UNIVERSIDAD COMPLUTENSE MADRID

nticmaster



Máster de Formación Permanente en

CIBERSEGURIDAD DEFENSIVA Y OFENSIVA

2ª EDICIÓN

Facultad de Estudios Estadísticos
Universidad Complutense de Madrid

PROGRAMA

1. Introducción a la ciberseguridad
2. Arquitectura de comunicaciones y seguridad
3. Criptografía aplicada y Esteganografía
4. Ingeniería inversa y exploiting
5. Red Team y Purple Team
6. Hacking hardware
7. Elementos de seguridad en empresa: on premise y cloud
8. Operaciones de seguridad - SecOps
9. Detección, correlación y acción
10. Infraestructuras críticas y ciberseguridad industrial
11. Redes privadas virtuales (VPNs) y comunicaciones Seguras
12. IDentidad: gestión y elementos de autenticación y autorización
13. Respuesta a incidentes de ciberseguridad
14. Práctica forense digital
15. Sistemas de Deception y Honeypots
16. Modelado de amenazas y comprensión de adversarios
17. Diseño y ejecución de operaciones de ciberinteligencia
18. Inteligencia OSINT
19. Inteligencia HUMINT y CORPINT
20. GRC y líneas de defensa
21. ENS, NIS2 y marcos europeos
22. eIDAS2 e identidades modernas
23. Inteligencia artificial aplicada a la ciberseguridad
24. TFM

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 formación práctica 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.

¿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.

El prestigio de la universidad está avalado por:

QS STARS ★★★★★

La universidad hispanohablante con **la máxima calificación en el raking** de la reconocida consultora **QS World University Rankings**.

7 Premios Nobel, 20 Príncipes de Asturias, 7 Premios Cervantes, etc.

Una de las **instituciones educativas más destacadas** de España y Europa.

Más de **500 años de historia** y reconocimiento social.

Más de 90 títulos de grado, 30 dobles grados, 200 programas máster, y **estudios de formación permanente**

Excelencia académica reconocida, una calidad docente de primer nivel.

Estudiantes de **más de 90 países** y convenios con universidades de los 5 continentes.

¿Por qué estudiar un Máster en Formación Permanente?

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.

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



UNIVERSIDAD COMPLUTENSE MADRID | nticmaster

INFORMACIÓN

Duración	**1 año académico**
Creditos ECTS	**60**

Modalidad Presencial

Viernes tarde y sábados mañana en la universidad

Modalidad Online

100% desde nuestra plataforma online

PROGRAMA

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

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

MÓDULO

Introducción a la Ciberseguridad

Descubre qué es realmente la ciberseguridad y por qué se ha convertido en **una de las profesiones más demandadas del mercado digital**. Aprende el idioma del sector (**amenazas, vulnerabilidades, riesgos y vectores de ataque**), cómo se relacionan entre sí y cómo identificarlos en un entorno real, siempre en torno a la triada CIA: **confidencialidad, integridad y disponibilidad**.

Analiza los **ciberataques más habituales**, como el malware, el ransomware, el phishing o el DDoS, desde la mirada del atacante (Red Team), y conoce **las estrategias de defensa** (Blue Team) que se aplican para mitigarlos.

Explora los perfiles profesionales más demandados, del analista de seguridad al especialista en respuesta a incidentes, pasando por el gestor de riesgos o el ingeniero de ciberseguridad. Entiende **cómo se organizan los equipos, qué responsabilidades tiene cada rol** y qué rutas de especialización puedes seguir desde el primer día.

Termina el módulo con una visión global del sector: las organizaciones internacionales que definen sus estándares, el **impacto de tecnologías como la inteligencia artificial, el IoT o la nube en la seguridad digital y las tendencias** que marcarán los próximos años.

Contenidos:

- Conceptos y terminología esencial de la ciberseguridad.
  - Amenazas, vulnerabilidades, riesgos y vectores de ataque.
  - Tipos de ciberataques (Red Team): malware, ransomware, phishing y DDoS.
  - Estrategias básicas de defensa (Blue Team).
  - La triada CIA: Confidencialidad, Integridad y Disponibilidad.
- Roles y perfiles profesionales en ciberseguridad.
  - Perfiles más demandados del mercado.
  - Organización de los equipos y responsabilidades de cada rol.
  - Rutas de especialización.
- El ecosistema global de la ciberseguridad.
  - Organizaciones internacionales y estándares del sector.
  - Impacto de la IA, el IoT y la computación en la nube.
  - Tendencias y visión estratégica.

UNIVERSIDAD COMPLUTENSE MADRID | ntic master

MÓDULO

Arquitectura de comunicaciones y seguridad

Construye infraestructuras de comunicación seguras desde la base. Domina los modelos de referencia OSI y TCP/IP, aprende a **segmentar redes y a aislar los segmentos críticos para limitar el alcance de un ataque**, y configura firewalls y sistemas IDS/IPS con las prácticas de seguridad perimetral que aplican hoy las grandes organizaciones.

Lleva esa **protección a la nube**, que no es segura por defecto. **Compara los modelos** IaaS, PaaS y SaaS y los despliegues públicos, privados e híbridos, y **trabaja la gestión de identidades**, el cifrado de datos y la configuración segura en AWS, Azure y Google Cloud.

Adéntrate después en las **arquitecturas distribuidas**. Entiende qué riesgos introduce el Fog Computing al procesar los datos cerca de donde se generan y cómo proteger los nodos intermedios, y qué vectores de ataque presentan los entornos Edge y P2P, donde no hay un servidor central que controle las comunicaciones.

Cierra el módulo con **el modelo Zero Trust, en el que ningún usuario ni dispositivo es de confianza** por defecto. Aplica la autenticación continua, la microsegmentación, la MFA y las políticas de acceso basadas en riesgo a partir de casos reales de organizaciones que ya lo han adoptado.

Contenidos:

- Arquitecturas de red seguras.
  - Modelos de referencia OSI y TCP/IP.
  - Segmentación de redes y aislamiento de segmentos críticos.
  - Firewalls, IDS/IPS y seguridad perimetral.
- Seguridad en la computación en la nube.
  - Modelos de servicio IaaS, PaaS y SaaS.
  - Modelos de despliegue: pública, privada e híbrida.
  - Identidades, cifrado y configuración segura en AWS, Azure y Google Cloud.
- Fog Computing: seguridad en el procesamiento local.
  - Principios, ventajas operativas y riesgos específicos.
  - Protección de datos en nodos intermedios.
- Edge/P2P: seguridad en entornos descentralizados.
  - Vectores de ataque en arquitecturas sin servidor central.
  - Técnicas para comunicaciones seguras entre pares.
- Modelos Zero Trust: nunca confíes, siempre verifica.
  - Autenticación continua y autorización basada en contexto.
  - Microsegmentación, IAM, MFA y políticas de acceso basadas en riesgo.
  - Casos reales de adopción.

