Máster Título Propio
Pentesting y Read Team

tech global university

tech global university

Máster Título Propio
Pentesting y Red Team

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Global University**
- Acreditación: **60 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: **www.techtitute.com/escuela-de-negocios/master/master-pentesting-red-team**

Índice

01 Presentación del programa — pág. 4

02 ¿Por qué estudiar en TECH? — pág. 8

03 Plan de estudios — pág. 12

04 Objetivos docentes — pág. 22

05 Salidas profesionales — pág. 26

06 Metodología de estudio — pág. 30

07 Cuadro docente — pág. 40

08 Titulación — pág. 44

01

Presentación del programa

En un contexto global donde las amenazas cibernéticas evolucionan a un ritmo acelerado, las organizaciones se enfrentan a desafíos cada vez más complejos para proteger sus activos digitales. Frente a esta situación, el *Pentesting* y el *Read Teaming* emergen como enfoques esenciales en la evaluación proactiva de la seguridad, permitiendo a los especialistas detectar vulnerabilidades antes de que sean explotadas por actores maliciosos. Por ello, es esencial que los profesionales adquieran competencias avanzadas para manejar las técnicas más modernas para la simulación de ataques y para fortalecer las infraestructuras digitales de las organizaciones. Con el objetivo de apoyarlos con dicha labor, TECH lanza un revolucionario programa universitario focalizado en la implementación de estas estrategias ofensivas.

Con este Máster Título Propio 100% online, liderarás estrategias de seguridad ofensiva y fortalecerás la resiliencia digital ante amenazas avanzadas"

Los ataques dirigidos, como el *ransomware* y la explotación de vulnerabilidades de día cero, representan amenazas críticas para las infraestructuras digitales en múltiples sectores. Aunque los sistemas de defensa convencionales ofrecen una primera línea de protección, los atacantes sofisticados logran evadir estas barreras. De ahí, la importancia de que los especialistas se mantengan al corriente de las metodologías más innovadoras de *Pentesting* y *Read Team* para evaluar la eficacia de los sistemas de seguridad existentes, identificar debilidades no detectadas y fortalecer las políticas de defensa cibernética en las instituciones.

En este escenario, TECH ha creado un vanguardista Máster Título Propio en *Pentesting* y *Read Team*. El itinerario académico profundizará en materias que comprenden desde los fundamentos de la seguridad ofensiva o la óptima gestión de los equipos de ciberseguridad hasta las técnicas más robustas para realizar simulaciones avanzadas de ataques y evaluar la resiliencia de las infraestructuras digitales. Además, se abordarán estrategias de evasión de defensas y el uso de software avanzado para la detección de vulnerabilidades. Gracias a esto, los alumnos desarrollarán habilidades técnicas para anticipar amenazas, mitigar riesgos y reforzar las defensas digitales de las organizaciones.

Por otro lado, esta titulación universitaria no solo ofrece un aprendizaje técnico profundo, sino también una visión estratégica. Su metodología 100% online, basada en el método *Relearning*, permite un aprendizaje flexible y autónomo, sin horarios ni traslados, facilitando la conciliación con responsabilidades laborales y personales. Además, cuenta con un cuadro docente de expertos en el área, garantizando que sean combinados teoría con casos reales para una preparación más efectiva. De esta forma, lo único que requerirán los egresados es contar con un dispositivo electrónico con conexión a internet para adentrase en el Campus Virtual.

Este **Máster Título Propio en *Pentesting y Red Team*** contiene el programa universitario más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en Pentesting y Read Team
- Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que están concebidos recogen una información científica y práctica sobre aquellas disciplinas indispensables para el ejercicio profesional
- Los ejercicios prácticos donde realizar el proceso de autoevaluación para mejorar el aprendizaje
- Su especial hincapié en metodologías innovadoras en Pentesting y Read Team
- Las lecciones teóricas, preguntas al experto, foros de discusión de temas controvertidos y trabajos de reflexión individual
- La disponibilidad de acceso a los contenidos desde cualquier dispositivo fijo o portátil con conexión a internet

Utilizarás herramientas avanzadas de análisis y evaluación de seguridad para identificar vulnerabilidades en diversos entornos digitales”

Manejarás las estrategias más sofisticadas para evaluar y mejorar la capacidad de respuesta de las arquitecturas digitales frente a amenazas"

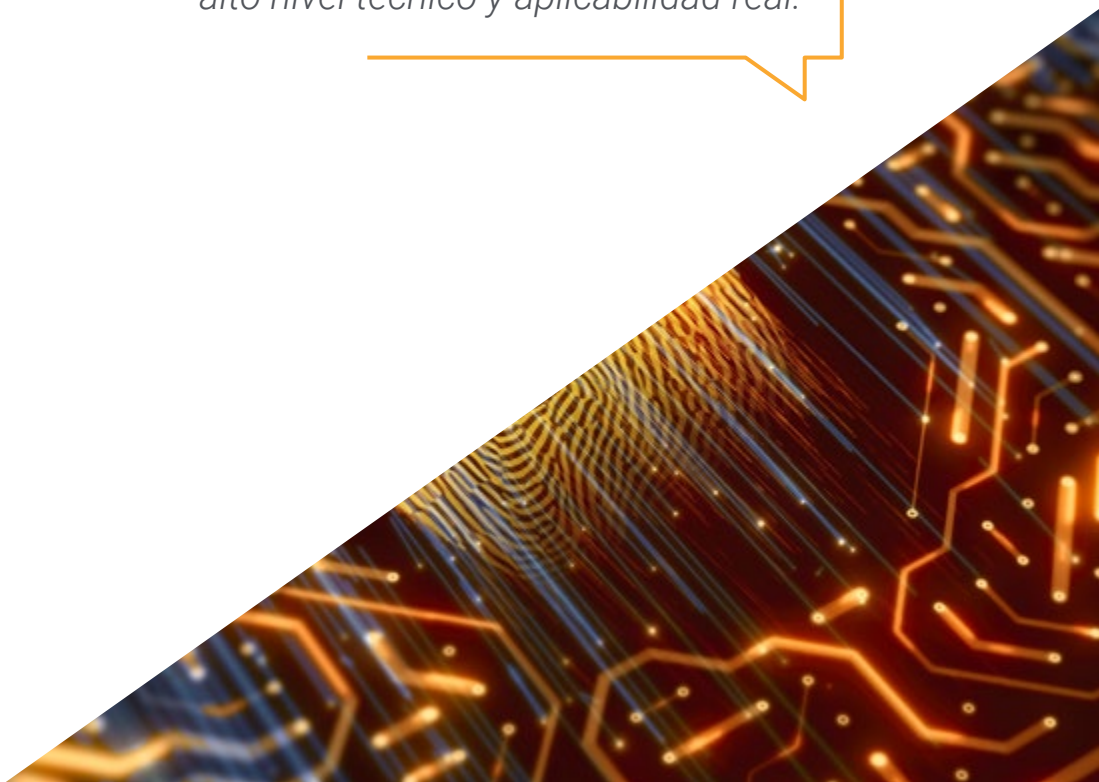
Profundizarás en la realización de simulaciones realistas de ciberataques mediante técnicas de Read Teaming.

Accederás a una biblioteca de recursos especializados disponible las 24 horas del día, con materiales de alto nivel técnico y aplicabilidad real.

Incluye en su cuadro docente a profesionales pertenecientes al ámbito del Pentesting y Read Team, que vierten en este programa la experiencia de su trabajo, además de reconocidos especialistas de sociedades de referencia y universidades de prestigio.

Su contenido multimedia, elaborado con la última tecnología educativa, permitirá al profesional un aprendizaje situado y contextual, es decir, un entorno simulado que proporcionará un estudio inmersivo programado para entrenarse ante situaciones reales.

El diseño de este programa se centra en el Aprendizaje Basado en Problemas, mediante el cual el alumno deberá tratar de resolver las distintas situaciones de práctica profesional que se le planteen a lo largo del curso académico. Para ello, el profesional contará con la ayuda de un novedoso sistema de vídeo interactivo realizado por reconocidos expertos.



02

¿Por qué estudiar en TECH?

TECH es la mayor Universidad digital del mundo. Con un impresionante catálogo de más de 14.000 programas universitarios, disponibles en 11 idiomas, se posiciona como líder en empleabilidad, con una tasa de inserción laboral del 99%. Además, cuenta con un enorme claustro de más de 6.000 profesores de máximo prestigio internacional.

Estudia en la mayor universidad digital del mundo y asegura tu éxito profesional. El futuro empieza en TECH”

La mejor universidad online del mundo según FORBES

La prestigiosa revista Forbes, especializada en negocios y finanzas, ha destacado a TECH como «la mejor universidad online del mundo». Así lo han hecho constar recientemente en un artículo de su edición digital en el que se hacen eco del caso de éxito de esta institución, «gracias a la oferta académica que ofrece, la selección de su personal docente, y un método de aprendizaje innovador orientado a formar a los profesionales del futuro».

