UNIVERSIDAD
COMPLUTENSE
MADRID

ntic master

Máster de Formación Permanente en

CIBERSEGURIDAD DEFENSIVA Y OFENSIVA

2ª EDICIÓN

Facultad de Estudios Estadísticos
Universidad Complutense de Madrid

UNIVERSIDAD COMPLUTENSE MADRID

nticmaster

PROGRAMA

Módulo · Introducción a la Ciberseguridad

Módulo · Arquitectura de comunicaciones y seguridad

Módulo · Tecnología - Herramientas de Ciberseguridad

Módulo · Criptografía

Módulo · IA aplicada a la Ciberseguridad

Módulo · Operaciones - Red Team

Módulo · Operaciones - Blue Team

Módulo · Operaciones - Threat

Módulo · DFIR - Respuesta

Módulo · DFIR - Forense

Módulo · Inteligencia - OSINT

Módulo · Inteligencia - HUMINT

Módulo · Inteligencia - CORPINT

Módulo · Inteligencia - PSYOPS

Módulo · Inteligencia - Propaganda y guerra híbrida

Módulo · Inteligencia - Cibervigilancia

Módulo · GRC - Introducción

Módulo · GRC - Gobierno

Módulo · GRC - Cumplimiento

Módulo · GRC - Identidad

Módulo · RPA/IA Programación

Módulo · RPA/IA Automatización

Módulo · RPA/IA Inteligencia Artificial

TFM · Trabajo Final de Máster

La importancia de la Ciberseguridad

CONFIDENCIALIDAD DE LA INFORMACIÓN:
Proteger los datos sensibles es esencial. La confidencialidad garantiza que solo las personas autorizadas puedan acceder a la información, evitando filtraciones que puedan dañar la reputación o comprometer la seguridad de una organización.

INTEGRIDAD DE LOS DATOS:
La ciberseguridad asegura que la información no sea alterada sin autorización. Proteger la integridad de los datos es clave para que las decisiones basadas en ellos sean fiables y para evitar fraudes o errores en procesos críticos.

DISPONIBILIDAD DE LOS SISTEMAS:
Los sistemas deben estar accesibles cuando se necesiten. La ciberseguridad incluye medidas para evitar ataques como el ransomware o el DDoS, que pueden dejar fuera de servicio servicios esenciales para empresas o usuarios.

RESPUESTA ANTE INCIDENTES:
Tener un plan de acción frente a incidentes de seguridad permite reaccionar de forma rápida y efectiva ante ataques. Detectar, contener, erradicar y recuperar son fases clave para minimizar daños y restaurar la normalidad cuanto antes.

AUTENTICACIÓN Y CONTROL DE ACCESO:
Verificar la identidad de los usuarios antes de acceder a sistemas es fundamental. Mediante contraseñas seguras, autenticación multifactor o biometría, se evita que personas no autorizadas accedan a recursos confidenciales.

ANÁLISIS FORENSE DIGITAL:
La informática forense permite investigar incidentes de ciberseguridad recopilando y analizando evidencias digitales. Es clave para identificar cómo ocurrió un ataque, quién lo ejecutó y cómo evitar que vuelva a suceder, apoyando también acciones legales.

ACTUALIZACIÓN Y GESTIÓN DE VULNERABILIDADES:
Mantener los sistemas y programas actualizados es vital. Las actualizaciones corrigen fallos de seguridad que pueden ser explotados por atacantes, por lo que una buena gestión de parches reduce riesgos significativamente.

¿Por qué estudiar un Máster de Ciberseguridad?

En un mundo donde las amenazas digitales evolucionan constantemente, contar con **una formación especializada en Ciberseguridad es una ventaja competitiva clave**. Este programa ofrece una comprensión profunda de las tecnologías más innovadoras en protección de la información, incluyendo seguridad en redes, análisis forense digital y gestión de riesgos, permitiendo a los estudiantes aplicar estrategias de defensa en múltiples sectores.

El máster está diseñado con un enfoque práctico, donde **los alumnos trabajan en proyectos reales que les permiten desarrollar soluciones de ciberseguridad de manera eficiente y aplicable al entorno laboral**. Desde la prevención de ciberataques hasta la implementación de marcos de seguridad robustos, los estudiantes explorarán las prácticas más demandadas en la actualidad.

En una era impulsada por la digitalización, este máster capacita a los profesionales con conocimientos actualizados sobre ciberseguridad y el uso de herramientas avanzadas para proteger sistemas y datos de forma eficaz.

Además, los alumnos tendrán la oportunidad de **interactuar con expertos del sector, analizar casos de éxito en la gestión de ciberamenazas y desarrollar su propia visión estratégica** sobre la seguridad digital.

El objetivo fundamental del máster es **formar profesionales capaces de diseñar e implementar estrategias de ciberseguridad** en su campo de especialización, optimizando la protección de la información y desarrollando soluciones innovadoras para el futuro digital.

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

Duración

1 año académico

Modalidades

Presencial, Semipresencial y Online

Creditos ECTS

60

INFORMACIÓN

Modalidad Presencial

Viernes tarde y sábados mañana en la universidad

Modalidad Semipresencial

3 Semanas en presencial en la universidad y en la plataforma online

Modalidad Online

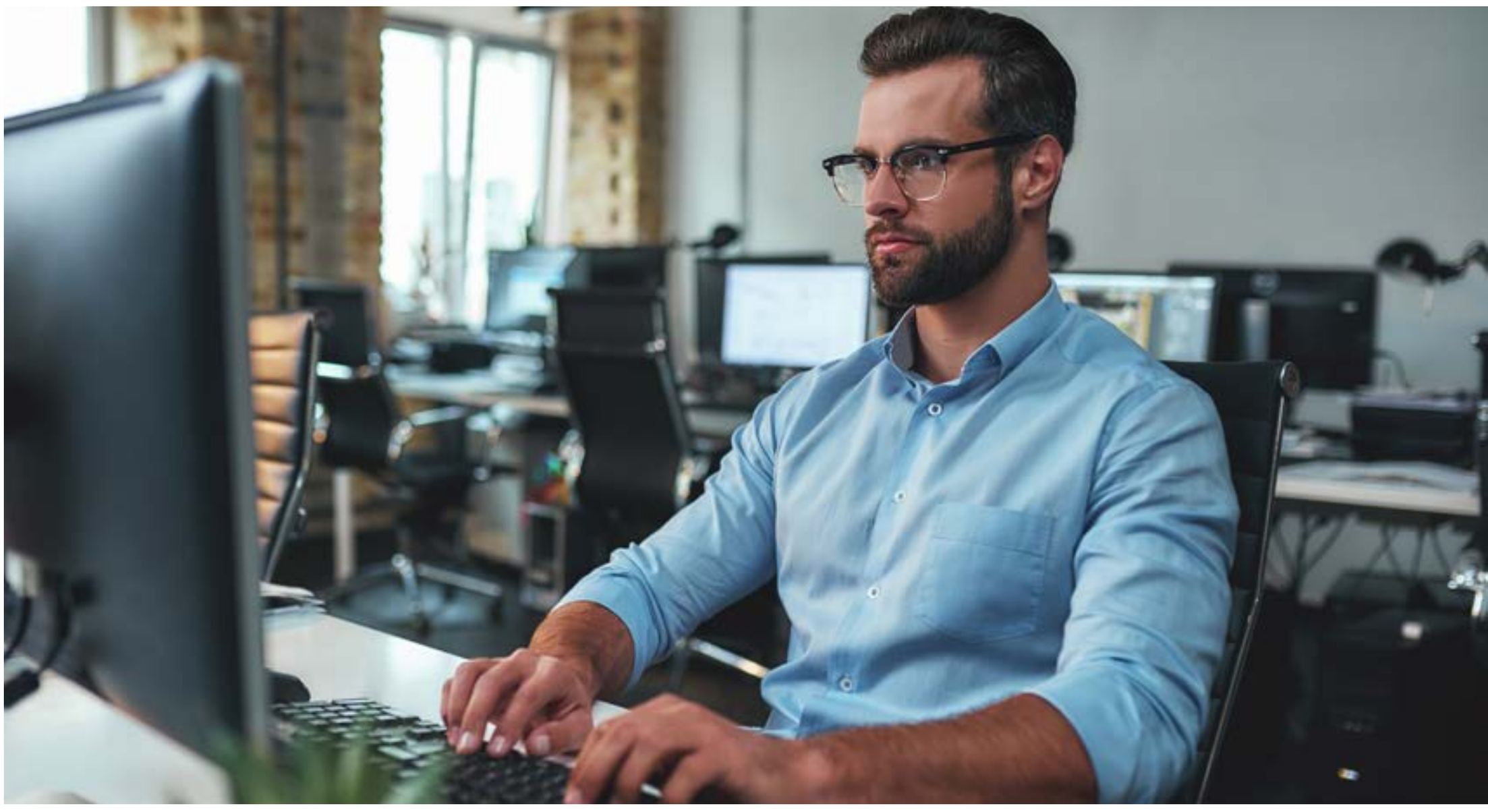
100% desde nuestra plataforma online

¿Por qué estudiar en la Universidad Complutense de Madrid?

La Universidad Complutense de Madrid (UCM) es una de las instituciones educativas más destacadas de Europa, reconocida por el prestigioso QS World Ranking como la mejor de España. Ofrece una amplia gama de oportunidades y beneficios para los estudiantes, así como una excelencia académica reconocida, una calidad docente de primer nivel. Ofrece alrededor de 90 títulos de grado y más de 30 dobles grados, más de 200 programas máster, además de estudios de formación permanente. La UCM tiene más de 500 años de historia y reconocimiento social. La Universidad Complutense de Madrid es la universidad española de referencia en 5 continentes.

El prestigio de la universidad está avalado por 7 Premios Nobel, 20 Príncipes de Asturias, 7 Premios Cervantes, Premios Nacionales de Investigación y a la Excelencia. La Universidad Complutense de Madrid tiene estudiantes de más de 90 países y convenios con universidades de los 5 continentes.

¿Por qué estudiar un Máster en Formación Permanente?



Si hay algo que afianza los conceptos teóricos de un programa educativo es la práctica.

Nuestros módulos formativos combinan una base teórica con ejercicios prácticos basados en situaciones reales de las empresas. Además, todos los módulos se evalúan con tareas prácticas, no con exámenes, tratándose de un programa de configuración eminentemente práctica.

La preparación del Trabajo Final de Máster (TFM) garantiza la puesta en práctica de todos los conceptos adquiridos a lo largo del curso, capacitando definitivamente al alumno para asumir responsabilidades dentro de un entorno laboral real.

PROGRAMA

Los módulos más completos de Ciberseguridad, diseñados para un aprendizaje eficaz y accesible para el alumno.

UNIVERSIDAD COMPLUTENSE MADRID

nticmaster

MÓDULO

Introducción a la Ciberseguridad

El primer módulo de nuestro Máster en Ciberseguridad está diseñado para ofrecer una comprensión integral de los fundamentos de la ciberseguridad, así como una visión detallada de los roles, actividades y el ecosistema global en este campo.

Introducción a la ciberseguridad

La primera sección, Introducción a la Ciberseguridad, proporciona una visión general de la importancia y la evolución de la ciberseguridad en el mundo moderno. Los estudiantes explorarán **los conceptos fundamentales y la terminología básica, adquiriendo una comprensión sólida de términos esenciales como amenazas, vulnerabilidades, riesgos y ataques**. Se analizarán los diferentes tipos de amenazas cibernéticas, desde malware y ransomware hasta ataques de phishing y DDoS, así como las estrategias básicas de defensa que pueden emplearse para mitigar estos riesgos. Además, se introducirá a los estudiantes en el modelo de la triada de confidencialidad, integridad y disponibilidad (CIA triad), que es un pilar central en la protección de la información.

Roles y actividades en ciberseguridad

La segunda sección, Roles y Actividades en Ciberseguridad, profundiza en los diversos roles y responsabilidades que existen dentro del ámbito de la ciberseguridad. Los estudiantes aprenderán sobre las **funciones y competencias de distintos profesionales, tales como analistas de seguridad, ingenieros de redes, gestores de riesgos y especialistas en respuesta a incidentes**. Se destacará la importancia de la colaboración interdisciplinaria y la comunicación efectiva entre los equipos de ciberseguridad para garantizar una defensa sólida contra las amenazas cibernéticas. Esta sección también explorará las diferentes **rutas profesionales y oportunidades de desarrollo en el campo de la ciberseguridad, proporcionando una guía clara sobre cómo avanzar y especializarse en esta área**.

