Máster de Formación Permanente

Pentesting y Red Team

tech universidad

tech universidad

Máster de Formación Permanente
Pentesting y Red Team

- Modalidad: **online**
- Duración: **7 meses**
- Titulación: **TECH Universidad**
- Acreditación: **60 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: **www.techtitute.com/informatica/master/master-pentesting-red-team**

Índice

01

Presentación del programa

El *Pentesting* y el *Red Team* se han convertido en elementos esenciales para la ciberseguridad en un mundo cada vez más digitalizado. Según un informe del Instituto Nacional de Ciberseguridad, se estima que los costos globales por cibercrimen alcanzarán los 10,5 billones de dólares anuales para 2025, lo que subraya la importancia de tener profesionales capacitados en estas áreas. Este panorama ha generado una creciente demanda de expertos en seguridad cibernética. En este contexto, el programa universitario de TECH se plantea como una respuesta a esta necesidad, ofreciendo una metodología innovadora que, a través de material didáctico 100% online, permitirá a los egresados desarrollar competencias prácticas y analíticas necesarias para liderar equipos de seguridad en escenarios de alta complejidad.

Este Máster de Formación Permanente 100% online te brindará el conocimiento excepcional necesario para dominar el Pentesting y el Red Team"

En la actualidad, la seguridad digital enfrenta desafíos complejos debido a la creciente sofisticación de los ataques cibernéticos. De hecho, el *Pentesting* y el *Red Team* se han vuelto fundamentales para evaluar la seguridad de sistemas y redes. A su vez, estas prácticas permiten a las organizaciones identificar y abordar vulnerabilidades antes de que sean explotadas, mejorando así su defensa frente a amenazas reales. Asimismo, la importancia de estas metodologías radica en su capacidad para proporcionar una visión detallada de las debilidades de una infraestructura y fortalecer su protección.

Teniendo en cuenta lo anterior, TECH Universidad profundizará en temas clave de ciberseguridad, abarcando la gestión de equipos especializados, fundamentales en la defensa de redes y sistemas. También, se incluirá el análisis de ataques dirigidos a redes y sistemas Windows, ofreciendo técnicas avanzadas para mitigar riesgos y prevenir amenazas recientes. Además, se integrará el *hacking* web, proporcionando herramientas para detectar y neutralizar vulnerabilidades en entornos digitales. Esto permitirá al profesional estar preparado para enfrentar las amenazas más sofisticadas, asegurando una defensa sólida en el panorama actual.

Posteriormente, este enfoque integral proporcionará al alumnado habilidades fundamentales para gestionar riesgos y proteger infraestructuras críticas. Del mismo modo, la capacidad de identificar brechas de seguridad, gestionar incidentes y aplicar estrategias de mitigación contribuye a fortalecer la seguridad organizacional. Como resultado, los egresados estarán mejor preparados para enfrentar los desafíos cibernéticos en un entorno en constante evolución.

Finalmente, la metodología de TECH Universidad permitirá una experiencia de capacitación flexible y accesible. A través del método *Relearning*, los profesionales podrán acceder a contenidos relevantes las 24 horas del día, los 7 días de la semana, desde cualquier dispositivo con conexión a internet. Este enfoque online garantizará que los egresados puedan avanzar a su propio ritmo, asegurando una inmersión total en los conceptos, independientemente de su ubicación o disponibilidad horaria.

Este **Máster de Formación Permanente 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 Red 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 ciberseguridad
- 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

> *Diseñarás simulaciones realistas de ataques cibernéticos replicando tácticas, técnicas y procedimientos utilizados por los actores maliciosos”*

Adquirirás las habilidades necesarias para gestionar equipos especializados, fundamentales en la defensa de redes y sistemas”

Profundizarás en la comprensión de las vulnerabilidades de redes y sistemas Windows, permitiendo el diseño de estrategias ajustadas a cada entorno.

Te mantendrás actualizado en técnicas avanzadas de hacking web, liderando proyectos de innovación en ciberseguridad.

Incluye en su cuadro docente a profesionales pertenecientes al ámbito del Pentesting y Red 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 contextualizado, 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 Wistuba, 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

Este plan de estudios abordará los conceptos clave en materia de *Pentesting* y *Red Team*. Por ejemplo, se ahondará en técnicas avanzadas para simular ataques y evaluar la seguridad de sistemas, lo que permitirá a los profesionales identificar vulnerabilidades antes de que sean explotadas. Además, se trabajará en el análisis de redes y sistemas en entornos controlados, con el objetivo de replicar amenazas reales y desarrollar respuestas adecuadas. Este enfoque práctico fortalecerá la capacidad para implementar medidas preventivas y defensivas, optimizando la protección de infraestructuras críticas frente a ciberataques.