El mejor claustro docente top internacional

El claustro docente de TECH está integrado por más de 6.000 profesores de máximo prestigio internacional. Catedráticos, investigadores y altos ejecutivos de multinacionales, entre los cuales se destacan Isaiah Covington, entrenador de rendimiento de los Boston Celtics; Magda Romanska, investigadora principal de MetaLAB de Harvard; Ignacio Wistumba, presidente del departamento de patología molecular traslacional del MD Anderson Cancer Center; o D.W Pine, director creativo de la revista TIME, entre otros.

La mayor universidad digital del mundo

TECH es la mayor universidad digital del mundo. Somos la mayor institución educativa, con el mejor y más amplio catálogo educativo digital, cien por cien online y abarcando la gran mayoría de áreas de conocimiento. Ofrecemos el mayor número de titulaciones propias, titulaciones oficiales de posgrado y de grado universitario del mundo. En total, más de 14.000 títulos universitarios, en once idiomas distintos, que nos convierten en la mayor institución educativa del mundo.

Los planes de estudio más completos del panorama universitario

TECH ofrece los planes de estudio más completos del panorama universitario, con temarios que abarcan conceptos fundamentales y, al mismo tiempo, los principales avances científicos en sus áreas científicas específicas. Asimismo, estos programas son actualizados continuamente para garantizar al alumnado la vanguardia académica y las competencias profesionales más demandadas. De esta forma, los títulos de la universidad proporcionan a sus egresados una significativa ventaja para impulsar sus carreras hacia el éxito.

Un método de aprendizaje único

TECH es la primera universidad que emplea el *Relearning* en todas sus titulaciones. Se trata de la mejor metodología de aprendizaje online, acreditada con certificaciones internacionales de calidad docente, dispuestas por agencias educativas de prestigio. Además, este disruptivo modelo académico se complementa con el "Método del Caso", configurando así una estrategia de docencia online única. También en ella se implementan recursos didácticos innovadores entre los que destacan vídeos en detalle, infografías y resúmenes interactivos.

La universidad online oficial de la NBA

TECH es la universidad online oficial de la NBA. Gracias a un acuerdo con la mayor liga de baloncesto, ofrece a sus alumnos programas universitarios exclusivos, así como una gran variedad de recursos educativos centrados en el negocio de la liga y otras áreas de la industria del deporte. Cada programa tiene un currículo de diseño único y cuenta con oradores invitados de excepción: profesionales con una distinguida trayectoria deportiva que ofrecerán su experiencia en los temas más relevantes.

Líderes en empleabilidad

TECH ha conseguido convertirse en la universidad líder en empleabilidad. El 99% de sus alumnos obtienen trabajo en el campo académico que ha estudiado, antes de completar un año luego de finalizar cualquiera de los programas de la universidad. Una cifra similar consigue mejorar su carrera profesional de forma inmediata. Todo ello gracias a una metodología de estudio que basa su eficacia en la adquisición de competencias prácticas, totalmente necesarias para el desarrollo profesional.

Google Partner Premier

El gigante tecnológico norteamericano ha otorgado a TECH la insignia Google Partner Premier. Este galardón, solo al alcance del 3% de las empresas del mundo, pone en valor la experiencia eficaz, flexible y adaptada que esta universidad proporciona al alumno. El reconocimiento no solo acredita el máximo rigor, rendimiento e inversión en las infraestructuras digitales de TECH, sino que también sitúa a esta universidad como una de las compañías tecnológicas más punteras del mundo.

La universidad mejor valorada por sus alumnos

Los alumnos han posicionado a TECH como la universidad mejor valorada del mundo en los principales portales de opinión, destacando su calificación más alta de 4,9 sobre 5, obtenida a partir de más de 1.000 reseñas. Estos resultados consolidan a TECH como la institución universitaria de referencia a nivel internacional, reflejando la excelencia y el impacto positivo de su modelo educativo.

03

Plan de estudios

Los materiales didácticos que conforman esta titulación universitaria han sido elaborados por expertos de renombre en la aplicación de técnicas vanguardistas de *Pentesting y Read Team*. Así, el plan de estudios abordará materias que abarcan desde las particularidades del funcionamiento de los equipos de ciberseguridad o la implementación de protocolos innovadores de seguridad hasta el uso de software de última generación para llevar a cabo simulaciones de ataques como malwares. Así, los alumnos desarrollarán competencias avanzadas para identificar vulnerabilidades críticas, diseñar estrategias ofensivas personalizadas y ejecutar evaluaciones de protección exhaustivas.

Diseñarás métodos que simulen ataques complejos y medirás la eficacia de los sistemas de defensas de las organizaciones”

Módulo 1. La seguridad ofensiva

1.1. Definición y contexto
- 1.1.1. Conceptos fundamentales de seguridad ofensiva
- 1.1.2. Importancia de la ciberseguridad en la actualidad
- 1.1.3. Desafíos y oportunidades en la seguridad ofensiva

1.2. Bases de la ciberseguridad
- 1.2.1. Primeros desafíos y evolución de las amenazas
- 1.2.2. Hitos tecnológicos y su impacto en la ciberseguridad
- 1.2.3. Ciberseguridad en la era moderna

1.3. Bases de la seguridad ofensiva
- 1.3.1. Conceptos clave y terminología
- 1.3.2. *Think outside the box*
- 1.3.3. Diferencias entre hacking ofensivo y defensivo

1.4. Metodologías de seguridad ofensiva
- 1.4.1. PTES (*penetration testing execution standard*)
- 1.4.2. OWASP (*open web application security project*)
- 1.4.3. *Cyber security kill chain*

1.5. Roles y responsabilidades en seguridad ofensiva
- 1.5.1. Principales perfiles
- 1.5.2. *Bug bounty hunters*
- 1.5.3. *Researching*: El arte de investigar

1.6. Arsenal del auditor ofensivo
- 1.6.1. Sistemas operativos para *hacking*
- 1.6.2. Introducción a los C2
- 1.6.3. Metasploit: Fundamentos y uso
- 1.6.4. Recursos útiles

1.7. OSINT: Inteligencia en fuentes abiertas
- 1.7.1. Fundamentos del OSINT
- 1.7.2. Técnicas y herramientas OSINT
- 1.7.3. Aplicaciones de OSINT en seguridad ofensiva

1.8. *Scripting*: Introducción a la automatización
- 1.8.1. Fundamentos de *scripting*
- 1.8.2. *Scripting* en Bash
- 1.8.3. *Scripting* en Python

1.9. Categorización de vulnerabilidades
- 1.9.1. CVE (*common vulnerabilities and exposure*)
- 1.9.2. CWE (*common weakness enumeration*)
- 1.9.3. CAPEC (*common attack pattern enumeration and classification*)
- 1.9.4. CVSS (*common vulnerability scoring system*)
- 1.9.5. MITRE ATT & CK

