplimiento.
- Aprende la normativa nacional e internacional relativa a la seguridad de los sistemas de información.
- Sabrás acerca de requisitos y procedimientos avanzados de certificación de sistemas seguros.
- Identifica cuáles son los organismos relacionados con la ciberseguridad nacionales e internacionales.
- Conoce cuáles son los delitos tipificados y fichas técnicas de los delitos telemáticos.

Seguridad en Infraestructuras críticas

- Aprende a intensificar las infraestructuras críticas como sistemas físicos o virtuales que facilitan funciones y servicios esenciales para apoyar a los sistemas más básicos a nivel social, económicos, medioambiental y político.
- Identifica las **áreas estratégicas** en las que se encuentran las infraestructuras críticas.
- Aprende sobre las **amenazas y vulnerabilidades** de las infraestructuras críticas.
- Comprende, aplica y evalúa la gestión de la seguridad de sistemas altamente segurizados por su naturaleza o criticidad.
- Sabrás cómo **proteger una infraestructura crítica y mitigar los daños** en caso de que ocurra algún incidente de seguridad.
- Lleva a cabo la implantación del sistema nacional de protección de infraestructuras críticas.



Seguridad en desarrollo software

- **Diseña y desarrolla aplicaciones** que garanticen la privacidad y la seguridad de la información.
- Crea y desarrolla aplicaciones atendiendo a **criterios de usabilidad, robustez y eficiencia**.
- Conoce y aplica los diferentes enfoques y metodologías del desarrollo y **auditoría de software seguro**.

Ciberseguridad y tecnologías disruptivas

- Aplica y evalúa técnicas avanzadas de **Inteligencia Artificial** como autenticación biométrica de acceso a sistemas.
- Conoce la **aplicación práctica de Blockchain** para garantizar la seguridad de los sistemas y la información.
- Protege los "nuevos activos" basado en la **conversión de tokens**, en una empresa.
- **Aplica técnicas de Big Data a la seguridad informática** mediante manejo del flujo de información en la organización.
- Aprende el impacto que tiene la llegada de Edge Computing en el campo de la seguridad informática como pieza clave para **la transformación de la tecnología 5G**.

Preparación para la certificación CEH

- La Certificación Hacker Ético se obtiene realizando el examen de certificación, tras haber asistido a un centro de entrenamiento (Centro de Formación Acreditada) o mediante el auto-estudio.
- Si un candidato opta por realizar auto-estudio, se debe llenar un formulario de solicitud y debe probar que tiene 2 años de experiencia en seguridad informática. En caso de que no se tengan los 2 años de experiencia, se podrá mandar una solicitud hablándoles sobre tu formación educativa y por qué deberían de considerarte.
- La versión actual del CEH es la V10 y usa el examen 312-50 del EC-Council. Este examen consta de 125 preguntas de opción múltiple, con un límite de 4 horas para resolverlo, y requiere por lo menos un puntaje del 70% para aprobarlo. El examen es resuelto vía web en la página de Prometric Prime.
- En esta asignatura te prepararás para que puedas presentarte y realizar el examen CEH.

C | EH
Certified Ethical Hacking

Preparación para la certificación OSCP

- El certificado profesional en seguridad ofensiva (OSCP) es una certificación de ethical hacking ofrecida por Offensive Security que enseña metodologías de exámenes de penetración y utiliza herramientas que incluyen el examen de penetración BackTrack usando la distribución Kali Linux.
- La certificación OSCP consiste en un examen práctico que requiere atacar y penetrar de manera satisfactoria varias máquinas en un ambiente seguro controlado.
- Es una de las pocas certificaciones que requiere evidencia de las habilidades en la parte práctica que consiste en una prueba de penetración. Además, su alto nivel de exigencia y dificultad técnica permite destacar la gran capacitación técnica de las pocas personas que logran obtenerla.
- La formación que lleva a la certificación OSCP cubre varios vectores de ataques comunes usados durante pruebas de penetración y auditorías, utilizando la distribución de Linux - Kali Linux.
- Al completar esta asignatura de preparación, tendrás la oportunidad de tomar el reto que implica la certificación:
- Te dan 24 horas en un laboratorio que no es familiar para ellos para atacar 5 máquinas diferentes y conseguir hacerte administrador o root.
- Cada máquina tiene diferentes puntos en función de la dificultad y hace falta un mínimo de 70 puntos para aprobar.
- Está prohibido durante el examen el uso de herramientas automatizadas de explotación de vulnerabilidades, por lo tanto, como pentester tienes que comprender el proceso de explotación a un nivel de detalle muy alto.
- Debes realizar documentación que incluya los procesos empleados y evidencias de que lograron una penetración exitosa incluyendo archivos especiales que son marcados y cambiados cada examen.
- Los resultados del examen son revisados por un comité de certificación y se da una respuesta escrita en las siguientes 72 horas.
- En esta asignatura se ofrece la formación y el material en formato vídeo, pdf, prácticas de laboratorio y acceso al mismo que te preparará para poder obtener la certificación OSCP.

Proyecto Fin de Máster

- El trabajo Fin de Máster (TFM) es la última prueba evaluable que nuestro alumnado deberá superar para obtener su título del Máster en Ciberseguridad, Hacking Ético y Seguridad Ofensiva.
- Para ello el alumno o alumna deberá ser capaz de implementar un sistema de gestión integral de Ciberseguridad.

Proyecto Fin de Máster:

Implantación de un sistema de gestión integral de Ciberseguridad en una organización.