MÓDULO

Criptografía aplicada y esteganografía

Recorre la evolución del cifrado, del César a AES, y entiende la **diferencia entre la criptografía simétrica y la asimétrica**. Analiza algoritmos como DES, 3DES, AES y RC4, cómo se gestionan y distribuyen las claves de forma segura, y cómo RSA, Diffie-Hellman y ECC permiten firmar documentos y abrir canales seguros en internet sin compartir antes un secreto.

Comprende cómo **las funciones hash** como SHA o MD5 garantizan la integridad de los datos y cuáles son sus debilidades, y cómo **protocolos como SSL/TLS e IPsec** protegen las comunicaciones web y de red. Aplícalo en casos reales de blockchain, dispositivos IoT y almacenamiento seguro.

Da un paso más con la **esteganografía, el arte de ocultar que existe un mensaje**. Aprende a esconder información en imágenes, audio o tráfico de red con técnicas como LSB, y a detectarla mediante estegoanálisis, una habilidad clave para **descubrir exfiltraciones de datos y malware camuflado** en archivos aparentemente inocentes.

Termina el módulo mirando al futuro: **cómo la computación cuántica amenaza los algoritmos actuales** y qué soluciones post-cuánticas se están desarrollando para hacerle frente.

Contenidos:

- Fundamentos de criptografía.
  - Historia y evolución: del cifrado César a AES.
  - Criptografía simétrica y asimétrica.
- Criptografía simétrica.
  - Cifrado de bloque y de flujo: DES, 3DES, AES y RC4.
  - Gestión y distribución segura de claves.
- Criptografía asimétrica.
  - RSA, Diffie-Hellman y ECC.
  - Firmas digitales y canales de comunicación seguros.
- Funciones hash e integridad de los datos.
  - SHA y MD5: usos, diferencias y vulnerabilidades.
- Protocolos criptográficos: SSL/TLS e IPsec.
- Criptografía aplicada: blockchain, IoT y almacenamiento seguro.
- Esteganografía.
  - Ocultación de información en imágenes, audio, vídeo y texto.
  - Técnicas LSB y canales encubiertos en el tráfico de red.
  - Estegoanálisis: detección de información oculta.
  - Usos en exfiltración de datos y malware.
- Criptografía cuántica y post-cuántica.

MÓDULO

Ingeniería inversa y exploiting

Desmonta el software para entender cómo funciona por dentro. Domina las técnicas de ingeniería inversa con herramientas como IDA Pro, Ghidra, OllyDbg y x64dbg, combinando el análisis estático y el dinámico para leer código máquina y reconstruir la lógica de cualquier binario aunque no tengas acceso a su código fuente.

Aplica estas técnicas sobre **muestras reales de malware**: entiende su comportamiento, localiza sus mecanismos de persistencia y neutraliza los trucos de ofuscación y evasión que utilizan para pasar desapercibidas ante los sistemas de detección. Documenta lo que encuentras para que el equipo de respuesta pueda actuar.

Identifica y explota vulnerabilidades reales en software y sistemas, como el desbordamiento de búfer, la inyección de código o la escalada de privilegios, siempre en entornos controlados. Practica cómo se construye un exploit, desde el fallo que lo hace posible hasta su ejecución.

Cierra el módulo con la otra cara de la moneda: las **medidas de mitigación que frenan cada técnica de explotación**, como la aleatorización de memoria (ASLR), la prevención de ejecución de datos (DEP) o los stack canaries, para que sepas tanto atacar un sistema como blindarlo.

Contenidos:

- Ingeniería inversa.
  - Análisis estático y dinámico de binarios.
  - Lectura de código máquina y reversing.
  - Herramientas.
- Análisis de malware.
  - Ingeniería inversa sobre muestras reales.
  - Mecanismos de persistencia.
  - Técnicas de ofuscación y evasión.
- Explotación de vulnerabilidades.
  - Desbordamiento de búfer.
  - Inyección de código.
  - Escalada de privilegios.
- Construcción de exploits y mitigaciones.
  - Cómo se desarrolla y se usa un exploit.
  - Medidas de mitigación.

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

MÓDULO

Red Team y Purple Team

Piensa como un atacante: es la mejor forma de construir defensas sólidas. Sigue **paso a paso el ciclo de vida de un ataque real**, desde el reconocimiento y la enumeración hasta la explotación, la escalada de privilegios, el movimiento lateral, la persistencia y la exfiltración de datos, con las herramientas y técnicas propias de cada fase.

Realiza **pruebas de penetración** sobre sistemas y aplicaciones web, y aprende a convertir lo que encuentras en informes profesionales que una organización pueda usar para corregir sus fallos.

Simula **adversarios reales en entornos controlados**, replica las tácticas, técnicas y procedimientos (TTP) de grupos avanzados y automatiza ejercicios de emulación con Caldera y Atomic Red Team para comprobar si las defensas de una organización detectarían a un atacante de verdad.

Termina el módulo con **el enfoque Purple Team, en el que atacantes y defensores trabajan juntos**. Traslada cada hallazgo ofensivo a mejoras concretas de detección y respuesta, y refuerza de forma continua la postura de seguridad de la organización.

Contenidos:

- Metodologías de Red Team.
  - Ciclo de vida de un ataque: reconocimiento, enumeración y explotación.
  - Escalada de privilegios, movimiento lateral, persistencia y exfiltración.
- Pentesting de sistemas y aplicaciones web.
  - Metasploit, Burp Suite y OWASP ZAP.
  - Escaneo, explotación y post-explotación.
  - Informes profesionales de hallazgos.
- Simulación de adversarios.
  - Cobalt Strike y PowerShell Empire.
  - Tácticas, técnicas y procedimientos (TTP) de atacantes avanzados.
  - Emulación automatizada con Caldera y Atomic Red Team.
- Purple Team.
  - Colaboración entre Red Team y Blue Team.
  - De los hallazgos ofensivos a mejoras de detección y respuesta.

MÓDULO

Hacking hardware

Abre un dispositivo y aprende a leerlo como lo haría un atacante. **Identifica sus componentes y su arquitectura, y comprende los protocolos que usan los chips para comunicarse entre sí**, como I2C, SPI y UART, la puerta de entrada a muchos ataques sobre hardware, desde un router doméstico hasta un equipo industrial.

Pasa a la práctica con **ataques reales sobre dispositivos físicos**: extrae y manipula su firmware, analiza su consumo y sus emisiones con ataques de canal lateral (side-channel) e induce errores controlados mediante la inyección de fallos para obtener claves, saltarte protecciones o alterar el comportamiento del dispositivo.

Trabaja en el laboratorio con las **herramientas profesionales del sector**, como programadores de chips, osciloscopios y analizadores lógicos, para capturar señales, leer memorias y entender qué ocurre dentro de cada circuito.

Cierra el módulo con la **seguridad en dispositivos IoT**, uno de los vectores de ataque que más ha crecido en los últimos años. Identifica y explota sus vulnerabilidades y aprende las técnicas para protegerlos frente a ataques físicos y electrónicos.