Ecosistema de la ciberseguridad*

Finalmente, la tercera sección, Ecosistema de la Ciberseguridad, ofrece una visión completa del entorno global de la ciberseguridad. Los estudiantes examinarán las principales **organizaciones y asociaciones** que desempeñan un papel crucial en la configuración de políticas y estándares de ciberseguridad a nivel mundial. Se discutirá el impacto de las tecnologías emergentes, como la inteligencia artificial, el Internet de las Cosas (IoT) y la computación en la nube, en la seguridad digital. Además, se analizarán **las tendencias actuales y futuras en ciberseguridad, permitiendo a los estudiantes estar al tanto de las innovaciones y desafíos que enfrentarán en el futuro**.

UNIVERSIDAD COMPLUTENSE MADRID

nticmaster

MÓDULO

Arquitectura de comunicaciones y seguridad

El segundo módulo del Máster en Ciberseguridad se centra en la arquitectura de comunicaciones y seguridad. Este módulo ofrece una comprensión profunda de **cómo se diseñan, implementan y protegen las infraestructuras de comunicación en diversas tecnologías y entornos**. El módulo se divide en tres secciones principales: Arquitectura de Comunicaciones y Seguridad (I), Arquitectura de Comunicaciones y Seguridad (II): Cloud, Fog, EDGE/P2P, y Arquitectura de Comunicaciones y Seguridad (III): Modelos ZeroTrust.

Los estudiantes obtendrán una base sólida en los principios y prácticas de diseño de arquitecturas de comunicaciones seguras. Se cubrirán temas como los modelos de referencia OSI y TCP/IP, la segmentación de redes, el uso de firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS). Los estudiantes aprenderán sobre **la importancia de la segmentación de redes y el aislamiento de segmentos críticos para minimizar el impacto de posibles ataques**. Además, se discutirán las prácticas recomendadas para la configuración y gestión de firewalls y otros dispositivos de seguridad perimetral.

Se abordarán las arquitecturas de comunicaciones y seguridad en entornos de computación en la nube, Fog Computing y EDGE/P2P. Los estudiantes explorarán los desafíos específicos y las estrategias de seguridad asociadas con cada uno de estos entornos.

Computación en la Nube

Se analizarán los **modelos de servicio (IaaS, PaaS, SaaS) y los modelos de despliegue (pública, privada, híbrida),** junto con las estrategias de seguridad específicas para cada uno. Se discutirán temas como la gestión de identidades y accesos, la encriptación de datos en tránsito y en reposo, y las prácticas de seguridad en la configuración de entornos de nube.

Fog Computing

Esta parte del módulo se centrará en la seguridad en entornos de Fog Computing, donde **los datos se procesan localmente cerca de la fuente de generación antes de ser enviados a la nube**. Se explorarán las ventajas y desafíos de esta arquitectura, incluyendo la gestión de dispositivos y la seguridad de los datos en nodos intermedios.

EDGE/P2P

Se analizarán las arquitecturas EDGE y P2P, **donde el procesamiento de datos se realiza en dispositivos de borde o entre pares**. Los estudiantes aprenderán sobre las técnicas de seguridad para proteger los datos y asegurar la comunicación entre dispositivos en estos entornos descentralizados.

Modelos ZeroTrust

Se dedicará a los modelos ZeroTrust, un enfoque moderno y robusto para la seguridad de la información. En lugar de confiar implícitamente en usuarios o dispositivos dentro de la red, **el modelo ZeroTrust asume que cada intento de acceso puede ser una potencial amenaza y requiere verificación constante**.

Los estudiantes aprenderán sobre los principios fundamentales del modelo ZeroTrust, que incluyen **la autenticación continua, la autorización basada en el contexto y el monitoreo exhaustivo de la actividad de la red**. Se discutirán las estrategias para implementar ZeroTrust en una organización, tales como la microsegmentación, la gestión de identidades y accesos (IAM), y el uso de tecnologías como multifactor authentication (MFA) y políticas de acceso basadas en el riesgo.

También se explorarán c**asos de estudio y ejemplos prácticos de organizaciones que han adoptado exitosamente el modelo ZeroTrust**, proporcionando a los estudiantes una visión práctica de cómo esta arquitectura puede mejorar significativamente la seguridad de la información en entornos empresariales.

MÓDULO

Herramientas de ciberseguridad

El tercer módulo del Máster en Ciberseguridad se centra en las tecnologías fundamentales y avanzadas utilizadas en la protección y defensa de los sistemas informáticos y redes. Este módulo está diseñado para proporcionar a los estudiantes **una comprensión profunda de las herramientas y tecnologías que forman la base de las prácticas modernas de ciberseguridad**. El módulo se divide en dos secciones principales: Herramientas de Ciberseguridad (I) y Herramientas de Ciberseguridad (II).

Los estudiantes explorarán las herramientas esenciales utilizadas para la protección y monitorización de sistemas informáticos y redes. **Se abordarán las herramientas de análisis de vulnerabilidades, sistemas de detección y prevención de intrusiones (IDS/IPS), y plataformas de gestión de eventos e información de seguridad (SIEM)**.

Análisis de Vulnerabilidades

Los estudiantes aprenderán a utilizar herramientas como **Nessus, OpenVAS y Qualys para identificar y evaluar vulnerabilidades en sistemas y redes**. Se cubrirán las mejores prácticas para realizar análisis de vulnerabilidades y cómo interpretar los resultados para aplicar correcciones efectivas.

Sistemas de Detección y Prevención de Intrusiones (IDS/IPS)

Esta parte del módulo se centrará en la configuración y uso de herramientas **IDS/IPS como Snort, Suricata y Bro (Zeek).** Los estudiantes aprenderán cómo estas herramientas pueden detectar y prevenir actividades maliciosas en la red, y cómo configurar reglas y políticas para maximizar su efectividad.

Gestión de Eventos e Información de Seguridad (SIEM)

Los estudiantes explorarán plataformas **SIEM como Splunk, ELK Stack (Elasticsearch, Logstash, Kibana) y IBM QRadar.** Se discutirán las funcionalidades clave de los SIEM, incluyendo la recolección y correlación de logs, la detección de amenazas en tiempo real y la generación de informes de seguridad. También se cubrirá la integración de SIEM con otras herramientas de seguridad y cómo utilizarlos para una respuesta rápida a incidentes.

Se abordarán las herramientas de análisis forense, pruebas de penetración, y gestión de parches y configuraciones.

Análisis Forense

Los estudiantes aprenderán a utilizar herramientas forenses como EnCase, FTK (Forensic Toolkit) y Autopsy. Se cubrirán técnicas para la adquisición y análisis de evidencias digitales, la reconstrucción de eventos y la preservación de la cadena de custodia. También se discutirán casos de estudio para ilustrar la aplicación práctica de estas herramientas en investigaciones forenses.

Pruebas de Penetración

Esta parte del módulo se centrará en herramientas de pruebas de penetración como **Metasploit, Burp Suite y OWASP ZAP.** Los estudiantes aprenderán cómo realizar pruebas de penetración para identificar y explotar vulnerabilidades en aplicaciones y sistemas. Se cubrirán técnicas de escaneo, explotación y post-explotación, así como la generación de informes de hallazgos y recomendaciones.

Gestión de Parches y Configuraciones

Los estudiantes explorarán herramientas para la gestión de parches y configuraciones como **Microsoft SCCM, Ansible y Puppet.** Se discutirá la importancia de mantener los sistemas actualizados y configurados de manera segura, y cómo estas herramientas pueden automatizar el proceso de aplicación de parches y la gestión de configuraciones.

Otras Herramientas Especializadas

Además, se introducirán otras herramientas especializadas que son útiles en diferentes contextos de ciberseguridad, como h**erramientas de análisis de tráfico de red (Wireshark), herramientas de cifrado y criptografía (OpenSSL), y plataformas de simulación de ataques (Caldera, Atomic Red Team)**.

MÓDULO

Criptografía

El cuarto módulo del Máster en Ciberseguridad se centra en la criptografía, una de las áreas más críticas y fundamentales de la seguridad de la información. Este módulo está diseñado para proporcionar a los estudiantes una comprensión profunda de los principios y aplicaciones de la criptografía, así como de las técnicas y herramientas utilizadas para proteger la confidencialidad, integridad y autenticidad de la información. El módulo se divide en una sección principal: Criptografía Aplicada.

Criptografía Aplicada

En esta sección, los estudiantes explorarán los **conceptos teóricos y las aplicaciones prácticas de la criptografía**. Se cubrirán tanto los fundamentos matemáticos como las implementaciones prácticas de algoritmos criptográficos en diversos contextos.

Fundamentos de la Criptografía

Los estudiantes comenzarán con una introducción a los conceptos básicos de la criptografía, incluyendo la historia y evolución de la criptografía, **los principios de cifrado y descifrado, y la diferencia entre criptografía simétrica y asimétrica**. Se discutirán los algoritmos de cifrado clásico, como el cifrado César y el cifrado de Vigenère, y su relevancia histórica.

Criptografía Simétrica

Esta parte del módulo se centrará en los algoritmos de criptografía simétrica, donde l**a misma clave se utiliza tanto para cifrar como para descifrar la información**. Los estudiantes aprenderán sobre **algoritmos de cifrado de bloque y de flujo, como DES (Data Encryption Standard), 3DES, AES (Advanced Encryption Standard) y RC4**. Se discutirán las ventajas y limitaciones de cada algoritmo, así como las técnicas para asegurar la gestión y distribución segura de claves.

Criptografía Asimétrica

A continuación, se explorarán los algoritmos de criptografía asimétrica, donde se utilizan **claves públicas y privadas diferentes para cifrar y descifrar la información**. Los estudiantes estudiarán algoritmos como RSA (Rivest-Shamir-Adleman), Diffie-Hellman y ECC (Elliptic Curve Cryptography). Se explicará cómo estos algoritmos permiten la creación de firmas digitales y el establecimiento de canales de comunicación seguros.

Funciones Hash y Firmas Digitales

Los estudiantes aprenderán sobre las funciones hash criptográficas, como SHA (Secure Hash Algorithm) y MD5, y su papel en la integridad de los datos. Se discutirá **cómo las firmas digitales utilizan la criptografía asimétrica para verificar la autenticidad y la integridad de los mensajes**. Se presentarán casos de uso comunes de funciones hash y firmas digitales en la seguridad de la información.

Protocolos Criptográficos

Esta parte del módulo se centrará en los protocolos criptográficos que utilizan algoritmos de cifrado para asegurar las comunicaciones. Se cubrirán **protocolos como SSL/TLS (Secure Sockets Layer / Transport Layer Security), que aseguran las comunicaciones en la web, y IPsec (Internet Protocol Security), que asegura las comunicaciones a nivel de red**. Los estudiantes aprenderán cómo estos protocolos utilizan criptografía para proporcionar confidencialidad, integridad y autenticación.

Criptografía en la Práctica

Los estudiantes explorarán aplicaciones prácticas de la criptografía en diversos contextos, incluyendo el uso de criptografía en sistemas de **almacenamiento seguro, criptomonedas y blockchain, y la protección de datos en aplicaciones móviles y dispositivos IoT** (Internet of Things). Se discutirán casos de estudio y ejemplos reales de cómo la criptografía se utiliza para proteger la información en diferentes industrias.

Criptografía Cuántica

Finalmente, se introducirá a los estudiantes en el campo emergente de **la criptografía cuántica y la criptografía resistente a la computación cuántica**. Se explicará cómo los avances en la computación cuántica podrían afectar la seguridad de los algoritmos criptográficos actuales y qué medidas se están tomando para desarrollar algoritmos resistentes a la computación cuántica. El módulo está dedicado a la inteligencia artificial (IA) y su aplicación en el campo de la ciberseguridad. Este módulo ofrece una comprensión profunda de cómo las técnicas y herramientas de IA pueden ser utilizadas para mejorar la detección, prevención y respuesta a las amenazas cibernéticas. La única sección en este módulo es Introducción a los Copilot/ LLM en Ciberseguridad.

MÓDULO

Inteligencia artificial aplicada a la ciberseguridad

El módulo está dedicado a la inteligencia artificial (IA) y su aplicación en el campo de la ciberseguridad. Este módulo ofrece una comprensión profunda de cómo las técnicas y herramientas de IA pueden ser utilizadas para mejorar la detección, prevención y respuesta a las amenazas cibernéticas. La única sección en este módulo es Introducción a los Copilot/LLM en Ciberseguridad.

Introducción a los Copilot/LLM en Ciberseguridad

En esta sección, los estudiantes explorarán el papel de la inteligencia artificial, específicamente **los modelos de lenguaje de gran escala (LLM, por sus siglas en inglés) y las herramientas de asistencia inteligente (Copilots)**, en la ciberseguridad. Se cubrirán tanto los fundamentos teóricos como las aplicaciones prácticas de estas tecnologías emergentes.