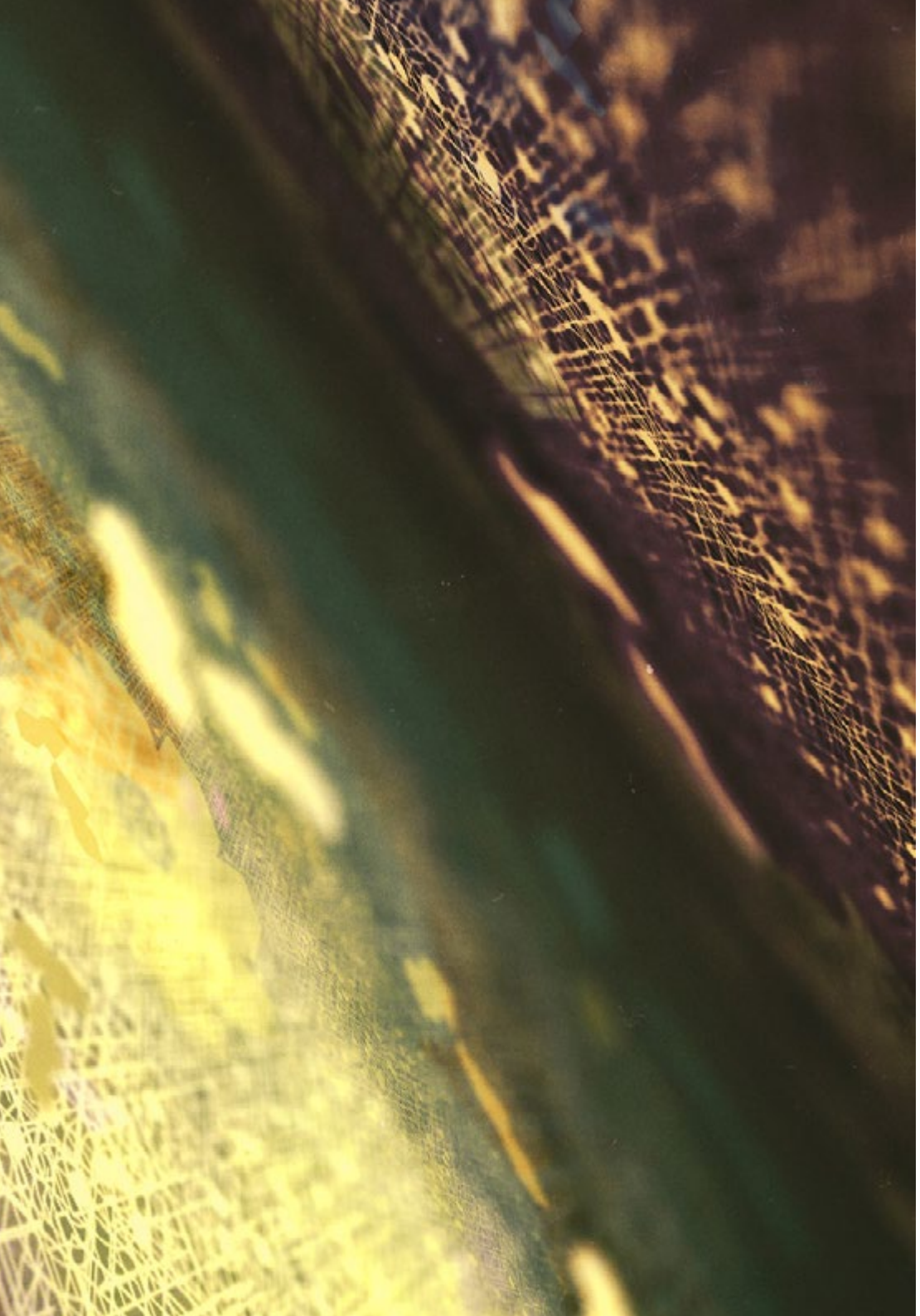
1.10. Ética y *hacking*
- 1.10.1. Principios de la ética *hacker*
- 1.10.2. La línea entre *hacking ético* y *hacking* malicioso
- 1.10.3. Implicaciones legales y consecuencias
- 1.10.4. Casos de estudio: Situaciones éticas en ciberseguridad

Módulo 2. Gestión de equipos de ciberseguridad

2.1. La gestión de equipos
- 2.1.1. Quién es quién
- 2.1.2. El director
- 2.1.3. Conclusiones

2.2. Roles y responsabilidades
- 2.2.1. Identificación de roles
- 2.2.2. Delegación efectiva
- 2.2.3. Gestión de expectativas

2.3. Formación y desarrollo de equipos
- 2.3.1. Etapas de formación de equipos
- 2.3.2. Dinámicas de grupo
- 2.3.3. Evaluación y retroalimentación



2.4. Gestión del talento
- 2.4.1. Identificación del talento
- 2.4.2. Desarrollo de capacidades
- 2.4.3. Retención de talentos

2.5. Liderazgo y motivación del equipo
- 2.5.1. Estilos de liderazgo
- 2.5.2. Teorías de la motivación
- 2.5.3. Reconocimiento de los logros

2.6. Comunicación y coordinación
- 2.6.1. Herramientas de comunicación
- 2.6.2. Barreras en la comunicación
- 2.6.3. Estrategias de coordinación

2.7. Planificaciones estratégicas del desarrollo profesional del personal
- 2.7.1. Identificación de necesidades de formación
- 2.7.2. Planes de desarrollo individual
- 2.7.3. Seguimiento y evaluación

2.8. Resolución de conflictos
- 2.8.1. Identificación de conflictos
- 2.8.2. Métodos de medición
- 2.8.3. Prevención de conflictos

2.9. Gestión de la calidad y la mejora continua
- 2.9.1. Principios de calidad
- 2.9.2. Técnicas para la mejora continua
- 2.9.3. *Feedback* y retroalimentación

2.10. Herramientas y tecnologías
- 2.10.1. Plataformas de colaboración
- 2.10.2. Gestión de proyectos
- 2.10.3. Conclusiones

Módulo 3. Gestión de proyectos de seguridad

3.1. La gestión de proyectos de seguridad
- 3.1.1. Definición y propósito de la gestión de proyectos en ciberseguridad
- 3.1.2. Principales desafíos
- 3.1.3. Consideraciones

3.2. Ciclo de vida de un proyecto de seguridad
- 3.2.1. Etapas iniciales y definición de objetivos
- 3.2.2. Implementación y ejecución
- 3.2.3. Evaluación y revisión

3.3. Planificación y estimación de recursos
- 3.3.1. Conceptos básicos de gestión económica
- 3.3.2. Determinación de recursos humanos y técnicos
- 3.3.3. Presupuestación y costos asociados

3.4. Ejecución y control del proyecto
- 3.4.1. Monitorización y seguimiento
- 3.4.2. Adaptación y cambios en el proyecto
- 3.4.3. Evaluación intermedia y revisiones

3.5. Comunicación y reporte del proyecto
- 3.5.1. Estrategias de comunicación efectiva
- 3.5.2. Elaboración de informes y presentaciones
- 3.5.3. Comunicación con el cliente y la dirección

3.6. Herramientas y tecnologías
- 3.6.1. Herramientas de planificación y organización
- 3.6.2. Herramientas de colaboración y comunicación
- 3.6.3. Herramientas de documentación y almacenamiento

3.7. Documentación y protocolos
- 3.7.1. Estructuración y creación de documentación
- 3.7.2. Protocolos de actuación
- 3.7.3. Guías

3.8. Normativas y cumplimiento en proyectos de ciberseguridad
- 3.8.1. Leyes y regulaciones internacionales
- 3.8.2. Cumplimiento
- 3.8.3. Auditorías

3.9. Gestión de riesgos en proyectos de seguridad
- 3.9.1. Identificación y análisis de riesgos
- 3.9.2. Estrategias de mitigación
- 3.9.3. Monitorización y revisión de riesgos

3.10. Cierre del proyecto
- 3.10.1. Revisión y evaluación
- 3.10.2. Documentación final
- 3.10.3. Feedback

Módulo 4. Ataques a redes y sistemas Windows

4.1. Windows y directorio activo
- 4.1.1. Historia y evolución de Windows
- 4.1.2. Conceptos básicos de directorio activo
- 4.1.3. Funciones y servicios del directorio activo
- 4.1.4. Arquitectura general del directorio activo

4.2. Redes en entornos de directorio activo
- 4.2.1. Protocolos de red en Windows
- 4.2.2. *DNS* y su funcionamiento en el directorio activo
- 4.2.3. Herramientas de diagnóstico de red
- 4.2.4. Implementación de redes en directorio activo

4.3. Autenticación y autorización en directorio activo
- 4.3.1. Proceso y flujo de autenticación
- 4.3.2. Tipos de credenciales
- 4.3.3. Almacenamiento y gestión de credenciales
- 4.3.4. Seguridad en la autenticación

4.4. Permisos y políticas en directorio activo
- 4.4.1. *GPOs*
- 4.4.2. Aplicación y gestión de GPOs
- 4.4.3. Administración de permisos en directorio activo
- 4.4.4. Vulnerabilidades y mitigaciones en permisos

4.5. Fundamentos de Kerberos
- 4.5.1. ¿Qué es Kerberos?
- 4.5.2. Componentes y funcionamiento
- 4.5.3. *Tickets* en *Kerberos*
- 4.5.4. *Kerberos* en el contexto de directorio activo

4.6. Técnicas avanzadas en Kerberos
- 4.6.1. Ataques comunes en Kerberos
- 4.6.2. Mitigaciones y protecciones
- 4.6.3. Monitorización del tráfico Kerberos
- 4.6.4. Ataques avanzados en Kerberos

4.7. *Active Directory Certificate Services* (ADCS)
- 4.7.1. Conceptos básicos de PKI
- 4.7.2. Roles y componentes de ADCS
- 4.7.3. Configuración y despliegue de ADCS
- 4.7.4. Seguridad en ADCS

4.8. Ataques y defensas en *Active Directory Certificate Services* (ADCS)
- 4.8.1. Vulnerabilidades comunes en ADCS
- 4.8.2. Ataques y técnicas de explotación
- 4.8.3. Defensas y mitigaciones
- 4.8.4. Monitorización y auditoría de ADCS

4.9. Auditoría del Directorio Activo
- 4.9.1. Importancia de la auditoría en el Directorio Activo
- 4.9.2. Herramientas de auditoría
- 4.9.3. Detección de anomalías y comportamientos sospechosos
- 4.9.4. Respuesta a incidentes y recuperación