Contenidos:

- Fundamentos de hacking hardware.
  - Identificación de componentes y arquitecturas de hardware.
  - Protocolos de comunicación: I2C, SPI y UART.
- Ataques físicos y electrónicos.
  - Extracción y manipulación de firmware.
  - Ataques de canal lateral (side-channel).
  - Inyección de fallos.
- Herramientas de laboratorio.
  - Programadores de chips, osciloscopios y analizadores lógicos.
- Seguridad en dispositivos IoT.
  - Vulnerabilidades y vectores de ataque.
  - Protección frente a ataques físicos y electrónicos.

MÓDULO

Elementos de seguridad en empresa: On premise y Cloud

Protege la infraestructura de una empresa allí donde esté. **Configura y gestiona firewalls, gateways de seguridad y sistemas** IDS/IPS como Snort, Suricata o Zeek para blindar el perímetro, segmenta la red corporativa con políticas de acceso granulares y monitoriza el tráfico para detectar actividad sospechosa antes de que escale.

Localiza los puntos débiles antes que el atacante con herramientas de análisis de vulnerabilidades como Nessus, OpenVAS o Qualys, **interpreta sus resultados con criterio profesional y decide qué corregir primero** en función del riesgo real para el negocio, antes de que un fallo conocido se convierta en una brecha.

Automatiza la aplicación de parches y el mantenimiento de configuraciones seguras con SCCM, Ansible y Puppet, para reducir los errores humanos y la superficie de ataque a cualquier escala, desde unos pocos servidores hasta miles de equipos.

Termina el módulo con la **defensa de entornos cloud en AWS, Azure y Google Cloud**: gestión de identidades y accesos, cifrado de datos y configuración segura. Entiende qué controles asume el proveedor y cuáles recaen siempre en el equipo de seguridad de la organización.

Contenidos:

- Seguridad perimetral on-premise.
  - Firewalls, gateways de seguridad e IDS/IPS: Snort, Suricata y Zeek.
  - Segmentación de redes corporativas y control de acceso granular.
  - Monitorización del tráfico y detección de actividad sospechosa.
- Gestión de vulnerabilidades.
  - Análisis con Nessus, OpenVAS y Qualys.
  - Interpretación y priorización de hallazgos.
- Gestión de parches y configuraciones seguras.
  - Automatización con SCCM, Ansible y Puppet.
- Seguridad en la nube.
  - Buenas prácticas en AWS, Azure y Google Cloud.
  - IAM, cifrado en tránsito y en reposo y configuración segura.
  - Modelo de responsabilidad compartida con el proveedor.

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

MÓDULO

Operaciones de seguridad – SecOps

Entra en el corazón de la defensa de cualquier organización: **el Centro de Operaciones de Seguridad (SOC)**. Conoce su función, su estructura y su operación diaria, cómo se reparten los roles entre analistas de distintos niveles y cómo se coordina con el resto de equipos de seguridad.

Gestiona **el flujo de alertas que llega cada día a un SOC**: monitoriza de forma continua, prioriza lo importante, reduce los falsos positivos y escala cada incidente al equipo adecuado en el momento justo. Aprende también qué métricas importan, como los tiempos de detección y respuesta, y cómo mejorarlas de forma sistemática.

Implementa **plataformas SOAR para automatizar las tareas repetitivas** mediante playbooks y orquestar respuestas coordinadas ante incidentes, de modo que el equipo humano se concentre en las decisiones que requieren criterio experto. La velocidad de respuesta marca la diferencia entre un incidente contenido y una brecha grave.

Cierra el módulo con **los límites legales y éticos de la monitorización continua**: cómo diseñar una operación de seguridad eficaz que respete la privacidad de empleados y usuarios y cumpla la normativa de protección de datos.

Contenidos:

- El Centro de Operaciones de Seguridad (SOC).
  - Función, estructura y operación diaria.
  - Roles y niveles de analista.
  - Coordinación con otros equipos de seguridad.
- Gestión de alertas.
  - Monitorización continua y escalado de incidentes.
  - Priorización y reducción de falsos positivos.
- Métricas del SOC.
  - Tiempos de detección y respuesta (MTTD y MTTR).
  - Mejora continua de la operación.
- Automatización y orquestación con SOAR.
  - Playbooks y automatización de tareas repetitivas.
  - Respuestas coordinadas ante incidentes.
- Límites legales y éticos de la monitorización continua.

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

MÓDULO

Detección, correlación y acción

Gana **visibilidad sobre todo lo que ocurre en una organización**, porque sin ella no hay defensa posible. **Trabaja con plataformas SIEM** como Splunk, ELK Stack o IBM QRadar para recolectar y analizar logs, y construye dashboards operativos que conviertan el volumen de eventos en alertas accionables.

Completa esa visión con **soluciones EDR para los equipos y NDR para la red, y analiza el tráfico con técnicas de inspección profunda de paquetes y herramientas** como Wireshark para distinguir la actividad legítima de las señales de compromiso que los sistemas automáticos pueden pasar por alto.

Domina la correlación de eventos procedentes de endpoints, red, cloud y aplicaciones. Un incidente rara vez se manifiesta en una sola señal, y cruzar fuentes es lo que permite **descubrir ataques complejos y amenazas persistentes** que pasan desapercibidas cuando los datos se analizan por separado.

Termina el módulo **pasando de la detección a la acción**: activa planes de contención, erradicación y recuperación con el mínimo impacto operativo y coordina la comunicación interna y externa durante una crisis de seguridad. Cuando el ataque ya está en marcha, cada minuto cuenta.

Contenidos:

- Plataformas SIEM.
  - Splunk, ELK Stack e IBM QRadar.
  - Recolección y análisis de logs.
  - Dashboards operativos y alertas accionables.
- Detección en equipos y en red: EDR y NDR.
  - Análisis de tráfico e inspección profunda de paquetes.
  - Wireshark.
- Correlación de eventos multifuente.
  - Endpoints, red, cloud y aplicaciones.
  - Detección de ataques complejos y amenazas persistentes.
- Acción: de la alerta a la contención.
  - Planes de contención, erradicación y recuperación.
  - Comunicación y coordinación durante una crisis.

MÓDULO

Infraestructuras críticas y ciberseguridad industrial

Identifica qué convierte un **sistema en infraestructura crítica y por qué su caída afecta a toda la sociedad**. Aprende a categorizar los activos de sectores estratégicos como la energía, el transporte, el agua o las telecomunicaciones según su impacto en la seguridad nacional y en la continuidad del negocio.

Conoce los **entornos industriales (OT/ICS) y en qué se diferencian de la informática corporativa**: sistemas SCADA y PLC, protocolos como Modbus o DNP3 y equipos pensados para funcionar durante décadas, a menudo sin parches ni autenticación. Descubre por qué aquí la disponibilidad pesa más que nunca y qué vectores de ataque son propios de estos sistemas.