Fundamentos de la Inteligencia Artificial en Ciberseguridad

Los estudiantes comenzarán con una introducción a los conceptos básicos de la inteligencia artificial y el aprendizaje automático (machine learning), incluyendo una visión general de los tipos de algoritmos de IA, como el aprendizaje supervisado, no supervisado y de refuerzo. Se discutirá cómo estos **algoritmos pueden ser aplicados en el contexto de la ciberseguridad para mejorar la detección de amenazas,** la respuesta a incidentes y la automatización de tareas.

Modelos de Lenguaje de Gran Escala (LLM)

Esta parte del módulo se centrará en **los modelos de lenguaje de gran escala, como GPT-4, y su aplicación en ciberseguridad**. Los estudiantes aprenderán cómo estos modelos pueden procesar y analizar grandes volúmenes de datos textuales para identificar patrones y anomalías que podrían indicar una amenaza. Se explorarán casos de uso específicos, como la detección de phishing, el análisis de logs de seguridad y la generación de informes de incidentes.

Herramientas de Asistencia Inteligente (Copilots)

Los estudiantes también explorarán las herramientas de asistencia inteligente, o Copilots, que utilizan IA para asistir a los profesionales de la ciberseguridad en sus tareas diarias. Estas herramientas pueden **proporcionar sugerencias en tiempo real, automatizar tareas repetitivas y mejorar la eficiencia de los analistas de seguridad**. Se discutirán ejemplos de Copilots en ciberseguridad, como asistentes de análisis de malware, herramientas de respuesta a incidentes y sistemas de gestión de vulnerabilidades.

Aplicaciones Prácticas de la IA en Ciberseguridad

Los estudiantes aprenderán cómo implementar y utilizar técnicas de IA en diversas áreas de la ciberseguridad. Se cubrirán aplicaciones prácticas como l**a detección de intrusiones, la prevención de fraudes, el análisis de comportamiento de usuarios y entidades (UEBA), y la identificación de amenazas avanzadas persistentes (APT)**. Los estudiantes también aprenderán a integrar herramientas de IA con sistemas de gestión de eventos e información de seguridad (SIEM) y otras infraestructuras de seguridad.

Desafíos y Limitaciones de la IA en Ciberseguridad

Además de las aplicaciones prácticas, se discutirán los desafíos y limitaciones del uso de la IA en ciberseguridad. Los estudiantes explorarán temas como **los sesgos en los datos de entrenamiento, la interpretabilidad de los modelos de IA y la necesidad de supervisión humana en los sistemas de IA**. También se discutirán las posibles amenazas que la IA puede presentar, como la generación de ataques automatizados y la manipulación de sistemas de IA por actores malintencionados.

Tendencias Futuras en IA y Ciberseguridad

Finalmente, los estudiantes analizarán las **tendencias emergentes en el uso de la IA en ciberseguridad y las oportunidades futuras en este campo**. Se explorarán áreas de investigación en curso, como el uso de la IA para la ciberdefensa proactiva, la simulación de ataques y la ciberinteligencia. Se discutirá cómo las organizaciones pueden prepararse para aprovechar estas tecnologías emergentes y mantenerse a la vanguardia de la ciberseguridad.

MÓDULO

Operaciones – Red Team

El módulo de Operaciones (Red Team) del Máster en Ciberseguridad está diseñado para proporcionar a los estudiantes una **comprensión profunda y práctica de las técnicas y estrategias utilizadas por los equipos de Red Team para evaluar y mejorar la seguridad de una organización**. Este módulo se divide en tres áreas fundamentales: Red Team y Purple Team, Ingeniería Inversa y Exploiting, e Introducción al Hacking de Hardware.

Red Team y Purple Team

Esta sección se centra en las metodologías y técnicas utilizadas por los equipos de Red Team y Purple Team. **Los equipos de Red Team simulan ataques reales** para identificar vulnerabilidades y evaluar la efectividad de las defensas de seguridad, mientras que los equipos de **Purple Team facilitan la colaboración entre los Red Team y los Blue Team (defensores)** para mejorar la postura de seguridad de una organización.

Metodologías de Red Team

Los estudiantes aprenderán sobre las fases del ciclo de vida de un ataque del Red Team, que incluyen **reconocimiento, enumeración, explotación, escalada de privilegios, movimiento lateral, persistencia y exfiltración de datos**. Se discutirán herramientas y técnicas comunes utilizadas en cada fase, así como la planificación y ejecución de ejercicios de Red Team.

Simulación de Ataques

Los estudiantes practicarán la simulación de ataques utilizando herramientas como **Metasploit, Cobalt Strike y PowerShell Empire**. Se explorarán escenarios de ataque realistas y se analizarán las tácticas, técnicas y procedimientos (TTP) utilizados por atacantes avanzados.

Colaboración con Purple Team

Se destacará la importancia de la **colaboración entre Red Team y Blue Team a través del enfoque Purple Team**. Los estudiantes aprenderán cómo los ejercicios de Purple Team pueden mejorar la detección y respuesta a incidentes, y cómo integrar las lecciones aprendidas en las defensas de seguridad.

Ingeniería Inversa y Exploiting

Esta sección profundiza en las técnicas de ingeniería inversa y explotación de vulnerabilidades. La ingeniería inversa se utiliza para **comprender el funcionamiento interno de software y sistemas, mientras que el exploiting se centra en encontrar y aprovechar vulnerabilidades** para obtener acceso no autorizado o control sobre los sistemas.

Fundamentos de Ingeniería Inversa

Los estudiantes aprenderán sobre las **herramientas y técnicas básicas de ingeniería inversa, incluyendo el uso de desensambladores (IDA Pro, Ghidra) y depuradores (OllyDbg, x64dbg)**. Se cubrirán conceptos como análisis estático y dinámico, análisis de código máquina y reversing de binarios.

Análisis de Malware

Los estudiantes practicarán la **ingeniería inversa de muestras de malware para entender su comportamiento y características**. Se discutirán técnicas para identificar y neutralizar técnicas de ofuscación y evasión utilizadas por el malware.

Explotación de Vulnerabilidades

Los estudiantes aprenderán a identificar y explotar vulnerabilidades en software y sistemas. Se cubrirán **técnicas de explotación como desbordamiento de búfer, inyección de código, y escalada de privilegios**. También se discutirá la creación y uso de exploits, así como la mitigación de estas vulnerabilidades.

MÓDULO

Operaciones – Red Team

Introducción al Hacking de Hardware

Esta sección introduce a los estudiantes en el mundo del hacking de hardware, una disciplina que involucra **la manipulación y explotación de dispositivos físicos** para comprometer su seguridad.

Fundamentos de Hacking de Hardware

Los estudiantes aprenderán sobre los conceptos básicos de hacking de hardware, incluyendo **la identificación de componentes y arquitecturas de hardware, la comprensión de protocolos de comunicación** (I2C, SPI, UART) y el uso de herramientas de análisis de hardware.

Ataques Físicos y Electrónicos

Se explorarán técnicas para realizar **ataques físicos y electrónicos en dispositivos de hardware, tales como manipulación de firmware, ataques de side-channel (canales laterales) y la inyección de fallos**. Los estudiantes aprenderán a utilizar herramientas como programadores de chips, osciloscopios y analizadores lógicos.

Seguridad en Dispositivos IoT

Los estudiantes analizarán la seguridad de dispositivos IoT (Internet de las Cosas), aprendiendo a **identificar y explotar vulnerabilidades en dispositivos conectados**. Se discutirán técnicas para asegurar dispositivos IoT y protegerlos contra ataques físicos y electrónicos.

MÓDULO

Operaciones – Blue Team

El módulo de Operaciones (Blue Team) del Máster en Ciberseguridad está diseñado para proporcionar a los estudiantes una comprensión profunda y práctica de las **estrategias, técnicas y herramientas utilizadas por los equipos de Blue Team para defender y proteger los sistemas y redes** de una organización contra amenazas cibernéticas. Este módulo se divide en varias secciones, cada una enfocada en aspectos críticos de la defensa cibernética: Seguridad Perimetral y Elementos de Seguridad en Empresa, Detección, Correlación y Acción, Infraestructuras Críticas, Gestión de Identidad y Autenticación, Operaciones de Seguridad General, y Smart Contracts y el Mundo de las Criptomonedas.

Seguridad Perimetral y Elementos de Seguridad en Empresa

Esta sección se centra en la protección del perímetro de la red y los elementos de seguridad esenciales tanto en entornos on-premise como en la nube.

Seguridad Perimetral On-Premise

Los estudiantes aprenderán sobre la **configuración y gestión de firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), y gateways de seguridad**. Se cubrirán técnicas para segmentar y aislar redes críticas, implementar políticas de control de acceso y monitorear el tráfico de red para detectar actividades sospechosas.

Seguridad en la Nube

Los estudiantes explorarán las mejores prácticas para **asegurar infraestructuras en la nube, incluyendo la configuración de entornos seguros en plataformas como AWS, Azure y Google Cloud**. Se discutirán temas como la gestión de identidades y accesos (IAM), la encriptación de datos, y la implementación de soluciones de seguridad específicas para la nube.

Detección, Correlación y Acción

Esta sección se enfoca en las **técnicas y herramientas utilizadas para detectar, correlacionar y responder a incidentes** de seguridad en tiempo real.

Sistemas de Monitoreo y Detección

Los estudiantes aprenderán a utilizar sistemas de monitoreo y detección como **SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), y NDR (Network Detection and Response)**. Se discutirá cómo recolectar y analizar logs de eventos, identificar patrones sospechosos y generar alertas de seguridad.

Correlación de Eventos

Los estudiantes explorarán técnicas para correlacionar **eventos de seguridad de múltiples fuentes para identificar incidentes complejos y persistentes**. Se cubrirán herramientas y metodologías para la correlación de eventos y el análisis de tendencias de amenazas.

Respuesta a Incidentes

Los estudiantes practicarán la respuesta a incidentes de seguridad, desarrollando **planes de respuesta y procedimientos para contener, erradicar y recuperar de incidentes**. Se discutirán las mejores prácticas para la comunicación y coordinación durante un incidente de seguridad.

MÓDULO

Operaciones – Blue Team

Introducción a las Infraestructuras Críticas

Esta sección introduce a los estudiantes en la protección de **infraestructuras críticas, tales como sistemas de energía, transporte, agua y telecomunicaciones**.

Identificación de Infraestructuras Críticas

Los estudiantes aprenderán a **identificar y categorizar infraestructuras críticas** dentro de una organización y comprenderán su importancia para la seguridad nacional y la continuidad del negocio.

Protección de Infraestructuras Críticas

Se explorarán las mejores prácticas y estándares para **proteger infraestructuras críticas contra amenazas cibernéticas**, incluyendo la implementación de controles de seguridad, la gestión de riesgos y la colaboración con entidades gubernamentales y privadas.

Gestión de Identidad y Autenticación

Esta sección se centra en la **gestión de identidades y los mecanismos de autenticación y autorización** utilizados para proteger el acceso a sistemas y datos.

Gestión de Identidades (IAM)

Los estudiantes aprenderán sobre las tecnologías y prácticas para la **gestión de identidades y acceso**s (IAM), incluyendo directorios de usuarios, federación de identidades y autenticación multifactor (MFA).

Autenticación y Autorización

Se discutirán métodos de autenticación seguros, como **biometría, tokens de hardware y contraseñas seguras**. También se cubrirán las políticas de autorización basadas en roles (RBAC) y atributos (ABAC) para controlar el acceso a recursos.

Operaciones de Seguridad General

Esta sección proporciona una visión general de las **operaciones de seguridad diarias y la gestión** de la seguridad en una organización.

Centro de Operaciones de Seguridad (SOC)

Los estudiantes aprenderán sobre la función y operación de un SOC, incluyendo la **monitorización continua, la gestión de incidentes y la coordinación** con otros equipos de seguridad.

Automatización y Orquestación

Se explorarán herramientas y técnicas para la **automatización de tareas de seguridad y la orquestación de respuestas a incidentes** utilizando plataformas como SOAR (Security Orchestration, Automation and Response).

Smart Contracts y el Mundo de las Criptomonedas

Esta sección introduce a los estudiantes en la seguridad de los **contratos inteligentes y las criptomonedas**, áreas emergentes en la ciberseguridad.

Contratos Inteligentes

Los estudiantes aprenderán sobre los fundamentos de los contratos inteligentes, **cómo se implementan en plataformas blockchain como Ethereum y las vulnerabilidades** comunes que pueden afectar a los contratos inteligentes.