4.10. Azure AD
- 4.10.1. Conceptos básicos de Azure AD
- 4.10.2. Sincronización con el Directorio Activo local
- 4.10.3. Gestión de identidades en Azure AD
- 4.10.4. Integración con aplicaciones y servicios

Módulo 5. *Hacking web* avanzado

5.1. Funcionamiento de una web
- 5.1.1. La URL y sus partes
- 5.1.2. Los métodos HTTP
- 5.1.3. Las cabeceras
- 5.1.4. Cómo ver peticiones web con *Burp Suite*

5.2. Sesiones
- 5.2.1. Las *cookies*
- 5.2.2. *Tokens* JWT
- 5.2.3. Ataques de robo de sesión
- 5.2.4. Ataques a JWT

5.3. *Cross site scripting* (XSS)
- 5.3.1. Qué es un XSS
- 5.3.2. Tipos de XSS
- 5.3.3. Explotando un XSS
- 5.3.4. Introducción a los *XSLeaks*

5.4. Inyecciones a bases de datos
- 5.4.1. Qué es una SQL *injection*
- 5.4.2. Exfiltrando información con SQLi
- 5.4.3. *SQLi blind*, *Time based* y *error based*
- 5.4.4. Inyecciones NoSQLi

5.5. *Path traversal* y local *file inclusion*
- 5.5.1. Qué son y sus diferencias
- 5.5.2. Filtros comunes y cómo saltarlos
- 5.5.3. Log *poisoning*
- 5.5.4. LFIs en PHP

5.6. *Broken authentication*
- 5.6.1. *User enumeration*
- 5.6.2. *Password bruteforce*
- 5.6.3. 2FA *Bypass*
- 5.6.4. Cookies con información sensible y modificable

5.7. *Remote command execution*
- 5.7.1. *Command injection*
- 5.7.2. *Blind command injection*
- 5.7.3. *Insecure deserialization* PHP
- 5.7.4. *Insecure deserialization* Java

5.8. *File uploads*
- 5.8.1. RCE *mediante webshells*
- 5.8.2. XSS en subidas de ficheros
- 5.8.3. XML *external entity* (XXE) *injection*
- 5.8.4. *Path traversal* en subidas de fichero

5.9. *Broken access* Control
- 5.9.1. Acceso a paneles sin restricción
- 5.9.2. *Insecure direct object references* (IDOR)
- 5.9.3. *Bypass* de filtros
- 5.9.4. Métodos de autorización insuficientes

5.10. Vulnerabilidades de DOM y ataques más avanzados
- 5.10.1. *Regex denial of service*
- 5.10.2. DOM *clobbering*
- 5.10.3. *Prototype pollution*
- 5.10.4. HTTP *request smuggling*

Módulo 6. Arquitectura y seguridad en redes

6.1. Las redes informáticas
- 6.1.1. Conceptos básicos: Protocolos LAN, WAN, CP, CC
- 6.1.2. Modelo OSI y TCP/IP
- 6.1.3. *Switching*: Conceptos básicos
- 6.1.4. *Routing*: Conceptos básicos

6.2. *Switching*
- 6.2.1. Introducción a VLAN's
- 6.2.2. *STP*
- 6.2.3. EtherChannel
- 6.2.4. Ataques a capa 2

6.3. VLAN´s
- 6.3.1. Importancia de las VLAN's
- 6.3.2. Vulnerabilidades en VLAN's
- 6.3.3. Ataques comunes en VLAN's
- 6.3.4. Mitigaciones

6.4. Routing
- 6.4.1. Direccionamiento IP- IPv4 e IPv6
- 6.4.2. Enrutamiento: Conceptos clave
- 6.4.3. Enrutamiento estático
- 6.4.4. Enrutamiento dinámico: Introducción

6.5. Protocolos IGP
- 6.5.1. RIP
- 6.5.2. OSPF
- 6.5.3. RIP vs OSPF
- 6.5.4. Análisis de necesidades de la topología

6.6. Protección perimetral
- 6.6.1. DMZs
- 6.6.2. *Firewalls*
- 6.6.3. Arquitecturas comunes
- 6.6.4. *Zero trust network access*

6.7. IDS e IPS
- 6.7.1. Características
- 6.7.2. Implementación
- 6.7.3. SIEM y SIEM CLOUDS
- 6.7.4. Detección basada en *honeypots*

6.8. TLS y *VPN´s*
- 6.8.1. SSL/TLS
- 6.8.2. TLS: Ataques comunes
- 6.8.3. VPNs con TLS
- 6.8.4. VPNs con IPSEC

6.9. Seguridad en redes inalámbricas
- 6.9.1. Introducción a las redes inalámbricas
- 6.9.2. Protocolos
- 6.9.3. Elementos claves
- 6.9.4. Ataques comunes

6.10. Redes empresariales y cómo afrontarlas
- 6.10.1. Segmentación lógica
- 6.10.2. Segmentación física
- 6.10.3. Control de acceso
- 6.10.4. Otras medidas a tomar en cuenta

Módulo 7. Análisis y desarrollo de *malware*

7.1. Análisis y desarrollo de *malware*
- 7.1.1. Historia y evolución del *malware*
- 7.1.2. Clasificación y tipos de *malware*
- 7.1.3. Análisis de *malware*
- 7.1.4. Desarrollo de *malware*

7.2. Preparando el entorno
- 7.2.1. Configuración de Máquinas Virtuales y *snapshots*
- 7.2.2. Herramientas para análisis de *malware*
- 7.2.3. Herramientas para desarrollo de *malware*

7.3. Fundamentos de Windows
- 7.3.1. Formato de fichero PE (*portable executable*)
- 7.3.2. Procesos y *threads*
- 7.3.3. Sistema de archivos y registro
- 7.3.4. Windows Defender

7.4. Técnicas de *malware* básicas
- 7.4.1. Generación de *shellcode*
- 7.4.2. Ejecución de *shellcode* en disco
- 7.4.3. Disco vs memoria
- 7.4.4. Ejecución de *shellcode* en memoria

7.5. Técnicas de *malware* intermedias
- 7.5.1. Persistencia en Windows
- 7.5.2. Carpeta de inicio
- 7.5.3. Claves del registro
- 7.5.4. Salvapantallas

7.6. Técnicas de *malware* avanzadas
- 7.6.1. Cifrado de *shellcode* (XOR)
- 7.6.2. Cifrado de *shellcode* (RSA)
- 7.6.3. Ofuscación de *strings*
- 7.6.4. Inyección de procesos

7.7. Análisis estático de *malware*
- 7.7.1. Analizando packers con DIE (detect it easy)
- 7.7.2. Analizando secciones con PE-Bear
- 7.7.3. Decompilación con Ghidra

7.8. Análisis dinámico de *malware*
- 7.8.1. Observando el comportamiento con Process Hacker
- 7.8.2. Analizando llamadas con API Monitor
- 7.8.3. Analizando cambios de registro con Regshot
- 7.8.4. Observando peticiones en red con TCPView

7.9. Análisis en .NET
- 7.9.1. Introducción a .NET
- 7.9.2. Decompilando con *dnSpy*
- 7.9.3. Depurando con *dnSpy*

7.10. Analizando un *malware* real
- 7.10.1. Preparando el entorno
- 7.10.2. Análisis estático del *malware*
- 7.10.3. Análisis dinámico del *malware*
- 7.10.4. Creación de reglas YARA

Módulo 8. Fundamentos forenses y DFIR

8.1. Forense digital
- 8.1.1. Historia y evolución de la informática forense
- 8.1.2. Importancia de la informática forense en la ciberseguridad
- 8.1.3. Historia y evolución de la informática forense

8.2. Fundamentos de la informática forense
- 8.2.1. Cadena de custodia y su aplicación
- 8.2.2. Tipos de evidencia digital
- 8.2.3. Procesos de adquisición de evidencia

8.3. Sistemas de archivos y estructura de datos
- 8.3.1. Principales sistemas de archivos
- 8.3.2. Métodos de ocultamiento de datos
- 8.3.3. Análisis de metadatos y atributos de archivos

8.4. Análisis de sistemas operativos
- 8.4.1. Análisis forense de sistemas Windows
- 8.4.2. Análisis forense de sistemas Linux
- 8.4.3. Análisis forense de sistemas macOS

8.5. Recuperación de datos y análisis de disco
- 8.5.1. Recuperación de datos de medios dañados
- 8.5.2. Herramientas de análisis de disco
- 8.5.3. Interpretación de tablas de asignación de archivos

8.6. Análisis de redes y tráfico
- 8.6.1. Captura y análisis de paquetes de red
- 8.6.2. Análisis de registros de firewall
- 8.6.3. Detección de intrusiones en red