Analiza ataques reales que demostraron **hasta dónde puede llegar una amenaza en este ámbito, como Stuxnet**, los apagones provocados en la red eléctrica de Ucrania o el ransomware que paralizó Colonial Pipeline, y extrae de ellos lecciones para la defensa.

Cierra el módulo con los **estándares y controles para proteger estos entornos**, como la norma IEC 62443, la gestión de riesgos en sistemas OT y la coordinación con entidades públicas y privadas ante incidentes de alto impacto.

Contenidos:

- Qué es una infraestructura crítica.
  - Sectores estratégicos: energía, transporte, agua y telecomunicaciones.
  - Identificación y categorización de activos críticos.
  - Impacto en la seguridad nacional y la continuidad del negocio.
- Entornos industriales OT/ICS.
  - Diferencias entre IT y OT.
  - Sistemas SCADA y PLC. Protocolos industriales: Modbus y DNP3.
  - Vectores de ataque específicos.
- Ataques reales a infraestructuras críticas.
  - Stuxnet, la red eléctrica de Ucrania y Colonial Pipeline.
- Estándares y controles de protección.
  - Marcos normativos y la norma IEC 62443.
  - Gestión de riesgos en entornos OT.
  - Coordinación con entidades públicas y privadas.

UNIVERSIDAD COMPLUTENSE MADRID | ntic master

MÓDULO

Redes privadas virtuales (VPNs) y comunicaciones seguras

Asegura cualquier comunicación partiendo de la criptografía que la sostiene. Entiende cómo una VPN combina AES para cifrar los datos, RSA o ECC para intercambiar claves y SHA para garantizar la integridad del tráfico, y cómo TLS y SSH protegen las comunicaciones web y la administración remota mediante certificados y autenticación mutua.

Compara los protocolos VPN que encontrarás en la empresa: IPsec, con sus protocolos AH y ESP, como estándar para interconectar sedes, y WireGuard, una alternativa moderna y ligera, con criptografía como Curve25519 y ChaCha20 y un código tan reducido que facilita su auditoría.

Ve más allá de la privacidad que ofrece una VPN con las redes diseñadas para el anonimato y la resistencia a la censura, como TOR, I2P y Freenet. Comprende cómo funcionan el enrutamiento de cebolla y los túneles de estas redes, una pieza clave tanto para la inteligencia como para la defensa.

Termina el módulo con la parte más técnica: configura en Linux entornos reales de IPsec con StrongSwan e intégralos con WireGuard, gestionando claves públicas y privadas y reglas de iptables y nftables, para salir con configuraciones funcionales en mano.

Contenidos:

- Criptografía aplicada a VPN.
  - AES para los datos, RSA/ECC para el intercambio de claves y SHA para la integridad.
- Protocolos TLS y SSH.
  - Certificados digitales, handshake y autenticación mutua.
  - Administración remota segura.
- IPsec.
  - Protocolos AH y ESP.
  - Interconexión de sedes (Site-to-Site).
- WireGuard.
  - Criptografía moderna: Curve25519 y ChaCha20.
  - Rendimiento y facilidad de auditoría.
- Anonimato en red: TOR, I2P y Freenet.
- Implementación práctica en Linux.
  - IPsec con StrongSwan e integración con WireGuard.
  - Gestión de claves y reglas de iptables y nftables.

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

MÓDULO

IDentidad: gestión y elementos de autenticación y autorización

Controla **quién es quién y qué puede hacer cada uno, uno de los pilares de la ciberseguridad moderna.** Domina la gestión de identidades y accesos (IAM): directorios de usuarios como Active Directory o LDAP, el ciclo de vida de cada identidad desde el alta hasta la baja, y el inicio de sesión único (SSO) y la federación entre sistemas.

Evalúa los **métodos de autenticación más robustos**, desde las contraseñas seguras y los tokens de hardware hasta la biometría y la autenticación multifactor (MFA), y conoce **el salto hacia el acceso sin contraseña** con FIDO2 y passkeys. Entiende cómo cada capa añade fricción al atacante sin perjudicar al usuario legítimo.

Diseña **políticas de autorización basadas en roles** (RBAC) y en atributos (ABAC) para controlar con precisión el acceso a los recursos sensibles, aplicando siempre el principio de mínimo privilegio en línea con el modelo Zero Trust. Revisa los permisos de forma periódica para que ningún acceso sobreviva a su necesidad.

Cierra el módulo con la **gestión de cuentas privilegiadas** (PAM), las llaves más valiosas de cualquier organización y el objetivo preferido de los atacantes, y con las prácticas para protegerlas y auditar su uso.

Contenidos:

- Gestión de identidades y accesos (IAM).
  - Directorios de usuarios: Active Directory y LDAP.
  - Ciclo de vida de las identidades: altas, cambios y bajas.
  - Inicio de sesión único (SSO) y federación de identidades.
- Elementos de autenticación.
  - Contraseñas seguras y tokens de hardware.
  - Autenticación multifactor (MFA) y biometría.
  - Autenticación sin contraseña: FIDO2 y passkeys.
- Autorización y control de acceso.
  - Modelos basados en roles (RBAC) y en atributos (ABAC).
  - Principio de mínimo privilegio y Zero Trust.
- Gestión de cuentas privilegiadas (PAM).

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

MÓDULO

Respuesta a incidentes de ciberseguridad

Prepárate para **responder con orden cuando un ataque ya está dentro**. Aprende a identificar qué constituye un incidente y a clasificarlo, desde el malware o el DDoS hasta el robo de datos o el abuso interno, y domina el **ciclo completo de respuesta**: preparación, identificación, contención, erradicación, recuperación y lecciones aprendidas.

Diseña **planes de respuesta operativos** con políticas, procedimientos estándar (SOP) y un equipo de respuesta (IRT) con roles bien definidos, y ponlos a prueba con simulaciones y ejercicios de mesa antes de que llegue un incidente real. Un plan que nunca se ha probado es un plan que falla justo cuando más se necesita.

Gestiona el incidente de principio a fin: **evalúa su alcance, aísla los sistemas afectados, elimina la amenaza y restaura** los servicios desde copias de seguridad fiables. Documenta cada paso con rigor y mantén informados a la dirección y a los equipos implicados.

Termina el módulo con la mejora continua: **analiza cada incidente cerrado para saber qué funcionó y qué no**, y refuerza las capacidades del equipo con auditorías, métricas y formación constante.

Contenidos:

- Tipos de incidentes y ciclo de respuesta.
  - Qué es un incidente y cómo clasificarlo.
  - Malware, DDoS, intrusiones, robo de datos y abuso interno.
  - Fases: preparación, identificación, contención, erradicación, recuperación y lecciones aprendidas.
- Planificación y preparación.
  - Planes de respuesta, políticas y procedimientos (SOP).
  - Equipos de respuesta (IRT): roles y responsabilidades.
  - Simulaciones y ejercicios de mesa (tabletop exercises).
- Gestión del incidente.
  - Contención, erradicación y restauración desde copias seguras.
  - Documentación e informes de incidentes.
  - Comunicación con la dirección y los equipos implicados.
- Mejora continua.
  - Análisis post-incidente y lecciones aprendidas.
  - Auditorías, métricas y capacitación del equipo.