Seguridad en Criptomonedas

Se explorarán las **amenazas y técnicas de seguridad asociadas con el uso y almacenamiento de criptomonedas**, incluyendo ataques a billeteras digitales, exchanges y la protección contra fraudes y robos.

MÓDULO

Operaciones – Threat

El módulo de Operaciones (Threat) del Máster en Ciberseguridad se enfoca en el **análisis, modelado y comprensión de las amenazas cibernéticas**. Este módulo está diseñado para proporcionar a los estudiantes las habilidades y conocimientos necesarios para identificar, analizar y mitigar amenazas avanzadas. El módulo se divide en cuatro secciones principales: Modelado de Amenazas y Comprensión de Adversarios, Tácticas, Técnicas y Procedimientos (TTPs), Repaso de Adversarios Relevantes, y Caso de Uso y Ejercicio Práctico.

Modelado de Amenazas y Comprensión de Adversarios (I)

En esta primera sección, los estudiantes aprenderán a modelar amenazas y comprender las motivaciones, capacidades y métodos de los adversarios cibernéticos.

Conceptos Fundamentales

Se introducirá a los estudiantes en los **conceptos básicos del modelado de amenazas**, incluyendo la identificación y categorización de amenazas, la evaluación de riesgos y la priorización de amenazas basadas en el impacto y la probabilidad.

Metodologías de Modelado de Amenazas

Los estudiantes explorarán diferentes metodologías de modelado de amenazas, como **STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) y ATT&CK de MITRE**. Se discutirán las ventajas y limitaciones de cada metodología y cómo aplicarlas en diferentes contextos.

Análisis de Adversarios

Se enseñará a los estudiantes a realizar **análisis de adversarios, incluyendo la recopilación de inteligencia sobre actores de amenazas**, la comprensión de sus objetivos y tácticas, y la evaluación de su capacidad para llevar a cabo ataques cibernéticos.

Modelado de Amenazas y Comprensión de Adversarios (II): TTPs

En esta sección, los estudiantes profundizarán en las tácticas, técnicas y procedimientos (TTPs) utilizados por los adversarios cibernéticos.

Tácticas y Técnicas

Los estudiantes aprenderán a **identificar y analizar las tácticas y técnicas empleadas por los adversarios** en las diferentes fases de un ataque cibernético, como la fase de reconocimiento, la obtención de acceso inicial, la ejecución de código, la persistencia, la escalada de privilegios, el movimiento lateral, la exfiltración de datos y la evasión de defensas.

Procedimientos

Se discutirá cómo los adversarios utilizan **procedimientos específicos para llevar a cabo sus ataques, incluyendo la utilización de herramientas y exploits** comunes, la configuración de infraestructura de comando y control (C2) y la implementación de técnicas de ocultación y evasión.

Uso de MITRE ATT&CK

Los estudiantes aprenderán a **utilizar el framework MITRE ATT&CK para mapear y analizar las TTPs** de los adversarios, identificando patrones de ataque y desarrollando estrategias de mitigación y defensa.

MÓDULO

Operaciones – Threat

Modelado de Amenazas y Comprensión de Adversarios (III): Repaso de Adversarios Relevantes

Esta sección se enfoca en el estudio de adversarios relevantes y sus campañas de ataque.

Adversarios Estatales y No Estatales

Los estudiantes analizarán ejemplos de **adversarios estatales y no estatales, comprendiendo sus motivaciones, capacidades y objetivos**. Se estudiarán casos de ataques cibernéticos atribuidos a grupos patrocinados por el estado, organizaciones criminales, hacktivistas y grupos de amenazas persistentes avanzadas (APT).

Campañas de Ataque

Se revisarán campañas de ataque notables llevadas a cabo por estos adversarios, evaluando las tácticas y técnicas empleadas, **el impacto de los ataques y las lecciones aprendidas**. Los estudiantes aprenderán a utilizar esta información para mejorar las defensas de sus organizaciones.

Inteligencia de Amenazas

Se discutirá el papel de la inteligencia de amenazas en la comprensión y mitigación de las amenazas cibernéticas, incluyendo **la recopilación y análisis de datos de inteligencia, la integración de inteligencia en operaciones de seguridad** y la colaboración con comunidades de intercambio de información.

Modelado de Amenazas y Comprensión de Adversarios (IV): Caso de Uso y Ejercicio Práctico

En esta última sección, los estudiantes aplicarán lo aprendido en un caso de uso y ejercicio práctico.

Desarrollo de un Caso de Uso

Los estudiantes trabajarán en el desarrollo de **un caso de uso basado en un escenario de amenaza realista**. Se les proporcionará información sobre un adversario y una campaña de ataque específica, y se les pedirá que **modelen la amenaza, analicen las TTPs utilizadas y desarrollen estrategias de mitigación y defensa**.

Ejercicio Práctico

Los estudiantes participarán en un ejercicio práctico donde simularán la respuesta a un ataque cibernético. **Trabajarán en equipos para identificar las TTPs empleadas por el adversario, implementar medidas de mitigación y coordinar la respuesta al incidente**. Este ejercicio les permitirá aplicar sus conocimientos en un entorno controlado y recibir retroalimentación sobre su desempeño.

Revisión y Lecciones Aprendidas

Al finalizar el ejercicio, los estudiantes **revisarán sus acciones y discutirán las lecciones aprendidas. Se enfatizará la importancia de la mejora continua** en la defensa cibernética y cómo aplicar las experiencias adquiridas en situaciones reales.

MÓDULO

DFIR – Respuesta

El módulo de DFIR (**Digital Forensics and Incident Respons**e) con enfoque en Respuesta del Máster en Ciberseguridad está diseñado para proporcionar a los estudiantes una comprensión profunda y práctica de las **metodologías, técnicas y herramientas utilizadas en la respuesta a incidentes de seguridad informática.** En este módulo, los estudiantes obtendrán una base sólida sobre los conceptos y principios fundamentales de la respuesta a incidentes de seguridad.

Definición

Comenzarán con una definición clara de lo que constituye un incidente de seguridad y los objetivos principales de una respuesta efectiva, destacando la importancia de minimizar el impacto, contener el incidente, recuperar operaciones normales y prevenir futuros incidentes. Explorarán los **diferentes tipos de incidentes que pueden ocurrir, incluyendo malware, ataques de denegación de servicio (DDoS), intrusiones de red, robo de datos y abuso interno, analizando cada tipo en términos de sus características y desafíos específicos**. Se introducirá un marco estructurado para la respuesta a incidentes, que incluirá las fases de preparación, identificación, contención, erradicación, recuperación y lecciones aprendidas, proporcionando una guía sistemática para manejar incidentes de seguridad de manera eficiente.

Desarrollo

En la fase de desarrollo de planes de respuesta, los estudiantes aprenderán a **desarrollar y documentar planes de respuesta a incidentes detallados y efectivos**. Discutirán la importancia de la preparación y planificación, estableciendo **políticas de seguridad, procedimientos operativos estándar (SOP) y equipos de respuesta a incidentes (IRT) bien definidos**. Trabajarán en la creación de políticas y procedimientos específicos para la respuesta a incidentes, abordando aspectos como la gestión de comunicaciones durante un incidente, la asignación de roles y responsabilidades y la documentación detallada de cada fase de la respuesta. Además, se enfatizará la importancia de realizar simulaciones y ejercicios de mesa para probar y refinar los planes de respuesta a incidentes, participando en ejercicios prácticos para evaluar la efectividad de sus planes y hacer ajustes según sea necesario.

Ejecución

Durante la fase de ejecución de la respuesta, los estudiantes se enfocarán en la ejecución práctica de la respuesta a incidentes, cubriendo desde la identificación inicial hasta la recuperación completa. Aprenderán sobre las técnicas y herramientas para detectar y alertar sobre incidentes de seguridad en tiempo real, utilizando **sistemas de detección y prevención de intrusiones (IDS/IPS), sistemas de gestión de eventos e información de seguridad (SIEM) y otros mecanismos de monitoreo**. Profundizarán en los métodos para identificar y contener incidentes de manera rápida y efectiva, evaluando el alcance y el impacto del incidente, aislando sistemas afectados y evitando la propagación del ataque. También explorarán las técnicas para erradicar completamente las amenazas de los sistemas afectados y recuperar operaciones normales, discutiendo estrategias para limpiar sistemas infectados, aplicar parches de seguridad y restaurar datos y servicios desde copias de seguridad seguras. Durante toda la ejecución de la respuesta, se enfatizará la importancia de documentar cada paso del proceso y mantener una comunicación clara y constante con todas las partes interesadas, aprendiendo a redactar informes de incidentes detallados y comunicar actualizaciones clave a la administración y otros equipos de la organización.

Mejora

Finalmente, en la fase de mejora continua, los estudiantes aprenderán a evaluar y mejorar continuamente sus capacidades de respuesta a incidentes. Discutirán la fase de lecciones aprendidas, en la cual se revisan y analizan los incidentes después de que se hayan resuelto, identificando áreas de mejora, documentando lo que funcionó bien y lo que no, y ajustando sus planes y procedimientos en consecuencia. Explorarán las metodologías para evaluar y auditar regularmente sus capacidades de respuesta a incidentes, cubriendo aspectos como la **realización de auditorías internas y externas, la revisión de políticas y procedimientos y la implementación de recomendaciones de mejora**. Además, se destacará la importancia de la capacitación continua y el desarrollo profesional para los equipos de respuesta a incidentes, aprendiendo a **planificar y ejecutar programas de capacitación, mantenerse actualizados con las últimas tendencias y tecnologías, y fomentar una cultura de seguridad dentro de la organización**.

Este módulo de DFIR (Respuesta) proporciona a los estudiantes una formación exhaustiva en las metodologías, técnicas y herramientas necesarias para gestionar eficazmente los incidentes de seguridad informática, equipándolos con las habilidades prácticas y el conocimiento teórico para responder a incidentes de seguridad de manera efectiva y desempeñar roles cruciales en la respuesta a incidentes, ayudando a proteger a sus organizaciones contra amenazas cibernéticas y minimizando el impacto de los incidentes de seguridad.

MÓDULO

DFIR – Forense

El módulo de DFIR (Digital Forensics and Incident Response) con enfoque en Forense del Máster en Ciberseguridad está diseñado para proporcionar a los estudiantes una comprensión profunda y práctica de las metodologías, técnicas y herramientas utilizadas en la investigación forense digital. Este módulo se estructura en tres secciones clave: Introducción a la Práctica Forense, Intelligence (Introducción) e Introducción a las Técnicas de Inteligencia y OSINT. Cada sección está diseñada para **equipar a los estudiantes con el conocimiento y las habilidades necesarias para realizar investigaciones forenses digitales** de manera efectiva y apoyar las actividades de respuesta a incidentes.

Introducción a la Práctica Forense

Esta sección proporciona una visión general de la investigación forense digital, destacando su importancia en la ciberseguridad y el ámbito legal. Los estudiantes comenzarán con una introducción a **los conceptos básicos y la terminología utilizada en forense digital, incluyendo la definición de evidencia digital, los principios de la cadena de custodia y las etapas del proceso forense. Se discutirá la relevancia de la forense digital en la resolución de incidentes de seguridad, el apoyo a investigaciones criminales y la defensa en litigios legales**. Además, se abordarán las normativas y estándares internacionales que rigen la práctica forense digital, como el ISO/IEC 27037, que proporciona directrices para la identificación, recolección y preservación de evidencia digital.

Los estudiantes aprenderán a **identificar y preservar adecuadamente la evidencia digital para garantizar su integridad y admisibilidad en procedimientos legales**. Se cubrirán las mejores prácticas para la recolección de evidencia en diferentes escenarios, incluyendo sistemas en vivo, dispositivos móviles, redes y entornos en la nube. Los estudiantes explorarán herramientas y técnicas para realizar copias forenses de discos duros, capturar imágenes de memoria y recolectar logs y datos de red. También se discutirá la importancia de documentar detalladamente cada paso del proceso de adquisición para mantener una cadena de custodia robusta y garantizar que la evidencia no sea contaminada o alterada.

Intelligence (Introducción)

Esta sección introduce a los estudiantes en el uso de la inteligencia en el contexto de la ciberseguridad y la forense digital. Se discutirá la importancia de la inteligencia de amenazas en la identificación y mitigación de riesgos cibernéticos, así como en la mejora de las capacidades de respuesta a incidentes. Los estudiantes aprenderán sobre **las diferentes fuentes de inteligencia de amenazas, incluyendo fuentes humanas (HUMINT), técnicas (TECHINT) y de fuentes abiertas (OSINT), y cómo integrar esta información en el proceso forense**.