8.7. *Malware* y análisis de código malicioso
- 8.7.1. Clasificación de *malware* y sus características
- 8.7.2. Análisis estático y dinámico de *malware*
- 8.7.3. Técnicas de desensamblado y depuración

8.8. Análisis de registros y eventos
- 8.8.1. Tipos de registros en sistemas y aplicaciones
- 8.8.2. Interpretación de eventos relevantes
- 8.8.3. Herramientas de análisis de registros

8.9. Responder a incidentes de seguridad
- 8.9.1. Proceso de respuesta a incidentes
- 8.9.2. Creación de un plan de respuesta a incidentes
- 8.9.3. Coordinación con equipos de seguridad

8.10. Presentación de evidencia y jurídico
- 8.10.1. Reglas de evidencia digital en el ámbito legal
- 8.10.2. Preparación de informes forenses
- 8.10.3. Comparecencia en juicio como testigo experto

Módulo 9. Ejercicios de *Read Team* avanzados

9.1. Técnicas avanzadas de reconocimiento
- 9.1.1. Enumeración avanzada de subdominios
- 9.1.2. Google Dorking avanzado
- 9.1.3. Redes Sociales y The Harvester

9.2. Campañas de phishing avanzadas
- 9.2.1. Qué es *reverse proxy phishing*
- 9.2.2. 2FA *Bypass* con *Evilginx*
- 9.2.3. Exfiltración de datos

9.3. Técnicas avanzadas de persistencia
- 9.3.1. *Golden tickets*
- 9.3.2. *Silver tickets*
- 9.3.3. Técnica DCShadow

9.4. Técnicas avanzadas de evasión
- 9.4.1. *Bypass* de AMSI
- 9.4.2. Modificación de herramientas existentes
- 9.4.3. Ofuscación de Powershell

9.5. Técnicas avanzadas de movimiento lateral
- 9.5.1. *Pass the titcket* (ptt)
- 9.5.2. *Overpass the hash* (*pass the key*)
- 9.5.3. *NTLM Relay*

9.6. Técnicas avanzadas de post-explotación
- 9.6.1. *Dump* de LSASS
- 9.6.2. *Dump* de SAM
- 9.6.3. Ataque DCSync

9.7. Técnicas avanzadas de *pivoting*
- 9.7.1. Qué es el *pivoting*
- 9.7.2. Túneles con SSH
- 9.7.3. *Pivoting* con Chisel

9.8. Intrusiones físicas
- 9.8.1. Vigilancia y reconocimiento
- 9.8.2. *Tailgating* y *piggybacking*
- 9.8.3. *Lock-picking*

9.9. Ataques Wi-Fi
- 9.9.1. Ataques a WPA/WPA2 PSK
- 9.9.2. Ataques de *rogue* AP
- 9.9.3. Ataques a WPA2 Enterprise

9.10. Ataques RFID
- 9.10.1. Lectura de tarjetas RFID
- 9.10.2. Manipulación de tarjetas RFID
- 9.10.3. Creación de tarjetas clonadas

Módulo 10. Reporte técnico y ejecutivo

10.1. Proceso de reporte
- 10.1.1. Estructura de un reporte
- 10.1.2. Proceso de reporte
- 10.1.3. Conceptos clave
- 10.1.4. Ejecutivo vs técnico

10.2. Guías
- 10.2.1. Introducción
- 10.2.2. Tipos de guías
- 10.2.3. Guías nacionales
- 10.2.4. Casos de uso

10.3. Metodologías
- 10.3.1. Evaluación
- 10.3.2. *Pentesting*
- 10.3.3. Repaso de metodologías comunes
- 10.3.4. Introducción a metodologías nacionales

10.4. Enfoque técnico de la fase de reporte
- 10.4.1. Entendiendo los límites del *pentester*
- 10.4.2. Uso y claves del lenguaje
- 10.4.3. Presentación de la información
- 10.4.4. Errores comunes

10.5. Enfoque ejecutivo de la fase de reporte
- 10.5.1. Ajustando el informe al contexto
- 10.5.2. Uso y claves del lenguaje
- 10.5.3. Estandarización
- 10.5.4. Errores comunes

10.6. OSSTMM
- 10.6.1. Entendiendo la metodología
- 10.6.2. Reconocimiento
- 10.6.3. Documentación
- 10.6.4. Elaboración del informe

10.7. LINCE
- 10.7.1. Entendiendo la metodología
- 10.7.2. Reconocimiento
- 10.7.3. Documentación
- 10.7.4. Elaboración del informe

10.8. Reportando vulnerabilidades
- 10.8.1. Conceptos clave
- 10.8.2. Cuantificación del alcance
- 10.8.3. Vulnerabilidades y evidencias
- 10.8.4. Errores comunes

10.9. Enfocando el informe al cliente
- 10.9.1. Importancia de las pruebas de trabajo
- 10.9.2. Soluciones y mitigaciones
- 10.9.3. Datos sensibles y relevantes
- 10.9.4. Ejemplos prácticos y casos

10.10. Reportando *retakes*
- 10.10.1. Conceptos claves
- 10.10.2. Entendiendo la información heredada
- 10.10.3. Comprobación de errores
- 10.10.4. Añadiendo información

04

Objetivos docentes

El Máster Título Propio en Pentesting y Read Team tiene como objetivo preparar expertos en ciberseguridad ofensiva capaces de identificar, analizar y explotar vulnerabilidades en entornos complejos. Los egresados serán capaces de liderar equipos de seguridad, gestionar proyectos y ejecutar pruebas de penetración avanzadas en redes, sistemas y aplicaciones web. Aprenderán a diseñar estrategias de defensa efectivas y responder a incidentes mediante técnicas forenses de vanguardia.

Desarrollarás la capacidad de liderar equipos especializados, gestionando proyectos de seguridad y coordinando estrategias de defensa cibernética"

Objetivos generales

- Aplicar conocimientos teóricos en escenarios prácticos y simulaciones, enfrentándose a desafíos reales para fortalecer habilidades de *Pentesting*
- Aprender a asignar eficientemente recursos dentro de un equipo de ciberseguridad, considerando las habilidades individuales y maximizando la productividad en proyectos
- Mejorar habilidades de comunicación específicas para entornos técnicos, facilitando la comprensión y coordinación entre los miembros del equipo
- Aprender técnicas de seguimiento y control de proyectos, identificando desviaciones y tomando acciones correctivas según sea necesario
- Desarrollar competencias para evaluar y mejorar las configuraciones de seguridad en sistemas Windows, asegurando la implementación de medidas eficaces
- Promover prácticas éticas y legales en la ejecución de ataques y pruebas en sistemas Windows, considerando los principios éticos de la ciberseguridad
- Familiarizar al egresado con la evaluación de la seguridad en APIs y servicios web, identificando posibles puntos de vulnerabilidad y fortaleciendo la seguridad en interfaces de programación
- Fomentar la colaboración efectiva con equipos de seguridad, integrando estrategias y esfuerzos para proteger la infraestructura de red

Objetivos específicos

Módulo 1. La seguridad ofensiva
- Identificar y aplicar metodologías de seguridad ofensiva utilizadas en pruebas de penetración y auditorías de sistemas
- Comprender el marco legal y ético en el que se desarrolla la ciberseguridad ofensiva

Módulo 2. Gestión de equipos de ciberseguridad
- Desarrollar estrategias de liderazgo y coordinación en equipos de seguridad ofensiva y defensiva
- Implementar metodologías ágiles y de gestión para la optimización de procesos en ciberseguridad

Módulo 3. Gestión de proyectos de seguridad
- Planificar y ejecutar proyectos de ciberseguridad alineados con los objetivos estratégicos de las organizaciones
- Evaluar riesgos y definir planes de mitigación efectivos para mejorar la seguridad empresarial

Módulo 4. Ataques a redes y sistemas Windows
- Analizar y explotar vulnerabilidades en redes y entornos Windows utilizando herramientas especializadas
- Aplicar técnicas de evasión y persistencia para evaluar la efectividad de las medidas de seguridad implementadas

Módulo 5. *Hacking web* avanzado
- Identificar y explotar vulnerabilidades en aplicaciones web mediante pruebas de penetración especializadas
- Aplicar técnicas avanzadas de inyección SQL, *Cross-Site Scripting* y *Server-Side Request Forgery*

Módulo 6. Arquitectura y seguridad en redes
- Diseñar infraestructuras seguras aplicando principios de segmentación y control de tráfico
- Analizar ataques en redes corporativas y proponer soluciones de mitigación efectivas

Módulo 7. Análisis y desarrollo de *malware*
- Diseñar y analizar código malicioso para comprender su funcionamiento y mecanismos de ataque
- Implementar técnicas de ingeniería inversa para la detección y neutralización de amenazas avanzadas