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

MÓDULO

Práctica forense digital

Investiga un ataque a partir de las huellas que deja en el disco, en la memoria, en los logs y en el tráfico de red. Aprende qué es una evidencia digital, cómo se mantiene la cadena de custodia y por qué su integridad decide tanto el éxito técnico como la validez legal de la investigación, conforme a estándares como la ISO/IEC 27037.

Adquiere evidencias sin contaminarlas en todo tipo de escenarios, desde sistemas en vivo y dispositivos móviles hasta redes y entornos cloud. Realiza **copias forenses** de discos, captura la memoria RAM y documenta cada paso para mantener la trazabilidad. El primer error de una investigación suele cometerse aquí.

Analiza lo recogido con **herramientas profesionales** como EnCase, FTK, Autopsy o Volatility y construye líneas de tiempo que te permitan reconstruir cómo ocurrió el ataque, paso a paso, a partir de casos reales. Identifica por dónde entró, qué hizo dentro y qué información se llevó.

Cierra el módulo **correlacionando las evidencias con inteligencia de amenazas** para perfilar al atacante, y aprende a redactar un informe forense claro, riguroso y capaz de sostenerse en un proceso legal.

Contenidos:

- Fundamentos de la investigación forense digital.
  - Evidencia digital y cadena de custodia.
  - Estándares internacionales: ISO/IEC 27037.
- Adquisición y preservación de evidencias.
  - Copias forenses de discos y capturas de memoria RAM.
  - Sistemas en vivo, dispositivos móviles, red y entornos cloud.
  - Trazabilidad y documentación del proceso.
- Análisis forense.
  - Herramientas: EnCase, FTK y Autopsy.
  - Análisis de memoria con Volatility.
  - Líneas de tiempo y reconstrucción del ataque.
- Contexto e informe.
  - Correlación con inteligencia de amenazas y perfilado de atacantes.
  - Informe forense y validez legal.

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

MÓDULO

Sistemas de Deception y Honeypots

Engaña al atacante para **detectarlo antes de que llegue a lo importante**. Descubre cómo la ciberdecepción llena la red de trampas: cualquier interacción con un señuelo es sospechosa por definición, lo que genera alertas casi sin falsos positivos, **ralentiza al adversario y te da tiempo para reaccionar**. Planifica estas operaciones con marcos como MITRE Engage.

Despliega **honeypots de baja y alta interacción**, tanto en producción como con fines de investigación, y combínalos en honeynets con herramientas como Cowrie, Dionaea, Conpot o T-Pot, capaces de simular desde un servidor SSH hasta un sistema industrial.

Siembra honeytokens por toda la organización: **credenciales falsas, documentos trampa o registros que avisan en cuanto alguien los toca**, con soluciones como Canarytokens. Aprende a situarlos e integrarlos con el SIEM, y evita que el atacante los reconozca o use un honeypot como punto de salto.

Termina el módulo **convirtiendo lo capturado en inteligencia**: extrae las TTP, los IOCs y las muestras de malware que deja cada intruso y úsalos para reforzar tus defensas, sin perder de vista los límites legales de estas prácticas.

Contenidos:

- Fundamentos de la ciberdecepción.
  - Qué es deception y qué aporta a la defensa.
  - Detección de alta fidelidad y desgaste del atacante.
  - Marco MITRE Engage.
- Honeypots y honeynets.
  - Honeypots de baja y alta interacción.
  - Honeypots de producción y de investigación.
  - Herramientas: Cowrie, Dionaea, Conpot y T-Pot.
- Honeytokens y señuelos.
  - Credenciales, documentos y registros trampa.
  - Canarytokens.
- Despliegue y explotación de la información.
  - Ubicación en la red e integración con el SIEM.
  - Riesgos, evasión por parte del atacante y aspectos legales.
  - Extracción de TTP e IOCs para inteligencia de amenazas.

MÓDULO

Modelado de amenazas y comprensión de adversarios

Conoce al enemigo con método. **Aprende a identificar, categorizar y priorizar las amenazas** según su impacto y su probabilidad, y aplica metodologías de modelado como STRIDE y DREAD para tomar decisiones de defensa informadas y reproducibles en cualquier organización.

Analiza **cómo opera un atacante en todas las fases** de un ataque, del reconocimiento a la exfiltración, cómo monta su infraestructura de comando y control (C2) y qué técnicas usa para ocultarse. Mapea todo ello con MITRE ATT&CK para detectar brechas de cobertura en tus defensas y priorizar las mitigaciones con criterios objetivos.

Distingue a los **distintos adversarios, de los grupos patrocinados por estados y las APT al crimen organizado y los hacktivistas**: sus objetivos, sus recursos y sus métodos. Estudia campañas reales para entender su impacto y extraer lecciones aplicables a tu organización.

Cierra el módulo con el **intercambio de inteligencia entre organizaciones a través de ISACs**, plataformas como MISP y feeds comerciales, e integra esas fuentes en las operaciones de seguridad del día a día para tomar decisiones más rápidas y mejor fundamentadas.

Contenidos:

- Modelado de amenazas.
  - Identificación, categorización y priorización por impacto y probabilidad.
  - Metodologías: STRIDE y DREAD.
- Tácticas, técnicas y procedimientos (TTP).
  - Fases de un ataque: del reconocimiento a la exfiltración.
  - Infraestructura de comando y control (C2).
  - Técnicas de ocultación y evasión.
- MITRE ATT&CK como framework operativo.
  - Mapeo de TTP y brechas de cobertura.
  - Priorización de mitigaciones.
- Comprensión de adversarios.
  - Actores estatales, grupos APT, crimen organizado y hacktivistas.
  - Campañas de ataque reales y lecciones aprendidas.
  - Intercambio de inteligencia: ISACs, MISP y feeds.

MÓDULO

Diseño y ejecución de operaciones de ciberinteligencia

Transforma la **información en conocimiento accionable**. Distingue entre dato, información e inteligencia, domina las seis fases del ciclo de inteligencia en sus niveles estratégico, operacional y táctico, y traduce una necesidad del negocio en requisitos de inteligencia (RI) y de información (RFI) concretos. Analiza con el Modelo Diamante y con técnicas estructuradas como ACH o el Pre-mortem para que tus sesgos no comprometan las conclusiones.

Prepara **un entorno seguro antes de investigar, con OPSEC del analista, máquinas dedicadas e identidades ficticias creíbles** (sock puppets). Recorre foros underground, marketplaces, leak sites y canales de Telegram, y automatiza la recolección con herramientas como Telethon o Pyrogram.

Procesa y enriquece lo recogido con VirusTotal, Shodan o WHOIS, **pondera la fiabilidad de cada fuente y guárdalo con trazabilidad** en MISP u OpenCTI. Con esa base, construye perfiles de actores, de los IABs a los grupos RaaS y las APT.