Los estudiantes explorarán las metodologías para recolectar, analizar y utilizar inteligencia de amenazas en la práctica forense. Se cubrirán **técnicas para identificar patrones de comportamiento malicioso, correlacionar eventos de seguridad y desarrollar perfiles de adversarios**. También se discutirá cómo la inteligencia de amenazas puede mejorar la detección de incidentes, la respuesta y la recuperación, proporcionando una visión más completa y proactiva de la seguridad cibernética.

Introducción a las Técnicas de Inteligencia y OSINT

En esta última sección, los estudiantes se enfocarán en las técnicas de inteligencia de **fuentes abiertas (OSINT) y cómo utilizarlas para apoyar las investigaciones forenses**. Se explorarán métodos para recolectar y analizar información de fuentes públicas, como redes sociales, bases de datos públicas y foros en línea, para identificar amenazas, perfilar a los atacantes y descubrir información relevante para la investigación. Los estudiantes aprenderán a utilizar herramientas de OSINT, como Maltego, Recon-ng y SpiderFoot, para automatizar la recolección y análisis de datos.

Se discutirán las mejores prácticas para realizar **investigaciones OSINT de manera ética y legal, garantizando el respeto a la privacidad y la conformidad con las normativas de protección de datos**. Además, se cubrirá la integración de la inteligencia de OSINT con otras fuentes de inteligencia y datos forenses para proporcionar una visión más completa y detallada de los incidentes de seguridad. Los estudiantes practicarán la aplicación de técnicas de OSINT en estudios de caso y ejercicios prácticos, desarrollando sus habilidades para recolectar y analizar información de manera efectiva en situaciones reales.

UNIVERSIDAD COMPLUTENSE MADRID

nticmaster

MÓDULO

Intelligence – OSINT

El módulo de Intelligence (OSINT) del Máster en Ciberseguridad está diseñado para proporcionar a los estudiantes una comprensión profunda y práctica de las técnicas y herramientas utilizadas en la inteligencia de fuentes abiertas (OSINT). Este módulo aborda la importancia de OSINT en el ámbito de la ciberseguridad, destacando su papel en la identificación de amenazas, la recopilación de información sobre actores maliciosos y la mejora de la capacidad de respuesta a incidentes. A lo largo de este módulo, los estudiantes aprenderán a recolectar, analizar y utilizar información de fuentes abiertas de manera efectiva y ética.

El módulo comienza con una introducción a los conceptos y fundamentos de OSINT, donde se explica qué es **la inteligencia de fuentes abiertas y cómo se diferencia de otros tipos de inteligencia**. Se discutirán las diversas fuentes de información disponibles públicamente, como redes sociales, foros en línea, blogs, bases de datos públicas y otros recursos accesibles en internet. Los estudiantes explorarán cómo estas fuentes pueden proporcionar información valiosa sobre amenazas cibernéticas, vulnerabilidades y actividades de actores maliciosos. También se cubrirá la importancia de la verificación y validación de la información obtenida para garantizar su precisión y relevancia.

Una parte fundamental del módulo se centra en las herramientas y técnicas de recolección de OSINT. Los estudiantes aprenderán a utilizar herramientas automatizadas y manuales para recolectar datos de diversas fuentes. Entre las herramientas destacadas se encuentran **Maltego, Recon-ng, SpiderFoot, y otras plataformas que facilitan la recolección y análisis de grandes volúmenes de datos**. Se enseñará a configurar y utilizar estas herramientas para realizar búsquedas avanzadas, extraer datos de manera eficiente y organizar la información recolectada para su posterior análisis. Los estudiantes también aprenderán técnicas de scraping web y el uso de APIs para acceder a datos específicos en línea.

El análisis de la información recolectada es otro componente crítico de OSINT. Los estudiantes aprenderán a **interpretar y correlacionar datos de diferentes fuentes para identificar patrones, tendencias y conexiones relevantes**. Se cubrirán técnicas de análisis de redes sociales, donde los estudiantes explorarán cómo analizar la actividad en plataformas como X, Facebook y LinkedIn para identificar **comportamientos sospechosos, conexiones entre actores y campañas de desinformación**. También se abordarán técnicas de análisis geoespacial para identificar ubicaciones y movimientos de actores maliciosos basándose en la información recolectada.

La ética y la legalidad en la práctica de OSINT son aspectos fundamentales que se abordarán a lo largo del módulo. Los estudiantes aprenderán sobre las **normativas y regulaciones que rigen la recolección y uso de información de fuentes abiertas**, asegurando el cumplimiento de las leyes de privacidad y protección de datos. Se discutirán **los límites éticos de la recolección de datos, destacando la importancia de respetar la privacidad y los derechos de las persona**s mientras se lleva a cabo la inteligencia de fuentes abiertas. Los estudiantes explorarán casos de estudio y ejemplos reales que ilustran las implicaciones legales y éticas de la práctica de OSINT.

El módulo también incluye la aplicación práctica de OSINT en el contexto de la ciberseguridad. Los estudiantes participarán en ejercicios y estudios de caso donde aplicarán las técnicas y herramientas aprendidas para resolver problemas específicos. Por ejemplo, podrán **realizar investigaciones sobre posibles amenazas a una organización, identificar a los actores detrás de un ataque cibernético o rastrear la difusión de información falsa en línea**. Estos ejercicios prácticos les permitirán desarrollar sus habilidades y obtener experiencia en la aplicación real de OSINT en situaciones de ciberseguridad.

MÓDULO

Intelligence – HUMINT

El módulo de Intelligence (HUMINT) del Máster en Ciberseguridad está diseñado para proporcionar a los estudiantes una comprensión profunda de la inteligencia humana (HUMINT) y su aplicación en el ámbito de la ciberseguridad. **HUMINT se refiere a la recopilación de información a través de interacciones humanas y se considera una de las formas más tradicionales y valiosas de inteligencia**. En este módulo, los estudiantes aprenderán sobre las técnicas y métodos utilizados para obtener información de fuentes humanas, así como la importancia de HUMINT en la identificación y mitigación de amenazas cibernéticas.

Los estudiantes comenzarán con una introducción a los conceptos fundamentales de HUMINT, **explorando su historia, evolución y relevancia en el contexto moderno de la ciberseguridad. Se discutirán los diferentes tipos de fuentes humanas, como empleados internos, informantes y contactos externos, y cómo establecer y mantener relaciones con estas fuentes**. Los estudiantes aprenderán técnicas de entrevista y comunicación, incluyendo cómo formular preguntas efectivas, establecer confianza y obtener información precisa y útil.

Un aspecto crucial del módulo es la ética y la legalidad en la práctica de HUMINT. Los estudiantes aprenderán sobre las **regulaciones y normativas que rigen la recopilación de información a través de fuentes humanas**, asegurando el cumplimiento de las leyes y la protección de los derechos de las personas involucradas. Se discutirán los dilemas éticos que pueden surgir en la práctica de HUMINT y cómo abordarlos de manera responsable y profesional.

Además, el módulo cubrirá la **integración de HUMINT con otras formas de inteligencia, como OSINT y SIGINT (inteligencia de señales), para proporcionar una visión más completa y detallada de las amenazas**. Los estudiantes explorarán cómo correlacionar y validar la información obtenida de fuentes humanas con datos de otras fuentes para mejorar la precisión y relevancia de la inteligencia recopilada.

MÓDULO

Intelligence – CORPINT

El módulo de Intelligence (CORPINT) se centra en la aplicación de la **inteligencia en entornos corporativos para proteger a las organizaciones de amenazas internas y externas**. La inteligencia corporativa (CORPINT) implica la recopilación, análisis y uso de información relevante para tomar decisiones informadas y estratégicas que fortalezcan la seguridad y competitividad de la empresa.

Los estudiantes comenzarán con una introducción a los conceptos básicos de la inteligencia corporativa, incluyendo la **identificación de fuentes de información internas y externas**. Se discutirá cómo recolectar información de fuentes internas, como **datos financieros, informes de seguridad y comunicaciones internas, así como de fuentes externas, como competidores, proveedores y el mercado en general**.

El módulo también abordará el análisis de la inteligencia corporativa, enseñando a los estudiantes t**écnicas para interpretar y correlacionar datos para identificar amenazas y oportunidades**. Los estudiantes aprenderán a utilizar herramientas y tecnologías avanzadas para el análisis de inteligencia, como software de análisis de datos y plataformas de inteligencia empresarial.

La integración de la inteligencia corporativa en la estrategia y la toma de decisiones empresariales es otro aspecto clave del módulo. Los estudiantes explorarán **cómo utilizar la inteligencia recopilada para informar y apoyar las decisiones estratégicas, mejorar la seguridad de la información y fortalecer la resiliencia de la organización ante amenazas cibernéticas y de otro tipo**. Se discutirá la importancia de la comunicación y colaboración entre los equipos de inteligencia y otros departamentos de la empresa para maximizar el impacto de la inteligencia corporativa.

MÓDULO

Intelligence – PSYOPS

El módulo de Intelligence (PSYOPS) se enfoca en la **ingeniería social y las operaciones psicológicas, dos áreas críticas en la ciberseguridad y la inteligencia**. La ingeniería social se refiere a la manipulación de personas para obtener información confidencial o acceso a sistemas, mientras que las Psyops se centran en influir en las percepciones y comportamientos de los individuos o grupos.

En la sección de ingeniería social, los estudiantes aprenderán sobre las tácticas y técnicas utilizadas por los atacantes para **explotar las vulnerabilidades humanas**. Se discutirán técnicas comunes de **ingeniería social, como phishing, pretexting, baiting y tailgating**. Los estudiantes aprenderán a identificar y mitigar estas tácticas a través de la concienciación y la capacitación de los empleados, así como mediante la **implementación de políticas y procedimientos de seguridad robustos**.

La sección de Psyops abordará cómo las operaciones psicológicas se utilizan para influir en las percepciones y comportamientos de los individuos o grupos. Los estudiantes explorarán las **técnicas de persuasión y manipulación utilizadas en las Psyops, como la desinformación, la propaganda y la guerra psicológica**. Se discutirán casos de estudio de operaciones psicológicas exitosas y fallidas, proporcionando a los estudiantes una comprensión de cómo estas técnicas se pueden aplicar en el contexto de la ciberseguridad.

Además, el módulo cubrirá la defensa contra las operaciones psicológicas y la ingeniería social. Los estudiantes aprenderán a desarrollar **estrategias y tácticas para proteger a sus organizaciones contra estos tipos de ataques**, incluyendo la educación y concienciación de los empleados, la implementación de controles técnicos y la colaboración con otras organizaciones y entidades gubernamentales para compartir información y mejores prácticas.

MÓDULO

Inteligencia – Propaganda

Propaganda y guerra híbrida

El módulo de Intelligence (Propaganda) del Máster en Ciberseguridad está diseñado para proporcionar a los estudiantes una comprensión profunda de la propaganda y su papel en la guerra híbrida. La propaganda, en el contexto de la ciberseguridad, se refiere a la **difusión de información, a menudo engañosa o sesgada, para influir en las percepciones y comportamientos de individuos y grupo**s. La guerra híbrida combina tácticas convencionales y no convencionales, incluyendo ciberataques, desinformación y operaciones psicológicas, para lograr objetivos estratégicos.

En la primera parte del módulo, se introduce a los estudiantes a los conceptos fundamentales de la propaganda y la guerra híbrida. Se explorará la historia y evolución de la propaganda, destacando **ejemplos significativos y su impacto en conflictos pasados y presentes**. Los estudiantes aprenderán sobre las técnicas y tácticas utilizadas en la propaganda, como la **manipulación de medios, la creación de narrativas falsas y la amplificación de divisiones sociales**.

Se abordará cómo los actores estatales y no estatales utilizan la propaganda en la guerra híbrida para **desestabilizar sociedades, influir en procesos políticos y erosionar la confianza en las instituciones.** Los estudiantes analizarán casos de estudio de campañas de propaganda y guerra híbrida, evaluando las estrategias empleadas y su efectividad. También se discutirá el papel de las redes sociales y otras plataformas digitales en la difusión de propaganda y cómo estas herramientas amplifican el alcance y el impacto de las campañas de desinformación.

Propaganda y guerra híbrida (II)

La segunda parte del módulo se enfoca en las estrategias y tácticas de **defensa contra la propaganda y la guerra híbrida**. Los estudiantes aprenderán a identificar y contrarrestar las campañas de desinformación y las operaciones psicológicas dirigidas a manipular la opinión pública y socavar la estabilidad de las sociedades.