Módulo 8. Fundamentos forenses y DFIR
- Aplicar técnicas de análisis forense para la recolección y preservación de evidencias digitales
- Implementar estrategias de respuesta a incidentes para contener y mitigar ciberataques en tiempo real

Módulo 9. Ejercicios de *Read Team* avanzados
- Desarrollar campañas de ataque simuladas para evaluar la resiliencia de infraestructuras críticas
- Aplicar metodologías avanzadas de *Read Teaming* para replicar escenarios de ataque realistas

Módulo 10. Informe técnico y ejecutivo
- Elaborar informes técnicos detallados con hallazgos, análisis y recomendaciones de seguridad
- Redactar informes ejecutivos dirigidos a la alta dirección con estrategias de mitigación y gestión de riesgos

05

Salidas profesionales

Con este completísimo Máster Título Propio en *Pentesting y Red Team*, los profesionales manejarán las técnicas más avanzadas para detectar vulnerabilidades, ejecutar simulaciones de ataques y fortalecer infraestructuras digitales. Gracias a esto, estarán altamente preparados para acceder a roles estratégicos de mayor importancia en las empresas como analistas de ciberseguridad o consultores en seguridad ofensiva, brindando competencias avanzadas en detección de amenazas y defensa proactiva.

Te desempeñarás como Especialista en Red Teaming, creando simulaciones exhaustivas para evaluar la resiliencia de las infraestructuras digitales y la capacidad de respuesta de los equipos"

Perfil del egresado

El egresado de este programa universitario será un experto elevadamente capacitado para identificar vulnerabilidades, ejecutar simulaciones de ciberataques y fortalecer infraestructuras digitales. A su vez, estará preparado para liderar operaciones de seguridad ofensiva, gestionar incidentes y desarrollar estrategias de defensa proactiva, garantizando la protección de los sistemas frente a amenazas avanzadas. Además, podrá asesorar a organizaciones en la implementación de políticas de ciberseguridad, cumplir con normativas internacionales y coordinar equipos multidisciplinarios para enfrentar desafíos complejos en entornos digitales.

Diseñarás estrategias de seguridad proactivas, que permitirán a las empresas responder eficazmente ante una variedad de incidentes.

- **Análisis de *Malware* e Ingeniería Inversa:** Competencia en la creación, detección y desensamblado de software malicioso para comprender sus mecanismos y desarrollar contramedidas efectivas
- ***Read Teaming* y Simulación de Ataques:** Capacidad para ejecutar ejercicios avanzados de *Read Team*, replicando amenazas reales para evaluar la resiliencia de infraestructuras críticas
- **Respuesta a Incidentes y Análisis Forense:** Habilidad para identificar, contener y mitigar incidentes de seguridad mediante técnicas forenses avanzadas
- **Diseño y Seguridad en Redes:** Conocimiento en la implementación de arquitecturas seguras, aplicando principios de segmentación, control de tráfico y mitigación de ataques en redes corporativas

Después de realizar el programa Máster Título Propio, podrás desempeñar tus conocimientos y habilidades en los siguientes cargos:

1. **Especialista en *Pentesting* y Seguridad Ofensiva:** Encargado de realizar pruebas de penetración en infraestructuras digitales, identificando y explotando vulnerabilidades para fortalecer la seguridad empresarial.
2. **Líder de *Read Team* y Simulación de Ataques:** Responsable de diseñar y ejecutar ejercicios avanzados de *Read Teaming*, replicando escenarios de ataque realistas para evaluar la resiliencia de los sistemas.
3. **Gestor de Ciberseguridad en Empresas y Organismos Gubernamentales:** Supervisor de estrategias de seguridad ofensiva y defensiva, asegurando el cumplimiento de normativas y la mitigación de riesgos digitales.
4. **Analista de Malware e Ingeniería Inversa:** Especialista en el estudio, desarrollo y desmontaje de software malicioso, aplicando técnicas de ingeniería inversa para la detección y neutralización de amenazas.
5. **Consultor en Seguridad Web y Evaluación de Vulnerabilidades:** Asesor de empresas en la identificación y mitigación de riesgos en aplicaciones web, utilizando metodologías avanzadas de hacking ético.
6. **Director de Respuesta a Incidentes y Forense Digital:** Responsable de coordinar la detección, análisis y mitigación de ciberataques.
7. **Arquitecto de Redes y Seguridad:** Encargado del diseño y mantenimiento de infraestructuras seguras, implementando medidas de protección para prevenir ataques en redes corporativas.
8. **Gestor de Proyectos de Seguridad Informática:** Líder en la planificación y ejecución de estrategias de ciberseguridad, asegurando la alineación con los objetivos empresariales y normativas internacionales.
9. **Especialista en Inteligencia de Amenazas Cibernéticas:** Analista de tendencias y técnicas utilizadas por actores maliciosos, proporcionando información clave para la anticipación y mitigación de ataques.
10. **Instructor y Formador en Ciberseguridad Ofensiva:** Responsable de capacitar equipos de seguridad, impartiendo conocimientos avanzados en *Pentesting, Read Teaming* y gestión de incidentes.

Gestionarás acciones para contener, analizar y reducir el impacto de ciberataques; garantizando la protección de las informaciones sensibles"

06

Metodología de estudio

TECH es la primera universidad en el mundo que combina la metodología de los ***case studies*** con el ***Relearning***, un sistema de aprendizaje 100% online basado en la reiteración dirigida.

Esta disruptiva estrategia pedagógica ha sido concebida para ofrecer a los profesionales la oportunidad de actualizar conocimientos y desarrollar competencias de un modo intensivo y riguroso. Un modelo de aprendizaje que coloca al estudiante en el centro del proceso académico y le otorga todo el protagonismo, adaptándose a sus necesidades y dejando de lado las metodologías más convencionales.

TECH te prepara para afrontar nuevos retos en entornos inciertos y lograr el éxito en tu carrera"

El alumno: la prioridad de todos los programas de TECH

En la metodología de estudios de TECH el alumno es el protagonista absoluto. Las herramientas pedagógicas de cada programa han sido seleccionadas teniendo en cuenta las demandas de tiempo, disponibilidad y rigor académico que, a día de hoy, no solo exigen los estudiantes sino los puestos más competitivos del mercado.

Con el modelo educativo asincrónico de TECH, es el alumno quien elige el tiempo que destina al estudio, cómo decide establecer sus rutinas y todo ello desde la comodidad del dispositivo electrónico de su preferencia. El alumno no tendrá que asistir a clases en vivo, a las que muchas veces no podrá acudir. Las actividades de aprendizaje las realizará cuando le venga bien. Siempre podrá decidir cuándo y desde dónde estudiar.

“En TECH NO tendrás clases en directo (a las que luego nunca puedes asistir)”

Los planes de estudios más exhaustivos a nivel internacional

TECH se caracteriza por ofrecer los itinerarios académicos más completos del entorno universitario. Esta exhaustividad se logra a través de la creación de temarios que no solo abarcan los conocimientos esenciales, sino también las innovaciones más recientes en cada área.

Al estar en constante actualización, estos programas permiten que los estudiantes se mantengan al día con los cambios del mercado y adquieran las habilidades más valoradas por los empleadores. De esta manera, quienes finalizan sus estudios en TECH reciben una preparación integral que les proporciona una ventaja competitiva notable para avanzar en sus carreras.

Y además, podrán hacerlo desde cualquier dispositivo, pc, tableta o smartphone.

El modelo de TECH es asincrónico, de modo que te permite estudiar con tu pc, tableta o tu smartphone donde quieras, cuando quieras y durante el tiempo que quieras”

Case studies o Método del caso

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de negocios del mundo. Desarrollado en 1912 para que los estudiantes de Derecho no solo aprendiesen las leyes a base de contenidos teóricos, su función era también presentarles situaciones complejas reales. Así, podían tomar decisiones y emitir juicios de valor fundamentados sobre cómo resolverlas. En 1924 se estableció como método estándar de enseñanza en Harvard.

Con este modelo de enseñanza es el propio alumno quien va construyendo su competencia profesional a través de estrategias como el *Learning by doing* o el *Design Thinking*, utilizadas por otras instituciones de renombre como Yale o Stanford.

Este método, orientado a la acción, será aplicado a lo largo de todo el itinerario académico que el alumno emprenda junto a TECH. De ese modo se enfrentará a múltiples situaciones reales y deberá integrar conocimientos, investigar, argumentar y defender sus ideas y decisiones. Todo ello con la premisa de responder al cuestionamiento de cómo actuaría al posicionarse frente a eventos específicos de complejidad en su labor cotidiana.

Método *Relearning*

En TECH los *case studies* son potenciados con el mejor método de enseñanza 100% online: el *Relearning*.