Termina el módulo con el reporting: **adapta el mismo informe al C-level, al SOC y al analista técnico**, y tradúcelo a objetos STIX 2.1 para compartir inteligencia de forma estructurada entre organizaciones.

Contenidos:

- Diseño de operaciones de inteligencia.
  - Ciclo de inteligencia y niveles estratégico, operacional y táctico.
  - Requisitos de inteligencia (RI) y de información (RFI).
  - Modelo Diamante y otros modelos de análisis.
  - Roles y organización de una unidad de ciberinteligencia.
  - Técnicas analíticas estructuradas (SATs): ACH, Pre-mortem y Devil's Advocate.
- Ejecución de operaciones de inteligencia.
  - OPSEC del analista y sock puppets.
  - Ecosistemas underground: foros, marketplaces y leak sites.
  - Telegram como fuente de inteligencia: Telethon y Pyrogram.
  - Procesamiento y enriquecimiento: MISP, VirusTotal y OpenCTI.
- Perfilado de actores y reporting.
  - Taxonomía de actores: IABs, APTs, RaaS y hacktivistas.
  - Construcción del perfil de un actor amenaza.
  - Informes para distintas audiencias y artefactos STIX 2.1.

MÓDULO

Inteligencia OSINT

Encuentra lo que otros dejan a la vista. **Aprende a planificar una investigación en fuentes abiertas** con método, a evaluar la fiabilidad de cada fuente y a recolectar información con técnicas de búsqueda avanzada y Google dorking en buscadores, bases de datos públicas, registros y foros.

Investiga personas y organizaciones en redes sociales (SOCMINT), extrae los metadatos EXIF de imágenes y documentos, y aplica la búsqueda inversa y la geolocalización para descubrir dónde y cuándo se tomó una fotografía. Aprende también a verificar lo que encuentras antes de darlo por bueno, porque en fuentes abiertas abundan los datos falsos y manipulados.

Mapea la huella digital de una organización: sus dominios, sus registros DNS y WHOIS y los servicios expuestos a internet que puedes descubrir con Shodan o Censys. Automatiza y escala la recolección con herramientas profesionales como Maltego, Recon-ng y SpiderFoot.

Cierra el módulo con **la ética y la normativa de la investigación OSINT**: cómo obtener información útil respetando la privacidad y la protección de datos, para que tus conclusiones sean válidas y no puedan impugnarse.

Contenidos:

- Metodología OSINT.
  - Planificación de la investigación.
  - Evaluación de la fiabilidad de las fuentes.
- Técnicas de búsqueda y recolección.
  - Búsqueda avanzada y Google dorking.
  - Investigación en redes sociales (SOCMINT).
  - Bases de datos públicas, registros y foros.
- Análisis de imágenes y metadatos.
  - Metadatos EXIF y búsqueda inversa de imágenes.
  - Geolocalización.
- Infraestructura y huella digital.
  - Dominios, DNS y WHOIS.
  - Servicios expuestos: Shodan y Censys.
- Automatización con Maltego, Recon-ng y SpiderFoot.
- Ética, privacidad y normativa en investigaciones OSINT.

MÓDULO

Inteligencia HUMINT y CORPINT

Obtén **inteligencia de la fuente más valiosa y menos predecible: las personas**. Aprende cómo se captan y gestionan fuentes humanas, cómo se conduce una entrevista y qué técnicas de elicitación permiten obtener información sin levantar sospechas, también en entornos digitales, donde el HUMINT virtual permite infiltrarse en comunidades online con identidades creíbles.

Comprende **cómo explotan los atacantes el factor humano mediante la ingeniería social** (phishing, pretexting, baiting o tailgating) y qué mecanismos psicológicos utilizan. Diseña programas de concienciación y controles que reduzcan la superficie de ataque humano de una organización.

Aplica la inteligencia al entorno empresarial con CORPINT: **recoge señales de fuentes internas y externas**, vigila a competidores, proveedores y cadena de suministro, y detecta a tiempo la amenaza interna, equilibrando la seguridad con los derechos de los empleados.

Termina el módulo integrando **la inteligencia corporativa en la toma de decisiones estratégicas** y estructurando su colaboración con los equipos de seguridad, legal, recursos humanos y dirección.

Contenidos:

- HUMINT: inteligencia de fuentes humanas.
  - Captación y gestión de fuentes.
  - Entrevista y técnicas de elicitación.
  - HUMINT virtual: infiltración en comunidades online.
- Ingeniería social.
  - Phishing, spear phishing, pretexting, baiting y tailgating.
  - Mecanismos psicológicos de la persuasión.
  - Concienciación y defensa frente a la manipulación.
- CORPINT: inteligencia corporativa.
  - Fuentes internas y externas.
  - Competidores, proveedores y cadena de suministro.
  - Amenaza interna (insider threat).
- Inteligencia corporativa aplicada a la estrategia.
  - Integración en la toma de decisiones.
  - Colaboración con seguridad, legal, RRHH y dirección.

MÓDULO

GRC y líneas de defensa

Alinea la seguridad con los objetivos del negocio. Comprende qué es el GRC (Gobierno, Riesgo y Cumplimiento), **por qué se ha convertido en un pilar estratégico de la ciberseguridad** y cómo se establecen las políticas, procedimientos y controles que definen quién decide y quién rinde cuentas en una organización.

Evalúa y gestiona los riesgos con metodologías reconocidas: **identifica los activos críticos, analiza sus amenazas y vulnerabilidades**, calcula el impacto potencial y define estrategias de mitigación para concentrar el esfuerzo donde más importa.

Desarrolla y mantén programas de cumplimiento que aseguren la conformidad con las regulaciones aplicables en un entorno cada vez más exigente, la base sobre la que se construyen los marcos normativos que verás más adelante.

Cierra el módulo con los **modelos de gobierno y el reparto de roles**. Aplica el modelo de las tres líneas de defensa, en el que la primera gestiona el riesgo, la segunda supervisa y la tercera audita, y entiende cómo se reparten las responsabilidades entre el CISO, el CIO, la dirección, los equipos técnicos y la auditoría interna.

Contenidos:

- Qué es GRC.
  - Gobierno, Riesgo y Cumplimiento como enfoque unificado.
  - Alineación de la seguridad con los objetivos del negocio.
- Gobierno de la seguridad.
  - Políticas, procedimientos y controles.
  - Responsabilidad y rendición de cuentas.
- Gestión de riesgos en ciberseguridad.
  - Identificación de activos críticos, amenazas y vulnerabilidades.
  - Cálculo del impacto y estrategias de mitigación.
- Cumplimiento normativo.
  - Programas de cumplimiento y principales regulaciones.
- Modelos de gobierno y roles.
  - El modelo de las tres líneas de defensa.
  - CISO, CIO, dirección, equipos técnicos y auditoría.