Se discutirán técnicas de **análisis de contenido para detectar y desmantelar narrativas de propaganda, incluyendo el uso de herramientas de inteligencia artificial y análisis de datos**. Los estudiantes explorarán métodos para monitorear y analizar el flujo de información en las redes sociales y otras plataformas digitales, identificando patrones y señales de campañas de desinformación coordinadas.

Además, se cubrirá la importancia de la colaboración y la cooperación internacional en la lucha contra la propaganda y la guerra híbrida. Los estudiantes aprenderán sobre las **iniciativas y marcos legales a nivel nacional e internacional diseñados para combatir la desinformación y proteger la integridad de la información**. Se discutirá el papel de las organizaciones gubernamentales, las empresas privadas y la sociedad civil en la respuesta a las amenazas de propaganda y guerra híbrida.

UNIVERSIDAD COMPLUTENSE MADRID

nticmaster

MÓDULO

GRC – Introducción

El módulo de GRC (**Gobierno, Riesgo y Cumplimiento**) proporciona a los estudiantes una visión integral de las prácticas y estrategias para gestionar el gobierno corporativo, los riesgos y el cumplimiento normativo en el ámbito de la ciberseguridad. GRC es un enfoque unificado que ayuda a las organizaciones a alcanzar sus objetivos empresariales mientras gestionan los riesgos y aseguran el cumplimiento de las regulaciones.

En este módulo introductorio, los estudiantes aprenderán sobre los conceptos fundamentales de GRC y su importancia en la gestión de la ciberseguridad. Se discutirá cómo establecer un marco de gobierno efectivo que incluya **políticas, procedimientos y controles para asegurar la integridad y la seguridad de los datos y sistemas**. Los estudiantes explorarán las metodologías de evaluación y gestión de riesgos, identificando y mitigando los riesgos potenciales que podrían afectar a la organización.

Además, se cubrirá el cumplimiento normativo, destacando las principales leyes y regulaciones que impactan la ciberseguridad, como el **GDPR, HIPAA, y otras normativas específicas de la industria**. Los estudiantes aprenderán a desarrollar y mantener programas de cumplimiento efectivos que aseguren la conformidad con las regulaciones y estándares aplicables.

MÓDULO

GRC – Gobierno

Modelos de gobierno y roles: líneas de defensa

En esta sección del módulo de GRC, los estudiantes se enfocarán en los **modelos de gobierno y los roles dentro de una organización, particularmente las líneas de defensa**. Se discutirán diferentes modelos de gobierno corporativo, incluyendo el modelo de las tres líneas de defensa, que es ampliamente utilizado para gestionar los riesgos y asegurar la efectividad de los controles internos.

Los estudiantes aprenderán sobre las responsabilidades y funciones de cada línea de defensa. La **primera línea de defensa incluye las funciones operativas que gestionan directamente los riesgos**, la segunda línea proporciona supervisión y establece políticas y procedimientos, y la tercera línea consiste en la auditoría interna que evalúa la efectividad de los controles y el cumplimiento de las políticas.

Esquema nacional de seguridad (ENS) y otros marcos específicos

En esta sección, los estudiantes se familiarizarán con el Esquema Nacional de Seguridad (ENS) y otros marcos específicos que regulan la ciberseguridad a nivel nacional e internacional. El ENS es un **conjunto de principios y requisitos que aseguran la protección adecuada de la información en el sector público y otros sectores críticos**.

Se discutirá la estructura y los componentes del ENS, incluyendo los niveles de seguridad y las medidas de protección que deben implementarse. Los estudiantes aprenderán a **aplicar estos principios y requisitos en sus organizaciones** para cumplir con las normativas y mejorar su postura de seguridad.

Además del ENS, se cubrirán **otros marcos y estándares de ciberseguridad relevantes, como ISO/IEC 27001, NIST Cybersecurity Framework y COBIT**. Los estudiantes aprenderán a comparar y contrastar estos marcos, y a seleccionar e implementar el más adecuado para sus necesidades organizacionales.

MÓDULO

GRC – Cumplimiento

Normativa NIS2, DSA/DMA, CSAM, Cibersolidaridad y otros marcos europeos

El módulo de GRC (Cumplimiento) del Máster en Ciberseguridad está diseñado para proporcionar a los estudiantes una comprensión exhaustiva de **las normativas y marcos europeos que regulan la ciberseguridad y la protección de datos**. Comenzando con la normativa NIS2 (Directiva de Seguridad de Redes y Sistemas de Información), se explorarán las obligaciones y requisitos para los operadores de servicios esenciales y los proveedores de servicios digitales. Los estudiantes aprenderán cómo implementar medidas de seguridad **adecuadas y gestionar incidentes de seguridad conforme a las directrices de NIS2**.

Se abordarán también el **DSA (Digital Services Act) y el DMA (Digital Markets Act), dos marcos legislativos que buscan regular los servicios digitales y los mercados en línea en la Unión Europea**. Los estudiantes explorarán cómo estas regulaciones impactan la ciberseguridad y la protección de datos en plataformas digitales y servicios en línea, y cómo las organizaciones pueden cumplir con estos requisitos.

El módulo también cubre la normativa **CSAM (Child Sexual Abuse Material), enfocándose en las obligaciones legales y las mejores prácticas para prevenir y combatir el abuso sexual infantil en línea**. Los estudiantes aprenderán sobre las tecnologías y estrategias para detectar y eliminar contenido ilegal, así como para cooperar con las autoridades competentes en la lucha contra este tipo de delitos.

Finalmente, se explorará el concepto de **Cibersolidaridad y otros marcos europeos que promueven la cooperación y el apoyo mutuo entre los estados miembros en materia de ciberseguridad**. Los estudiantes analizarán iniciativas y programas que fomentan la resiliencia cibernética a nivel europeo, incluyendo la compartición de información, la asistencia técnica y el desarrollo de capacidades conjuntas.

Privacidad, legislación, protección de datos y RGPD

En esta sección, los estudiantes profundizarán en la privacidad y la protección de datos, centrándose en la legislación y las normativas clave que rigen estos aspectos en Europa, particularmente el Reglamento General de Protección de Datos (RGPD). Se discutirá la importancia de **la privacidad en el contexto de la ciberseguridad y cómo las organizaciones deben manejar y proteger los datos personales** para cumplir con las leyes de privacidad.

Los estudiantes aprenderán sobre los principios fundamentales del RGPD, incluyendo **la transparencia, la limitación de la finalidad, la minimización de datos, la exactitud, la limitación del almacenamiento, la integridad y la confidencialidad**. Se abordarán las obligaciones de los responsables y encargados del tratamiento de datos, así como los derechos de los interesados, como el derecho de acceso, rectificación, supresión y portabilidad de los datos.

También se explorarán los procedimientos para **gestionar brechas de datos personales**, incluyendo la notificación a las autoridades de protección de datos y la comunicación a los afectados. Los estudiantes analizarán casos de estudio de violaciones de datos y las respuestas regulatorias, proporcionando una visión práctica de cómo manejar incidentes de privacidad en el entorno real.

También se enfocará en la implementación práctica de los requisitos de privacidad y protección de datos. Los estudiantes aprenderán a realizar **evaluaciones de impacto de protección de datos (DPIA) para identificar y mitigar riesgos de privacidad en nuevos proyectos y tecnologías**. Se discutirán las mejores prácticas para integrar la privacidad por diseño y por defecto en el desarrollo de productos y servicios.

Además, se cubrirá **la gestión de consentimientos y las políticas de privacidad, asegurando que las organizaciones recojan, procesen y almacenen datos personales de manera transparente y conforme a las regulaciones**. Los estudiantes explorarán herramientas y tecnologías para la protección de datos, incluyendo el cifrado, la anonimización y la seudonimización.

El módulo también abordará **las auditorías y la gobernanza de datos**, enseñando a los estudiantes a establecer programas de cumplimiento continuo y a realizar auditorías internas para verificar la conformidad con las leyes de privacidad. Se discutirán los roles y responsabilidades del delegado de protección de datos (DPO) y la importancia de una cultura de privacidad en toda la organización.

MÓDULO

GRC – Identidad

eIDAS2: obligaciones y oportunidades

El módulo de GRC (Identidad) se enfoca en la **identidad digital y las oportunidades y obligaciones que presenta el reglamento eIDAS2** (electronic IDentification, Authentication and trust Services). Los estudiantes aprenderán sobre los objetivos y el alcance de eIDAS2, que busca facilitar las transacciones electrónicas seguras y confiables dentro del mercado único digital europeo.

Se explorarán los diferentes **niveles de seguridad de las identidades electrónicas (bajo, sustancial y alto) y los requisitos para los prestadores de servicios de confianza**, como las firmas electrónicas, los sellos electrónicos y los servicios de autenticación. Los estudiantes analizarán cómo las organizaciones pueden implementar y gestionar estos servicios para cumplir con eIDAS2 y aprovechar sus beneficios para la transformación digital.

Identidades modernas, federación y autosoberanía

Esta sección aborda las **identidades digitales modernas, la federación de identidades y el concepto emergente de autosoberanía**. Los estudiantes aprenderán sobre las tecnologías y estándares utilizados para la gestión de identidades, como **OAuth, OpenID Connect y SAML**, y cómo implementarlos para asegurar el acceso a los sistemas y datos.

Se discutirá la federación de identidades, que permite a las organizaciones y usuarios **gestionar múltiples identidades de manera segura y eficiente a través de diferentes dominios y plataformas**. Los estudiantes explorarán casos de uso y beneficios de la federación, así como los desafíos y soluciones para asegurar la interoperabilidad y la protección de datos.

El concepto de **identidades autosoberanas, donde los individuos tienen control total sobre sus identidades digitales** sin intermediarios centralizados, también se cubrirá en esta sección. Se analizarán las tecnologías subyacentes, como blockchain, y los casos de uso potenciales para la autosoberanía de identidades en el futuro de la ciberseguridad.

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

MÓDULO

RPA/IA – Programación

El módulo de RPA/IA (Programación) introduce a los estudiantes en el **uso de Python para la automatización y la inteligencia artificial. Python es un lenguaje de programación ampliamente utilizado en ciberseguridad por su simplicidad y versatilidad**. Los estudiantes aprenderán los conceptos básicos de Python, incluyendo sintaxis, estructuras de datos, funciones y módulos.

Se cubrirán las **bibliotecas y frameworks más utilizados en la automatización y la IA, como Pandas para la manipulación de datos, NumPy para el cálculo numérico y scikit-learn para el aprendizaje automático**. Los estudiantes desarrollarán scripts para automatizar tareas comunes en ciberseguridad, como el análisis de logs, la recolección de datos y la generación de informes.

Además, se introducirán conceptos básicos de inteligencia artificial y aprendizaje automático, enseñando a los estudiantes a crear modelos predictivos y a utilizar **técnicas de machine learning para detectar y responder a amenazas cibernéticas.**

UNIVERSIDAD COMPLUTENSE MADRID

nticmaster

MÓDULO

RPA/IA – Automatización

En esta sección, los estudiantes aprenderán a utilizar **herramientas y frameworks avanzados para la automatización de procesos repetitivos y la orquestación de tareas complejas**.

Selenium se utilizará para la automatización de navegadores web, permitiendo a los estudiantes automatizar pruebas y recopilar datos de sitios web de manera eficiente.

Airflow será explorado para la orquestación y gestión de flujos de trabajo de datos, enseñando a los estudiantes a crear, programar y monitorear pipelines de datos.

Pyppeteer, una biblioteca para la automatización de navegadores basada en Puppeteer, también será cubierta, proporcionando a los estudiantes capacidades avanzadas para interactuar con **aplicaciones web**.

PyAutoGui se utilizará para la automatización de interfaces gráficas de usuario (GUI), permitiendo a los estudiantes controlar el **mouse y el teclado** para automatizar tareas en aplicaciones de escritorio.

MÓDULO

RPA/IA – Inteligencia Artificial

Inteligencia Artificial: usos (I)

El módulo de RPA/IA (Inteligencia Artificial) proporciona a los estudiantes una visión integral de las aplicaciones de la inteligencia artificial en la ciberseguridad. En esta primera parte, los estudiantes explorarán los **usos de la IA en la detección de amenazas, la respuesta a incidentes y la mejora de la seguridad de la información**.

Se discutirán los **algoritmos y técnicas de aprendizaje automático más utilizados, como la clasificación, la regresión y el clusterin**g. Los estudiantes aprenderán a aplicar estos algoritmos para crear modelos que puedan identificar patrones sospechosos y predecir comportamientos maliciosos.