Este método rompe con las técnicas tradicionales de enseñanza para poner al alumno en el centro de la ecuación, proveyéndole del mejor contenido en diferentes formatos. De esta forma, consigue repasar y reiterar los conceptos clave de cada materia y aprender a aplicarlos en un entorno real.

En esta misma línea, y de acuerdo a múltiples investigaciones científicas, la reiteración es la mejor manera de aprender. Por eso, TECH ofrece entre 8 y 16 repeticiones de cada concepto clave dentro de una misma lección, presentada de una manera diferente, con el objetivo de asegurar que el conocimiento sea completamente afianzado durante el proceso de estudio.

El Relearning te permitirá aprender con menos esfuerzo y más rendimiento, implicándote más en tu especialización, desarrollando el espíritu crítico, la defensa de argumentos y el contraste de opiniones: una ecuación directa al éxito.

Un Campus Virtual 100% online con los mejores recursos didácticos

Para aplicar su metodología de forma eficaz, TECH se centra en proveer a los egresados de materiales didácticos en diferentes formatos: textos, vídeos interactivos, ilustraciones y mapas de conocimiento, entre otros. Todos ellos, diseñados por profesores cualificados que centran el trabajo en combinar casos reales con la resolución de situaciones complejas mediante simulación, el estudio de contextos aplicados a cada carrera profesional y el aprendizaje basado en la reiteración, a través de audios, presentaciones, animaciones, imágenes, etc.

Y es que las últimas evidencias científicas en el ámbito de las Neurociencias apuntan a la importancia de tener en cuenta el lugar y el contexto donde se accede a los contenidos antes de iniciar un nuevo aprendizaje. Poder ajustar esas variables de una manera personalizada favorece que las personas puedan recordar y almacenar en el hipocampo los conocimientos para retenerlos a largo plazo. Se trata de un modelo denominado *Neurocognitive context-dependent e-learning* que es aplicado de manera consciente en esta titulación universitaria.

Por otro lado, también en aras de favorecer al máximo el contacto mentor-alumno, se proporciona un amplio abanico de posibilidades de comunicación, tanto en tiempo real como en diferido (mensajería interna, foros de discusión, servicio de atención telefónica, email de contacto con secretaría técnica, chat y videoconferencia).

Asimismo, este completísimo Campus Virtual permitirá que el alumnado de TECH organice sus horarios de estudio de acuerdo con su disponibilidad personal o sus obligaciones laborales. De esa manera tendrá un control global de los contenidos académicos y sus herramientas didácticas, puestas en función de su acelerada actualización profesional.

> *La modalidad de estudios online de este programa te permitirá organizar tu tiempo y tu ritmo de aprendizaje, adaptándolo a tus horarios”*

La eficacia del método se justifica con cuatro logros fundamentales:

1. Los alumnos que siguen este método no solo consiguen la asimilación de conceptos, sino un desarrollo de su capacidad mental, mediante ejercicios de evaluación de situaciones reales y aplicación de conocimientos.
2. El aprendizaje se concreta de una manera sólida en capacidades prácticas que permiten al alumno una mejor integración en el mundo real.
3. Se consigue una asimilación más sencilla y eficiente de las ideas y conceptos, gracias al planteamiento de situaciones que han surgido de la realidad.
4. La sensación de eficiencia del esfuerzo invertido se convierte en un estímulo muy importante para el alumnado, que se traduce en un interés mayor en los aprendizajes y un incremento del tiempo dedicado a trabajar en el curso.

La metodología universitaria mejor valorada por sus alumnos

Los resultados de este innovador modelo académico son constatables en los niveles de satisfacción global de los egresados de TECH.

La valoración de los estudiantes sobre la calidad docente, calidad de los materiales, estructura del curso y sus objetivos es excelente. No en valde, la institución se convirtió en la universidad mejor valorada por sus alumnos según el índice global score, obteniendo un 4,9 de 5.

Accede a los contenidos de estudio desde cualquier dispositivo con conexión a Internet (ordenador, tablet, smartphone) gracias a que TECH está al día de la vanguardia tecnológica y pedagógica.

Podrás aprender con las ventajas del acceso a entornos simulados de aprendizaje y el planteamiento de aprendizaje por observación, esto es, Learning from an expert.

Así, en este programa estarán disponibles los mejores materiales educativos, preparados a conciencia:

Material de estudio

Todos los contenidos didácticos son creados por los especialistas que van a impartir el curso, específicamente para él, de manera que el desarrollo didáctico sea realmente específico y concreto.

Estos contenidos son aplicados después al formato audiovisual que creará nuestra manera de trabajo online, con las técnicas más novedosas que nos permiten ofrecerte una gran calidad, en cada una de las piezas que pondremos a tu servicio.

Prácticas de habilidades y competencias

Realizarás actividades de desarrollo de competencias y habilidades específicas en cada área temática. Prácticas y dinámicas para adquirir y desarrollar las destrezas y habilidades que un especialista precisa desarrollar en el marco de la globalización que vivimos.

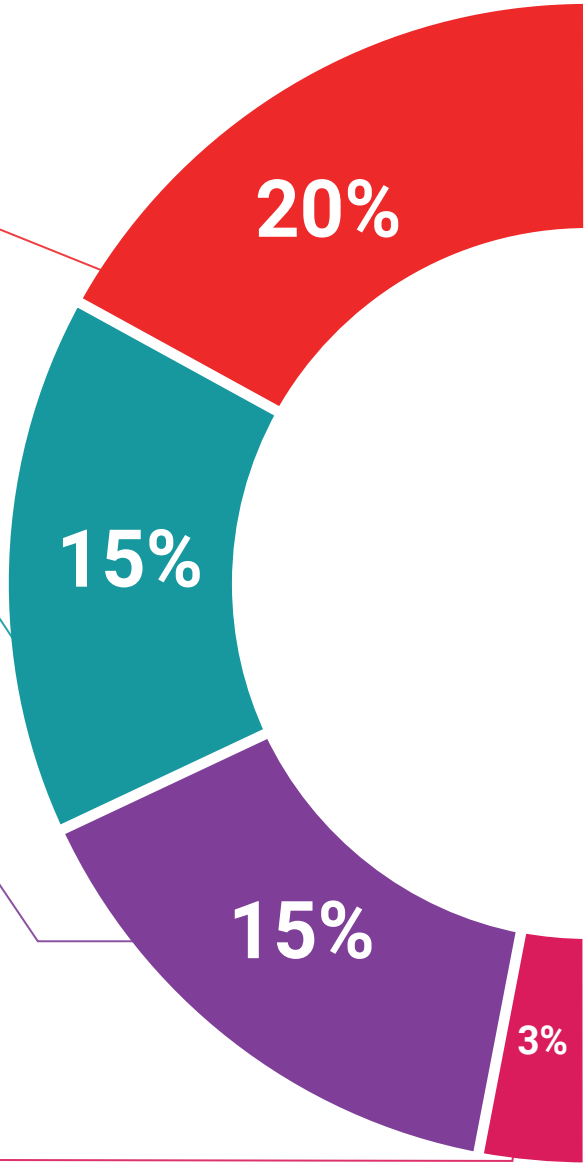
Resúmenes interactivos

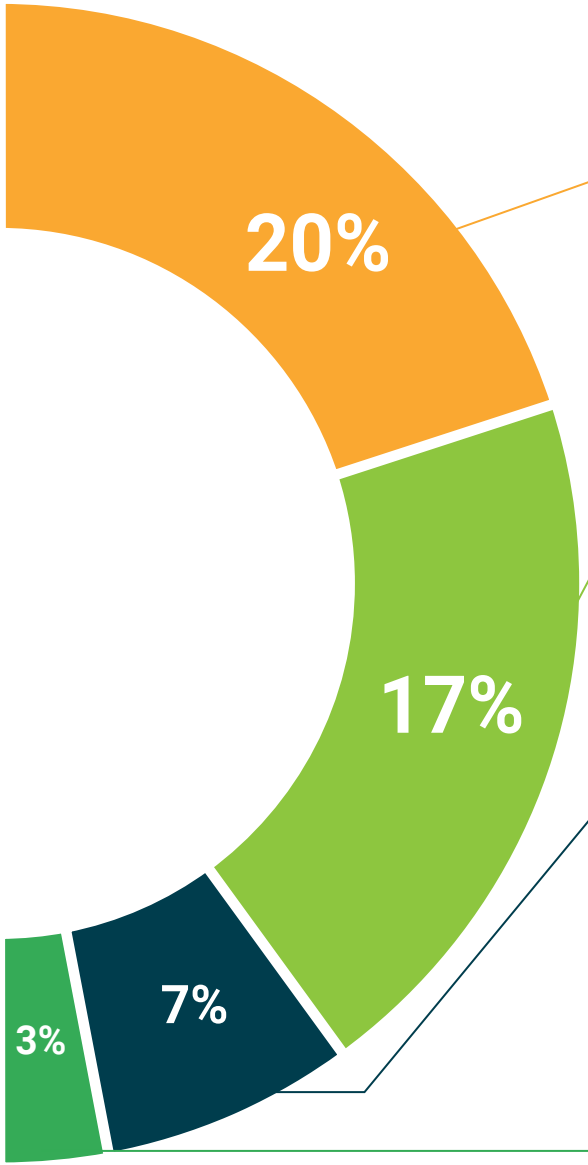
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

Este sistema exclusivo educativo para la presentación de contenidos multimedia fue premiado por Microsoft como "Caso de éxito en Europa".