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

MÓDULO

ENS, NIS2 y marcos europeos

Domina el **mapa normativo de la ciberseguridad en España y en Europa**. Conoce en profundidad el Esquema Nacional de Seguridad (ENS), obligatorio en el sector público y para sus proveedores: sus principios, sus niveles de seguridad y las medidas de protección que exige en cada caso.

Compara los **grandes estándares internacionales**, ISO/IEC 27001, NIST Cybersecurity Framework y COBIT, con **sus alcances, sus diferencias y sus puntos en común**, y aprende a elegir e implementar el más adecuado según el sector y las necesidades de cada organización.

Aplica la Directiva NIS2: **evalúa si una organización entra en su ámbito, implanta las medidas de seguridad que exige y gestiona la notificación de incidentes** conforme a sus plazos. Entiende también cómo la DSA y la DMA redefinen las obligaciones de las plataformas digitales en la Unión Europea.

Termina el módulo con los **marcos europeos de cooperación, como el Reglamento de Cibersolidaridad o la normativa CSAM** contra el abuso sexual infantil en línea, y con el encaje del RGPD en todo este conjunto de obligaciones, para que sepas qué se exige a cada organización y cómo demostrar que lo cumple.

Contenidos:

- Esquema Nacional de Seguridad (ENS).
  - Principios, niveles de seguridad y medidas de protección.
  - Aplicación en el sector público y sus proveedores.
- Otros marcos y estándares.
  - ISO/IEC 27001, NIST Cybersecurity Framework y COBIT.
  - Criterios para elegir e implementar cada uno.
- Directiva NIS2.
  - Ámbito de aplicación y obligaciones de seguridad.
  - Gestión y notificación de incidentes.
- Regulación de servicios y mercados digitales: DSA y DMA.
- Cooperación europea: Cibersolidaridad y CSAM.
- Otros marcos europeos: RGPD y protección de datos.

MÓDULO

eIDAS2 e identidades modernas

Adapta tu organización al nuevo marco europeo de identidad digital. **Comprende el reglamento eIDAS2, sus objetivos, su alcance y sus tres niveles** de seguridad (bajo, sustancial y alto), y descubre qué supone la Cartera Europea de Identidad Digital para empresas y ciudadanos, con sus obligaciones y sus oportunidades.

Explora los servicios de confianza que regula: **la firma y el sello electrónicos, las marcas de tiempo y los servicios de autenticación**, junto con los requisitos que deben cumplir sus prestadores y cómo implantarlos para aprovechar la transformación digital sin salirte de la norma.

Implementa **la federación de identidades con los estándares más extendidos**, OAuth, OpenID Connect y SAML, para dar un acceso seguro, centralizado e interoperable a sistemas y datos. Entiende sus diferencias y cuándo conviene usar cada uno.

Cierra el módulo con el **modelo de identidad que devuelve el control al usuario**: las identidades autosoberanas (SSI), basadas en credenciales verificables, identificadores descentralizados (DID) y blockchain, y los casos reales que ya están transformando la gestión de la identidad digital.

Contenidos:

- eIDAS2: identidad electrónica en Europa.
  - Objetivos, alcance y niveles de seguridad: bajo, sustancial y alto.
  - Cartera Europea de Identidad Digital (EUDI Wallet).
  - Obligaciones y oportunidades para las organizaciones.
- Servicios de confianza.
  - Firma y sello electrónicos, marcas de tiempo y autenticación.
  - Requisitos de los prestadores de servicios de confianza.
- Federación de identidades.
  - OAuth, OpenID Connect y SAML.
  - Casos de uso e integración en arquitecturas modernas.
- Identidades autosoberanas (SSI).
  - Credenciales verificables y DID (Decentralized Identifiers).
  - Blockchain y casos de uso reales.

MÓDULO

Inteligencia artificial aplicada a la ciberseguridad

Aprovecha la inteligencia artificial también en defensa, porque los atacantes ya la usan. **Entiende cómo funcionan el aprendizaje supervisado, el no supervisado y el aprendizaje por refuerzo**, y qué aportan la clasificación, el clustering o la detección de anomalías para identificar patrones sospechosos antes de que se conviertan en un incidente.

Aplícala a la **protección de una organización**: detección de intrusiones y respuesta automática, análisis del comportamiento de usuarios y entidades (UEBA), identificación de APT y prevención del fraude, integrando estas soluciones con el SIEM. Descubre cómo acelera también el análisis forense.

Trabaja con **modelos de lenguaje (LLM) y copilots de ciberseguridad** para detectar phishing, analizar logs, clasificar malware y generar informes de incidentes en una fracción del tiempo habitual.

Termina el módulo con una mirada crítica: **los sesgos, la falta de interpretabilidad, el exceso de automatización y los ataques contra los propios modelos**, junto con las tendencias que vienen, como la ciberdefensa proactiva y la simulación automática de ataques.

Contenidos:

- Fundamentos de IA aplicada a la seguridad.
  - Aprendizaje supervisado, no supervisado y por refuerzo.
  - Clasificación, clustering y detección de anomalías.
- IA para la detección y la respuesta.
  - Detección de intrusiones y respuesta automática.
  - UEBA, amenazas persistentes avanzadas (APT) y fraude.
  - Integración con plataformas SIEM.
- LLM y copilots de ciberseguridad.
  - Detección de phishing y análisis de logs con NLP.
  - Clasificación de malware y generación de informes.
  - Copilots para analistas.
- IA en el análisis forense.
- Riesgos y límites de la IA.
  - Sesgos, falta de interpretabilidad y exceso de automatización.
  - Ataques contra los propios modelos de IA.
- Tendencias: ciberdefensa proactiva y simulación de ataques.

MÓDULO

Trabajo Final de Máster — TFM en Ciberseguridad

El Trabajo Final de Máster (TFM) es el momento en el que todo cobra sentido. **Desarrolla un Plan de Ciberseguridad integral para una empresa u organización, real o simulada**: analiza sus activos, sus amenazas y sus riesgos, y propón medidas concretas de protección. El resultado es **un documento profesional que demuestra tu capacidad para abordar la seguridad de una organización de forma global y estructurada**.

En él pondrás en juego lo aprendido en todo el programa: el análisis de riesgos, el gobierno y el cumplimiento normativo de los módulos de GRC, las técnicas ofensivas de Red Team y las defensivas de SecOps, la respuesta a incidentes y el análisis forense, y la inteligencia de amenazas.

Presentarás y defenderás el trabajo ante un tribunal de expertos del sector, que valorará no solo el documento, sino también tu capacidad para argumentar las decisiones tomadas, responder a preguntas técnicas y demostrar criterio propio ante situaciones imprevistas, igual que en un entorno profesional real.

Además, dependiendo de la modalidad elegida, puedes **optar a un premio gracias a la Competición de Becas**.

EQUIPO DOCENTE

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

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

EQUIPO DOCENTE

Directivos



Cristóbal Pareja Flores

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.