Inteligencia Artificial: usos (II)

La segunda parte se enfocará en el uso de la IA para la automatización de tareas de ciberseguridad. Los estudiantes explorarán cómo implementar **sistemas de detección de intrusiones basados en IA**, soluciones de respuesta automática a incidentes y **herramientas de análisis forense potenciadas por la inteligencia artificial**.

Se cubrirán también técnicas avanzadas, como el **procesamiento de lenguaje natural (NLP) para el análisis de textos y la detección de phishing, y el uso de redes neuronales profundas** para la clasificación de malware y la identificación de amenazas en tiempo real.

Inteligencia Artificial: usos (III)

La última parte del módulo se centrará en la **investigación y desarrollo de nuevas aplicaciones de la IA en la ciberseguridad**. Los estudiantes trabajarán en proyectos innovadores, aplicando técnicas de IA para resolver problemas complejos y explorar nuevas fronteras en la protección de la información.

UNIVERSIDAD COMPLUTENSE MADRID

nticmaster

TFM

Trabajo Fin de Máster

Asimilados todos los conceptos previos, llega el momento de poner a prueba todos los conocimientos adquiridos en el Máster.

El alumno planteará un Plan de Ciberseguridad para una empresa u organización, para ello utilizará todas las técnicas estudiadas y las herramientas aprendidas en los distintos módulos del Máster.

EQUIPO DOCENTE

Clases y tutorías con grandes profesionales del sector de la Ciberseguridad.

UNIVERSIDAD COMPLUTENSE MADRID

nticmaster

EQUIPO DOCENTE

Directivos

Cristóbal Pareja Flores

Director. Catedrático EU en la UCM. Con más de 30 años como docente, Cristóbal es matemático especializado en Ciencias de la Computación, Doctor en Informática. Además, es Decano de la Facultad de Estudios Estadísticos y Vicedecano de Postgrado e Investigación.

Jose Carlos Soto Gómez

Co-Director del Máster. Socio Fundador de NTIC Master y Aplimovil. Amplia experiencia en proyectos nacionales e internacionales en IT y analítica en empresas como Banco de España, NEC, Telefónica, Vodafone, Orange, medios de comunicación...

Coordinadores

David del Ser

Coordinador Máster

David es Lic. en Marketing por ESIC, Honours Degree in Business Administration por Humberside University, MBA por UNED, Máster Dirección Financiera, Máster Marketing Digital, Máster en Big Data. Especializado en el desarrollo de negocio y transformación digital en Ntic Master. Gran experiencia profesional trabajando en Grupo Iberostar, Grupo Avintia, entre otras.

Cristóbal Martínez Martínez

Coordinador Máster

Cristóbal es Ingeniero informático. Director de IT en Aplimovil y Ntic Master. Profesor máster marketing digital de la UCM, UNED, Cámara de Comercio y CEEIC. Experto en sistemas y procesos informáticos. Gran experiencia profesional trabajando en empresas referentes como NEC, BNP Paribas, Banco de España, Vodafone.

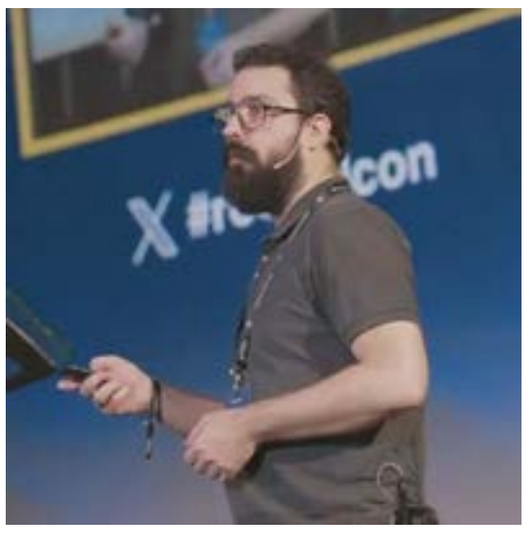
Javier Domínguez Gómez

Coordinador académico y Security Engineer en BBVA

Security Engineer en BBVA. Especialista en Ciberseguridad, modelado de amenazas, inteligencia y seguridad en comunicaciones. Profesor de Big Data, Data Science e Inteligencia Artificial en la UCM. Miembro y divulgador de la Free Software Foundation (FSF) y la Electronic Frontier Foundation (EFF).

EQUIPO DOCENTE

Docentes



Javier Domínguez Gómez

Coordinador académico y Security Engineer en BBVA

Security Engineer en BBVA. Especialista en Ciberseguridad, modelado de amenazas, inteligencia y seguridad en comunicaciones. Profesor de Big Data, Data Science e Inteligencia Artificial en la UCM. Miembro y divulgador de la Free Software Foundation (FSF) y la Electronic Frontier Foundation (EFF).

Román Ramírez Giménez

Director general y fundador de RootedCON

Román es ingeniero informático. Su dilatada experiencia laboral le ha llevado ha recibir numerosas conmemoraciones como el premio ISACA de Madrid al mejor comunicador en 2024. Medalla al mérito de la Guardia Civil. Mejor trayectoria profesional por el ministerio de defensa y ha estado en el TOP 25 empresas de mejor ciberseguridad de España.

Alfonso Muñoz Muñoz

Fundador y director de Criptored

Alfonso es Doctor en Ingeniería de Telecomunicaciones, experto en Ciberseguridad y criptografía. Cuenta con 60 artículos académicos, 2 patentes y 6 libros. Ha recibido premios como el Hall of Fame Google y TOP 50 Cybersecurity Blue Team.

Ricard Martínez Martínez

Miembro del Heatlhcare Data Innovation Council

Ricard es Doctor en el Departamento de Derecho Constitucional, Ciencia Política y Administración. Ha formado parte del Grupo de Trabajo sobre Derechos Digitales de los Ciudadanos del Ministerio de Energía, Turismo y Agenda Digital. Actualmente realiza una investigación sobre las condiciones para la generación de repositorios masivos de datos, concretamente en el ámbito de la salud y al cumplimiento normativo en el ámbito de la Inteligencia Artificial.

Jezer Ferreira Da Silva

Instructor experto en Fuentes Abierta en la INTERPOL

Jezer cuenta con más de 15 años de experiencia en el campo de la ciberseguridad. Ha escrito el libro OSINT aplicado a redes sociales. También ha recibido numerosas conmemoraciones por parte de la policía.

Pablo San Emeterio

Fundador y Director de Vapasec Technology Consulting

Pablo es ingeniero informático. Ha trabajado durante más de 20 años en puestos relacionados con el desarrollo web e I+D+I. También ha sido el encargado de la ciberseguridad de empresas como Optenet y Telefónica. Sus investigaciones sobre ciberseguridad le han hecho participar como ponente en congresos de renombre como Rootedcon, Jornadas STIC y NcN.

EQUIPO DOCENTE

Docentes

Antonio Fernándes

Hacker, Advisor y responsable de Ciberseguridad

Pionero en Ciberseguridad en España con más de 20 años de experiencia. Ha descubierto fallos de seguridad en gigantes como NASA, Google, Facebook, Twitter o el Departamento de Defensa de EEUU. Miembro del subgrupo de expertos en Inteligencia Artificial y productos conectados de la Comisión Europea, donde ha evaluado proyectos de innovación y Ciberseguridad.

Igor Lukic

Especialista en ciberseguridad y fundador de HACKRON

Especialista en ciberseguridad con más de 20 años de experiencia participando en proyectos multinacionales y ejercicios PSYOPS. Es fundador del congreso de hacking «HACKRON», Co-autor del libro 0xWord «HACKING EN IOS». Poseé múltiples certificaciones de seguridad informática emitidas por Carnegie Mellon University, EC-COUNCIL y Microsoft, entre otras.

Raúl Riesco Granadino

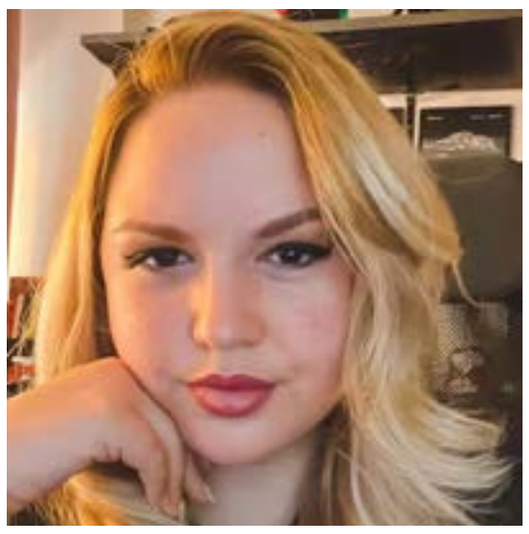
Experto en Seguridad Blockchain y Smart Contracts en Polygon Labs

Doctor en Ingeniería de Telecomunicaciones con más de 25 años de experiencia en Ciberseguridad. White Hacker / Bug Hunter. Líder del equipo español de Hacking, ganador dos veces en el European Cybersecurity Challenge CTF.

Carlos Manchado Martín

Global CISO at Acciona | Corporate Cybersecurity Director

Carlos es Ingeniero Superior en Informática especializado en Ciberseguridad, Seguridad de la Información, Gestión de Riesgos Tecnológicos, Auditoría de Sistemas y Privacidad. Ha sido director de Ciberseguridad para España en Microsoft, así como asesor en estrategia de ciberdefensa, y consultor y asesor estratégico en compañías como E&Y, Accenture o Deloitte.



Gabriela García

Especialista en Ciberseguridad y programación

Desarrolladora de software con enfoque en el desarrollo seguro. Organizadora y ponente en comunidades de hackers tanto en España como a nivel internacional, comprometida siempre con un mundo digital más seguro y accesible.

Iris Martín

Especialista en Ciberseguridad y Ciencia de Datos en Evolutio

Iris trabaja en el departamento de Innovación de Evolutio y en un proyecto de Inteligencia Artificial aplicada a la Ciberseguridad para INCIBE. Ponente, docente y divulgadora en diversas conferencias. Posee una amplia experiencia en integración y automatización.

EQUIPO DOCENTE

Docentes

David
Meléndez

Ingeniero en Informática e investigador en ciberseguridad de infraestructuras críticas

Ponente habitual en los congresos de hacking y ciberseguridad más relevantes nacionales e internacionales como RootedCON o DEFCON USA con investigaciones sobre ataques a infraestructuras críticas, drones, ferrocarriles, etc. Autor del Libro «Hacking con Drones» de 0xWord.

Joseba
García Velasco

Responsable del Arquitectura y Proyectos de Ciberseguridad en Naturgy

Ingeniero en Informática con más de 25 años de experiencia en servicios de Tecnologías de la Información. Responsable de arquitectura y proyectos de Ciberseguridad en Naturgy Energy.

Jesús
Angosto Iglesias

DFIR Technical Lead en Babel

Experto en Ciberseguridad y Análisis Forense, ex Pentester y ponente en conferencias como las jornadas del CCN-Cert.

Tomás
Hidalgo Salvador

Ingeniero informático y auditor interno en SIA

Con más de 20 años de experiencia laboral en entorno bancario en las áreas de TI, Ciberseguridad y Auditoría de riesgos tecnológicos. En la actualidad trabaja como auditor interno en el área de Digital Identity & Signature de SIA.

Fernando
Rubio Román

CTO de Azure en Microsoft España y responsable del equipo de IA y desarrollo de software

Ha tenido múltiples roles en Microsoft, tanto como responsable del equipo de seguridad dentro del área de customer success, como arquitecto de seguridad, así como en respuesta a incidentes. Es parte del grupo de trabajo de Inteligencia Artificial del ISMS así como presentador habitual del sector de la seguridad con múltiples ponencias en eventos como las jornadas del CCN-CERT o RootedCON.

José Ramón
Monleón

Ingeniero superior en Telecomunicaciones.

CISO, CISM, Third Party Risk Management & Awareness en MASORANGE, y miembro de la Junta Directiva de ISMS, organización sin ánimo de lucro para promover la concienciación en Ciberseguridad.

EQUIPO DOCENTE

Docentes

Sofía Sánchez Margolles

Especialista en HUMINT | Analista de Threat Intelligence en Telefónica Tech

Sofía es analista de Threat Intelligence en Telefónica Tech. Psicóloga con un Máster en Inteligencia Económica, co-creadora de UNVEIL framework, además de autora de múltiples publicaciones sobre HUMINT virtual, ingeniería social y persuasión personalizada.