Lecturas complementarias

Artículos recientes, documentos de consenso, guías internacionales... En nuestra biblioteca virtual tendrás acceso a todo lo que necesitas para completar tu capacitación.





Case Studies

Completarás una selección de los mejores *case studies* de la materia. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.

Testing & Retesting

Evaluamos y reevaluamos periódicamente tu conocimiento a lo largo del programa. Lo hacemos sobre 3 de los 4 niveles de la Pirámide de Miller.

Clases magistrales

Existe evidencia científica sobre la utilidad de la observación de terceros expertos.

El denominado *Learning from an expert* afianza el conocimiento y el recuerdo, y genera seguridad en nuestras futuras decisiones difíciles.

Guías rápidas de actuación

TECH ofrece los contenidos más relevantes del curso en forma de fichas o guías rápidas de actuación. Una manera sintética, práctica y eficaz de ayudar al estudiante a progresar en su aprendizaje.

07

Cuadro docente

Este programa universitario cuenta con un cuadro docente de prestigio internacional, compuesto por expertos en Pesting y Red Team. De esta forma, han elaborado múltiples contenidos didácticos que sobresalen tanto por su elevada calidad como por adaptarse a las demandas del mercado laboral actual. Así pues, los egresados se adentrarán en una experiencia de alta intensidad que ampliará sus perspectivas laborales de manera significativa.

Accederás a una titulación universitaria diseñada por verdaderos referentes en la aplicación de soluciones de Pentesting y Red Team en el ámbito organizacional"

Dirección

D. Gómez Pintado, Carlos

- Gerente de Ciberseguridad y Red Team Cipherbit en Grupo Oesía
- Gerente *Advisor & Investor* en Wesson App
- Graduado en Ingeniería del Software y Tecnologías de la Sociedad de la Información, por la Universidad Politécnica de Madrid
- Colabora con instituciones educativas para la confección de Ciclos Formativos de Grado Superior en ciberseguridad

Profesores

D. Siles Rubia, Marcelino

- Cibersecurity Engineer
- Ingeniería de la Ciberseguridad en la Universidad Rey Juan Carlos
- Conocimientos: Programación Competitiva, *Hacking Web, Active Directory y Malware Development*
- Ganador del Concurso AdaByron

D. Redondo Castro, Pablo

- Pentester en Grupo Oesía
- Ingeniero de Ciberseguridad por Universidad Rey Juan Carlos
- Amplia experiencia como *Cibersecurity Evaluator Traineev*
- Acumula experiencia docente, impartiendo formaciones relacionadas con torneos de Capture The Flag

D. Gallego Sánchez, Alejandro

- Pentester en Grupo Oesía
- Consultor de Ciberseguridad en Integración Tecnológica Empresarial, S.L
- Técnico Audiovisual en Ingeniería Audiovisual S.A
- Graduado en Ingeniería de la Ciberseguridad por la Universidad Rey Juan Carlos

D. Mora Navas, Sergio

- Consultor en Ciberseguridad en Grupo Oesía
- Ingeniero en Ciberseguridad por la Universidad Rey Juan Carlos
- Ingeniero Informático por la Universidad de Burgos

D. González Parrilla, Yuba

- Coordinador de Línea Seguridad Ofensiva y Red Team
- Especialista en Dirección de Proyectos *Predictive* en Project Management Institute
- Especialista en *SmartDefense*
- Experto en *Web Application Penetration Tester* en eLearnSecurity
- *Junior Penetration Tester* en eLearnSecurity
- Graduado en Ingeniería computacional en Universidad Politécnica de Madrid

D. González Sanz, Marcos

- Consultor de Ciberseguridad en Cipherbit
- eLearnSecurity Certified eXploit Developer
- Offensive Security Certified Professional
- Offensive Security Wireless Professional
- Virtual Hacking Labs Plus
- Graduado en Ingeniería del Software por la Universidad Politécnica de Madrid

D. Villaverde, David

- Consultor de Ciberseguridad en Cipherbit
- Experto en Plataformas de Retos de Hacking y HackTheBox
- Especialista en Pentesting
- Experto en Malware
- Ingeniero de software especializado en ciberseguridad por el Centro Universitario de Tecnología y Arte Digital Las Rozas

D. Castillo, Carlos

- Cybersecurity Consultant y Red Teamer en Cipherbit
- Offensive Security Wireless Professional
- eLearnSecurity Web Application Penetration Tester
- eLearnSecurity Certified Professional Penetration Tester v2
- eLearnSecurity Junior Penetration Tester
- Consultor de Ciberseguridad
- Ingeniero de Software por la Universidad Politécnica de Madrid

Una experiencia de capacitación única, clave y decisiva para impulsar tu desarrollo profesional"

08

Titulación

El Máster Título Propio en Pentesting y Red Team garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Máster Propio expedido por TECH Global University.

Supera con éxito este programa y recibe tu titulación universitaria sin desplazamientos ni farragosos trámites”

Este programa te permitirá obtener el título propio de **Máster Título Propio en Pentesting y Red Team** avalado por **TECH Global University**, la mayor Universidad digital del mundo.

TECH Global University, es una Universidad Oficial Europea reconocida públicamente por el Gobierno de Andorra (*boletín oficial*). Andorra forma parte del Espacio Europeo de Educación Superior (EEES) desde 2003. El EEES es una iniciativa promovida por la Unión Europea que tiene como objetivo organizar el marco formativo internacional y armonizar los sistemas de educación superior de los países miembros de este espacio. El proyecto promueve unos valores comunes, la implementación de herramientas conjuntas y fortaleciendo sus mecanismos de garantía de calidad para potenciar la colaboración y movilidad entre estudiantes, investigadores y académicos.

Este título propio de **TECH Global University**, es un programa europeo de formación continua y actualización profesional que garantiza la adquisición de las competencias en su área de conocimiento, confiriendo un alto valor curricular al estudiante que supere el programa.

Título: **Máster Título Propio en Pentesting y Red Team**

Modalidad: **online**

Duración: **12 meses**

Acreditación: **60 ECTS**

tech global university

D/Dña _____, con documento de identificación _____ ha superado con éxito y obtenido el título de:

Máster Título Propio en Pentesting y Red Team

Se trata de un título propio de 1.800 horas de duración equivalente a 60 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH Global University es una universidad reconocida oficialmente por el Gobierno de Andorra el 31 de enero de 2024, que pertenece al Espacio Europeo de Educación Superior (EEES).

En Andorra la Vella, a 28 de febrero de 2024

Dr. Pedro Navarro Illana
Rector

código único TECH: AFWOR23S techtitute.com/titulos

Máster Título Propio en Pentesting y Red Team

Distribución General del Plan de Estudios

Tipo de materia	Créditos ECTS
Obligatoria (OB)	60
Optativa (OP)	0
Prácticas Externas (PR)	0
Trabajo Fin de Máster (TFM)	0
	Total 60

Distribución General del Plan de Estudios

Curso	Materia	ECTS	Carácter
1º	seguridad ofensiva	6	OB
1º	Gestión de equipos de ciberseguridad	6	OB
1º	Gestión de proyectos de seguridad	6	OB
1º	Ataques a redes y sistemas Windows	6	OB
1º	*Hacking web* avanzado	6	OB
1º	Arquitectura y seguridad en redes	6	OB
1º	Análisis y desarrollo de *malware*	6	OB
1º	Fundamentos forenses y DFIR	6	OB
1º	Ejercicios de *Read Team* avanzados	6	OB
1º	Reporte técnico y ejecutivo	6	OB

Dr. Pedro Navarro Illana
Rector

tech global university

*Apostilla de La Haya. En caso de que el alumno solicite que su título en papel recabe la Apostilla de La Haya, TECH Global University realizará las gestiones oportunas para su obtención, con un coste adicional.

tech global university

Máster Título Propio
Pentesting y Red Team

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Global University**
- Acreditación: **60 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Máster Título Propio
Pentesting y Read Team

tech global university