José Carlos Soto Gómez

Co-Director. 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. Especialista 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

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

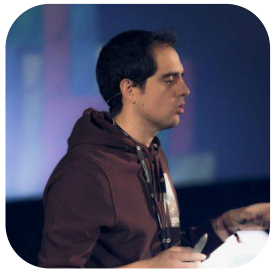
Security Engineer en BBVA. Especialista en Ciberseguridad, modelado de amenazas, inteligencia y seguridad en comunicaciones. Profesor de Big Data, Data Science e Inteligencia Artificial en la UCM. Miembro y divulgador de la Free Software Foundation (FSF) y la Electronic Frontier Foundation (EFF).



Román Ramírez Giménez

Director general y fundador de RootedCON

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

Dr Ingeniería Teleco, experto en Ciberseguridad y criptografía

Fundador y director de Criptored. 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.



Jézer Ferreira

Instructor experto en Fuentes Abierta en la INTERPOL

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

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.



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.

EQUIPO DOCENTE

Docentes



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.



Carlos Antonini Cepeda

Global Head of Red Team & Pentesting en Acciona

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.



Carlos Manchado Martín

Global CISO at Acciona

CISO global en multinacionales como Naturgy y Acciona. Director de Ciberseguridad para España en Microsoft. Directivo especializado en Ciberseguridad, Seguridad de la Información y Riesgos Tecnológicos. Asesor en estrategia de ciberdefensa. Consultor y asesor estratégico en compañías como E&Y, Accenture o Deloitte.



David Meléndez

Ingeniero en Informática e investigador en ciberseguridad

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.



Félix Brezo

Dr. en IT y Ms Análisis de Inteligencia y Seguridad de la Información

Más de 10 años de experiencia en ciberinteligencia. Actualmente lidera la unidad CTI de Telefónica Tech, gestionando la compartición y modelado de informes de inteligencia. Posee la Cruz al Mérito Policial con Distintivo Blanco y es autor de libros y publicaciones sobre investigación en fuentes abiertas. Ponente en eventos de Cibeseguridad



Fernando Rubio Román

CTO de Azure en Microsoft España

Responsable del equipo de especialistas técnicos de IA y desarrollo de software. Previamente, carrera en Microsoft con roles como responsable de seguridad en customer success, arquitecto de seguridad y respuesta a incidentes. Miembro del grupo de trabajo de IA del ISMS y ponente en eventos de seguridad (CCN-CERT, RootedCON).

EQUIPO DOCENTE

Docentes



Francisco Martín Vázquez

Gerente en auditoría interna de ciberseguridad en Telefónica

Profesional con más de 20 años de experiencia en tecnología y seguridad informática. Apasionado por la programación, sistemas Unix/Linux (*NIX) y la ciberseguridad, su carrera se ha centrado en el análisis, desarrollo e implementación de soluciones avanzadas para proteger infraestructuras críticas y datos sensibles.



Jacobo Blancas

AI, Threat Intelligence and Cybersecurity Advisor

Especialista en Inteligencia y Threat Intel con experiencia en el sector privado y como consultor independiente. Tiene formación en Filosofía y un Máster en Ciberseguridad, con especialización en HUMINT, OSINT e infiltración. Es coautor de un libro sobre inteligencia de amenazas y ha sido ponente en eventos de referencia como Black Hat y RootedCON.



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.



Jesús Angosto Iglesia

DFIR Technical Lead en Babel

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



Joaquín Molina

Auditor, hacker ético y red team

Profesional de gran reputación desde hace más de 20 años en Seguridad Informática. Cuenta con numerosas certificaciones y pertenece a organizaciones de reconocido nombre como ENISA o la obtención del premio Microsoft MVP los últimos años. Fundador de la consultora SeguridadSi.



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



Joseba García Velasco

Responsable del Arquitectura y Proyectos de Ciberseguridad

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.



Sara Concepción Mariscal

Analista Forense y Analista de Inteligencia en Telefónica Tech

Especialista en ciberseguridad con amplia trayectoria en análisis forense. Ha sido Analista e Incident Handler en respuesta a incidentes y coordinación de análisis de vulnerabilidades. Actualmente, es analista de inteligencia en Telefónica Tech, utilizando su experiencia para apoyar a equipos de respuesta.



Sofía Sánchez Margolles

Especialista en HUMINT | Analista de Threat Intelligence

Actualmente en Telefónica Tech es 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.



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.

Tú

Fúturo experto en CIberseguridad

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

-

SALIDAS PROFESIONALES

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

ntic master

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:

Operador de Red Team (Hacker Ético)

Ejecuta ataques controlados para evaluar la resistencia real de las infraestructuras críticas.

Especialista en DFIR (Forense)

Investiga incidentes, reconstruye ataques y preserva evidencias digitales con validez legal.

Especialista en DFIR (Forense)

Investiga incidentes, reconstruye ataques y preserva evidencias digitales con validez legal.

Analista de Operaciones Psicológicas

Detecta y neutraliza campañas de desinformación y ataques de ingeniería social avanzada.

CISO (Chief Information Security Officer)

Lidera la estrategia global de seguridad y la resiliencia digital en grandes organizaciones.

Analista de Blue Team (Defensa)

Gestiona la detección y respuesta ante intrusiones en centros de operaciones de seguridad (SOC).

Arquitecto de Seguridad Cloud

Diseña infraestructuras blindadas y gestiona la identidad en entornos AWS, Azure o Google Cloud.

Especialista en Seguridad de Aplicaciones

Audita el código y asegura el ciclo de vida del software mediante metodologías DevSecOps.

Analista de Ciberinteligencia

Evalúa el panorama de amenazas (TTPs) para diseñar estrategias de defensa proactivas.

Experto en Threat Hunting

Busca activamente indicadores de compromiso ocultos dentro de las redes corporativas.

ADMISIONES

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

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

PROCESO DE ADMISIÓN

Preinscripción
Envío de solicitud para evaluar candidaturas.

Preinscripción
Evaluación de candidaturas.

Preinscripción
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**

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

- 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**

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

- 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

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

UNIVERSIDAD COMPLUTENSE MADRID

ntic master

MÁSTER PRESENCIAL

Duración

1 Año / 520 horas

60 ECTS

Inicio: Febrero de 202
Fin: Febrero de 2028

Viernes de 16h a 21h
Sábados de 9h a 14h

Lugar

Facultad de Estudios Estadísticos

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

Precio

6.995 €

+ 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, noticias y contenidos.
- ➔ Foro de los módulos del máster.
- ➔ Comunicación con los profesores vía mensajería.
- ➔ Chat entre alumnos.

MÁSTER ONLINE

Duración

1 Año / 520 horas

60 ECTS

Inicio: Febrero de 2027

Fin: Febrero de 2028

Lugar

Plataforma Online

Precio

4.855€

+ 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, noticias 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@masterciberseguridaducm.com

Sitio Web

masterucm.com



UNIVERSIDAD COMPLUTENSE MADRID

ntic master