Felix Brezo

Líder de la unidad CTI de Telefónica Tech

Doctor en Telecomunicaciones e Informática y Máster en Análisis de Inteligencia, con más de 10 años en ciberinteligencia. Lidera la unidad CTI en Telefónica Tech, especializado en compartición de inteligencia y modelado de informes. Ha recibido la Cruz al Mérito Policial con Distintivo Blanco y es autor de varias publicaciones en investigación de fuentes abiertas. Ponente en eventos internacionales como BlackHat o Defcon.

Carlos Antonini Cepeda

Global Head of Red Team & Pentesting en Acciona

Carlos cuenta con varios años de experiencia en el sector de la seguridad en múltiples ámbitos (Ethical hacking y Threat Hunting). Seguridad defensiva en IPS/IDS, Siem y EDR. También Seguridad ofensiva con técnicas de hacking en entornos de caja negra y caja blanca.

Sara Concepción Mariscal

Analista Forense y Analista de Inteligencia en Telefónica Tech

Especialista en ciberseguridad con amplia trayectoria en análisis forense, desempeñando roles clave en la respuesta a incidentes como Analista e Incident Handler. Su carrera profesional abarca diversas áreas de la ciberseguridad, incluyendo la coordinación en análisis de vulnerabilidades. Actualmente, ejerce como analista de inteligencia en Telefónica Tech, integrando su experiencia técnica y estratégica para ayudar a los equipos de respuesta con información de modelados.

Alberto Jódar Borrego

Especialista en Ciberseguridad en Evolutio

Ingeniero en Telecomunicaciones. Analista de respuesta ante incidentes de seguridad. Especializado en Detección y Respuesta ante amenazas. Trabaja actualmente como analista de respuesta ante incidentes en el CERT de Evolutio. Cofundador del blog DFIRPills.

Francisco Martín Vázquez

Gerente Auditoría Interna de Ciberseguridad Telefónica S.A.

Gerente en auditoría interna de ciberseguridad en Telefónica, con una sólida trayectoria de más de 20 años de experiencia en el ámbito de la tecnología y la seguridad informática. Apasionado por la tecnología, la programación, los sistemas basados en Unix/Linux (*NIX) y el desafío constante que representa la ciberseguridad, ha dedicado su carrera al análisis, desarrollo e implementación de soluciones avanzadas para proteger infraestructuras críticas y datos sensibles.

EQUIPO DOCENTE

Docentes

Javier Corbalán

Responsable de Detección y Respuesta en Ibercaja

Ingeniero Informático especializado en Ciberseguridad, apasionado por la informática forense y la respuesta a incidentes. Actualmente lidera el área de detección y respuesta a incidentes en Ibercaja Banco, coordinando los servicios de monitorización, inteligencia de amenazas, threat hunting y respuesta a incidentes.

Yolanda García Ruiz

Docente en la UCM. Jurado del Máster

Licenciada en C.C. Matemáticas en la especialidad de C.C. de la Computación por la Universidad Complutense de Madrid desde el año 1995 y doctora en Informática. Hasta su incorporación al mundo académico ha desarrollado su carrera profesional en el área de la informática en diferentes compañías.

Luis Fernando Llana Díaz

Docente en la UCM. Jurado del Máster

Luis F. Llana es licenciado y doctor en Ciencias Matemáticas por la UCM. Docente en la UCM y forma parte de grupos de investigación: Design and Testing of Reliable Systems. Experto en Computer Science.

Gabriel Marín Díaz

PhD, Análisis de Datos. Jurado del Máster

Gabriel es Licenciado en Matemáticas y Doctor en Análisis de Datos, Data Science. Tiene una amplia experiencia en el sector empresarial siendo consultor data Science, actividad que compatibiliza actualmente con la de profesor en la UCM

José Javier Galán Hernández

Responsable de Sistemas. Jurado del Máster

José Javier es Ingeniero Informático y trabaja como Responsable de Sistemas CED. Además es profesor asociado UCM. Ha trabajado en proyectos de sistemas en El Corte Inglés y Comel, entre otros.

Tú

Futuro experto en Ciberseguridad

Porque con nosotros aprenderás seguridad informática. Pero al final el camino tienes que recorrerlo tú y quizás muy pronto estés aquí como nuestro profesor.

SALIDAS PROFESIONALES

El sector de la Ciberseguridad continuará siendo un pilar fundamental del crecimiento laboral, ocupando los primeros lugares en demanda y nivel salarial. La creciente digitalización y la sofisticación de las amenazas han convertido a los expertos en ciberseguridad en perfiles indispensables para las empresas.

UNIVERSIDAD COMPLUTENSE MADRID

nticmaster

Salidas Profesionales

La Ciberseguridad ofrece una gran variedad de salidas profesionales debido a su importancia creciente en la estrategia de protección empresarial. Estas son solo algunas de las muchas oportunidades profesionales que podrás explorar dentro de este ámbito:

Con el avance de la tecnología y la evolución constante del entorno digital, es probable que sigan surgiendo nuevas especialidades y roles.

Analista de Seguridad de la Información

Monitorea y protege los sistemas de la organización, mitigando riesgos de seguridad.

Especialista en Seguridad de Redes

Diseña, implementa y gestiona la seguridad en las redes de datos, protegiendo el tráfico de información contra accesos no autorizados e intrusiones.

Ingeniero en Ciberseguridad

Desarrolla soluciones avanzadas de seguridad y arquitecturas de defensa en profundidad.

Consultor en Ciberseguridad

Proporciona asesoramiento experto en gestión de riesgos y estrategias de seguridad, ayudando a las empresas a fortalecer su protección frente a amenazas.

Especialista en Respuesta a Incidentes

Gestiona incidentes de seguridad y asegura la continuidad operativa tras ataques.

Administrador de Seguridad en la Nube

Gestiona la seguridad de infraestructuras en la nube, protegiendo datos y aplicaciones de accesos no autorizados y amenazas externas.

Auditor de Seguridad de la Información

Realiza evaluaciones para garantizar que los sistemas cumplen con normativas y estándares de seguridad, detectando áreas de mejora.

Hacker Ético

Lleva a cabo pruebas de penetración para identificar vulnerabilidades y reforzar la seguridad de los sistemas, trabajando junto al equipo de ciberseguridad.

Chief Information Security Officer (CISO)

Responsable de definir y dirigir la estrategia de ciberseguridad de la empresa, asegurando que las políticas de seguridad estén alineadas con los objetivos de negocio.

ADMISIONES

Tanto la preinscripción como la pre matrícula quedan abiertas hasta comenzar el curso académico o completar plazas.

UNIVERSIDAD COMPLUTENSE MADRID

nticmaster

Proceso de admisión

Preinscripción

Envío de solicitud para evaluar candidaturas.

Evaluación

Evaluación de candidaturas.

Pre-admisión

Confirmación como alumno del candidato.

Admisión

Confirmación de plaza y formalización de la matrícula.

1. Preinscribirse cumplimentando el formulario ubicado en la pestaña “Preinscripción” de la web **www.masterciberseguridaducm.com**
2. Enviar la documentación requerida a fin de evaluar la candidatura.
3. Entrevista con el solicitante.
4. Confirmación de selección.
5. Realización de un pago inicial.

Tanto la preinscripción como la pre matrícula quedan abiertas hasta comenzar el curso académico o completar plazas, estableciéndose lista de espera si procede. Los alumnos deberán ingresar 600 euros en concepto de pago inicial para el Máster Presencial y 500 euros en concepto de pago inicial para el Máster Semipresencial y el Máster Online, los cuales les serán descontados del importe total de la matrícula. En ningún caso se tendrá derecho a devolución de dicha cantidad, a excepción de que no se llegara a celebrar el curso.

Documentación requerida

Alumnos con titulación de **España**

Los documentos identificativos requeridos para la inscripción en el Máster son:

- Fotocopia del documento de identidad/pasaporte.
- Certificado de notas oficial.
- Título universitario o resguardo de solicitud de título.
- Currículum Vitae.

Alumnos con titulación de **Unión Europea**

- Currículum Vitae.
- Pasaporte/NIE (no válidas las cédulas de identificación de fuera de España).
- Título universitario (no es valido el certificado del título).
- Certificado oficial de notas.

*La documentación debe estar traducida al castellano por un traductor jurado homologado. (Solicitar listado oficial)

Alumnos con titulación de **Fuera de la Unión Europea**

- Currículum Vitae.
- Pasaporte/NIE (no válidas las cédulas de identificación de fuera de España).
- Título universitario legalizado con la Apostilla de la Haya (no es valido el certificado del título).
- Certificado oficial de notas.

*La documentación debe estar traducida al castellano por un traductor jurado homologado. (Solicitar listado oficial)

MODALIDADES

La evaluación de los alumnos se realizará a lo largo de todo el programa a través de ejercicios y casos prácticos.

UNIVERSIDAD COMPLUTENSE MADRID

nticmaster

Máster Presencial

Duración

1 Año / 520 horas

60 ECTS

Inicio: octubre de 2025
Fin: octubre de 2026

Viernes: de 16:00 a 21:00 h
Sábados: de 09:00 a 14:00 h

Lugar

Facultad de Estudios Estadísticos

Ciudad Universitaria Avenida Puerta de Hierro, s/n, 28040 Madrid

Precio

6.850 €

+ 40 € de tasas de secretaría

Pregunta por nuestras becas, facilidades de pago, prácticas en empresas y bolsa de trabajo.

Una vez finalizados y superados estos estudios, la Universidad Complutense de Madrid emitirá el título, conforme a las normas de admisión y matriculación de los títulos de Formación Permanente de la UCM

Metodología Presencial

El curso se impartirá en aulas de la Universidad Complutense de Madrid, en la Facultad de Estudios Estadísticos los viernes y sábados con masterclasses impartidas por diferentes expertos. La formación se realizará de forma tutorizada por los profesores. También se utilizará una plataforma de formación virtual para la comunicación entre los alumnos y profesores, creando una comunidad virtual de trabajo. Los distintos profesores de cada módulo, guiarán a los alumnos proponiendo actividades adicionales dependiendo del temario que se esté cubriendo en cada momento.

Características plataforma On-line

La plataforma actuará como vía de comunicación entre el alumno y el entorno global de formación.

El estudiante tendrá información actualizada sobre los conceptos que se estén estudiando en cada momento, como enlaces a contenidos adicionales incluyendo noticias, artículos, etc.

Los alumnos deberán realizar y aprobar todas las prácticas de los distintos módulos, y realizar el trabajo fin de máster para poder aprobar el máster.

La plataforma cuenta con:

- Mensajería individualizada para cada alumno.
- Vídeos de las clases y de casos prácticos.
- Tutorías online con el profesorado.
- Documentación, noticas y contenidos.
- Foro de los módulos del máster.
- Comunicación con los profesores vía mensajería.
- Chat entre alumnos.

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

Máster Online

Duración

1 Año / 520 horas

60 ECTS

Inicio: octubre de 2025
Fin: octubre de 2026

Lugar

Plataforma Online

Precio

4.750€

+ 40€ de tasas de secretaría

Pregunta por nuestras becas, facilidades de pago, prácticas en empresas y bolsa de trabajo.

Una vez finalizados y superados estos estudios, la Universidad Complutense de Madrid emitirá el título, conforme a las normas de admisión y matriculación de los títulos de Formación Permanente de la UCM

Metodología 100% Online

La formación se realizará de forma tutorizada por los profesores. Se utilizará una plataforma de formación virtual para la comunicación entre los alumnos y profesores, creando una comunidad virtual de trabajo. Los distintos profesores de cada módulo, guiarán a los alumnos proponiendo actividades adicionales dependiendo del temario que se esté cubriendo en cada momento.

Características plataforma On-line

La plataforma actuará como vía de comunicación entre el alumno y el entorno global de formación.

El estudiante tendrá información actualizada sobre los conceptos que se estén estudiando en cada momento, como enlaces a contenidos adicionales incluyendo noticias, artículos, etc.

Los alumnos deberán realizar y aprobar todas las prácticas de los distintos módulos, y realizar el trabajo fin de máster para poder aprobar el máster.

La plataforma cuenta con:

- Mensajería individualizada para cada alumno.
- Vídeos de las clases y de casos prácticos.
- Tutorías online con el profesorado.
- Documentación, noticas y contenidos.
- Foro de los módulos del máster.
- Comunicación con los profesores vía mensajería.
- Chat entre alumnos.

Contacto

Teléfono de información

+34 687 30 04 04

Teléfono de admisiones

+34 667 89 05 83

Correo electrónico

info@mastercibersegurida ducm.com

Sitio Web

www.mastercibersegurida ducm.com/

*La dirección del máster se reserva el derecho de modificar, suprimir y actualizar los profesores, la información y el programa del máster.

UNIVERSIDAD COMPLUTENSE MADRID

nticmaster