III. Salidas Profesionales

Tras finalizar la formación podrás ocupar puestos de:

- Director de seguridad de la información (CISO).
- Consultor de Ciberseguridad.
- Consultor de seguridad ofensiva.
- Hacker ético y pentester.
- Experto en ciberinteligencia.
- Analista de informática forense.
- Perito judicial tecnológico.
- Arquitecto de sistemas de seguridad.
- Analista de riesgos y vulnerabilidades.
- Experto en desarrollo seguro de sofware.

IV. Prácticas en Empresa

- La mejor manera de afianzar las competencias adquiridas es poniéndolas en práctica en un entorno laboral real.
- Es por eso que el Máster en Dirección de Ciberseguridad, Hacking Ético y Seguridad Ofensiva
- cuenta con la opción de realizar prácticas en empresas
- Te pondremos en contacto con las mejores empresas del sector de la Ciberseguridad donde podrás desarrollarte profesionalmente y ampliar tu red de contactos.
- El departamento de prácticas tratará a cada alumno de manera individualizada para ofrecerle la mejor opción en su zona geográfica.
- Estas prácticas tendrán una duración de entre 3 y 6 meses.

V. Claustro docente

Nuestro equipo docente está formado por expertos en activo, profesionales de la Ingeniería de la Ciberseguridad, directivos, analistas y auditores especialistas en la protección de datos de empresas y usuarios

MARÍA JOSÉ PEÑA

Directora del Máster en Ciberseguridad, Hacking Ético y Seguridad Ofensiva

MANUEL GARCÍA

Director del Área de Posgrados en Ingeniería y Arquitectura

MIGUEL INFANTES

Director de Innovación en Grupo Mainjobs

JAVIER MEJÍAS

Analista programador web, experto en criptología

CARLOS SEISDEDOS

Responsable de Ciberinteligencia en Internet Security Auditors

DAVID SÁNCHEZ

Experto en Ciberseguridad en The Security Sentinel

JOSUÉ LÓPEZ

CEO en Auditech

DANIEL VICENTE

Consultor de Ciberseguridad en KPMG España

ÁNGEL RUÍZ

Ingeniero de Seguridad IT en Isdefe

JAIME TRINIDAD

Consultor de Gestión de Seguridad de la Información en QUEST GLOBAL

DIEGO TINEDO

Experto en digitalización y optimización de procesos

SANTIAGO MARTÍN

Técnico de Sistemas, Comunicaciones e Infraestructuras TIC

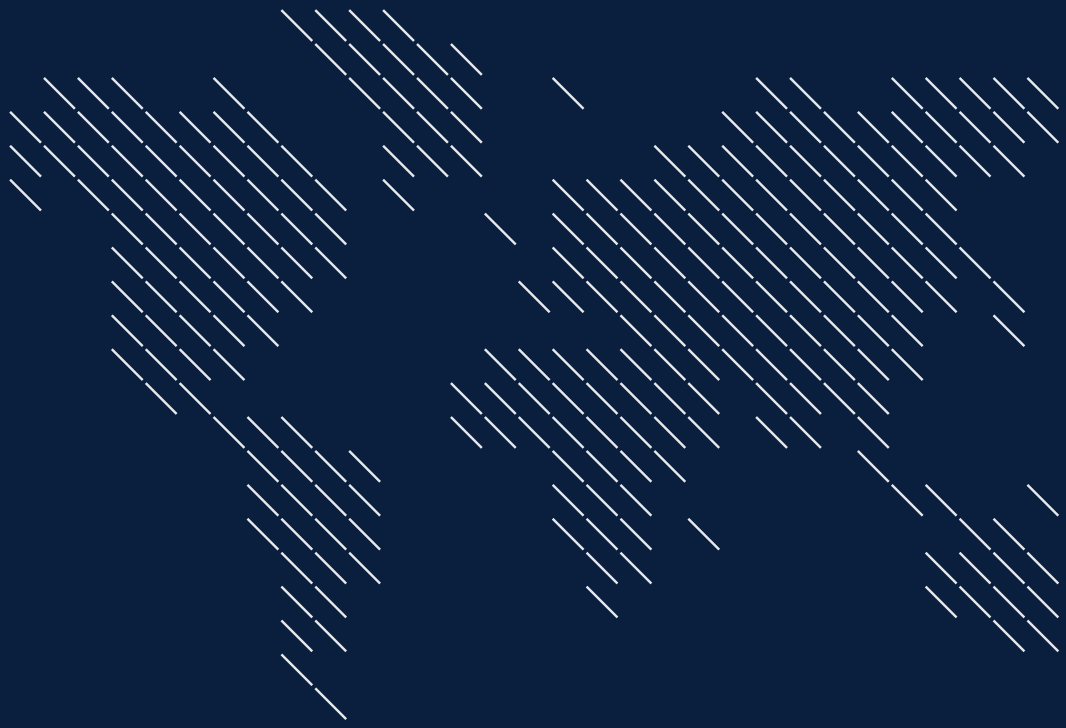
IVONNE SÁNCHEZ

Abogada especialista en Protección de Datos

ALEJANDRO CORTÉS

Perito Informático forense

eip
ESCUELA
INTERNACIONAL
POSGRADOS



C|EH CERTIFIED ETHICAL HACKER

OFFENSIVE Security OSCP

UEMC Universidad Europea Miguel de Cervantes

GRUPO MAINJOBS