Desarrollarás una visión táctica y actualizada sobre las principales amenazas digitales"

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 *Red 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 theHarvester

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 - Ticket* (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

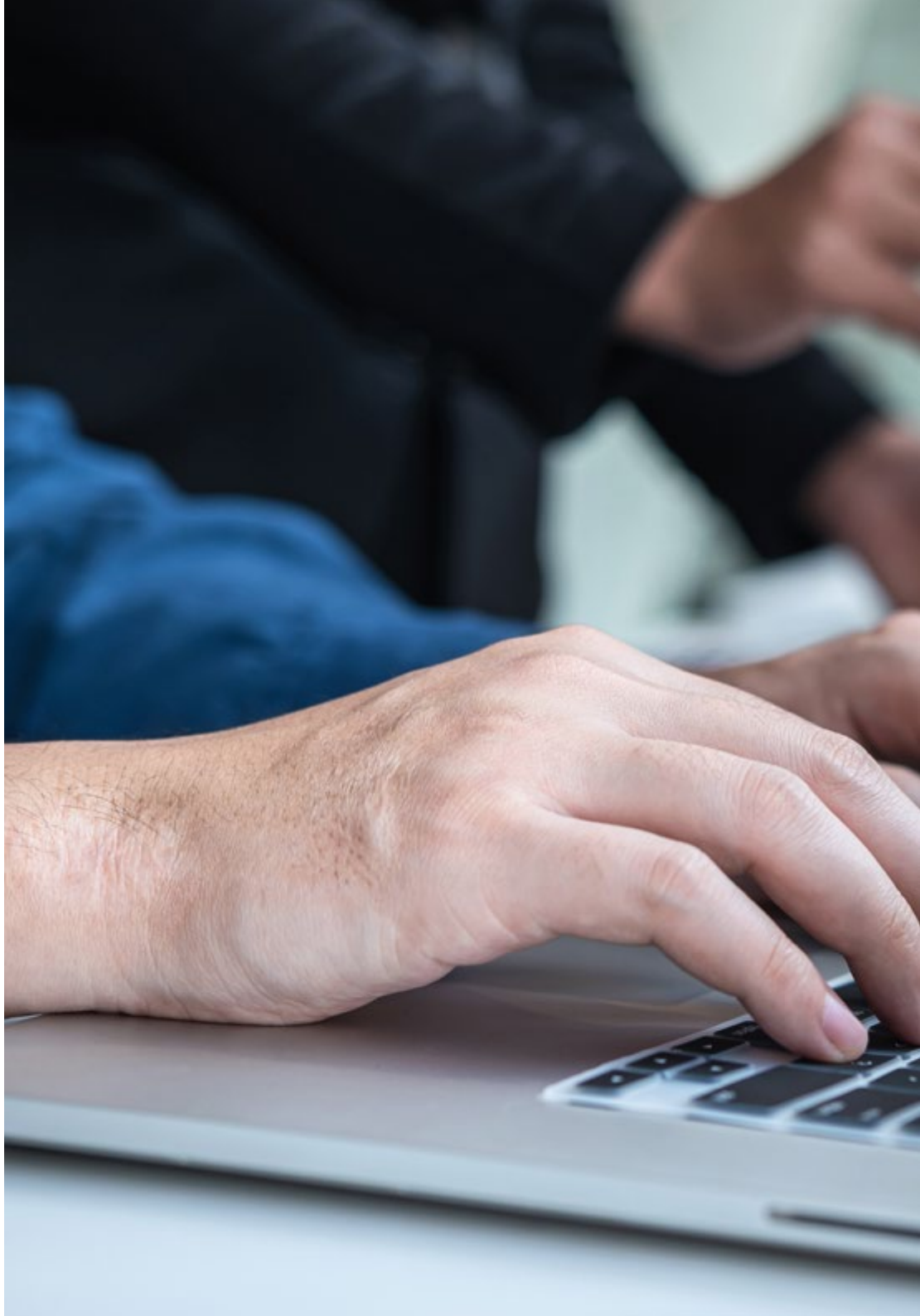
Objetivos docentes

Este Máster de Formación Permanente tiene como finalidad proporcionar una comprensión sólida sobre *Pentesting* y *Red Team*, permitiendo desarrollar competencias esenciales para proteger infraestructuras digitales. A través del análisis de sistemas operativos específicos para hacking, los profesionales adquirirán habilidades avanzadas para identificar y explotar vulnerabilidades. Además, se fomentará la capacidad de pensar de manera innovadora, adoptando un enfoque "*Think Outside the Box*" para abordar desafíos complejos en ciberseguridad. Como resultado, estas competencias permitirán diseñar soluciones eficaces ante ataques cibernéticos, fortaleciendo la defensa de redes y sistemas en diversos entornos, y mejorando la capacidad de respuesta ante amenazas avanzadas.

Dominarás las técnicas avanzadas para el análisis y de sistemas operativos específicos para hacking"

Objetivos generales

- Implementar estrategias de seguridad ofensiva en entornos digitales, detectando y mitigando vulnerabilidades
- Gestionar equipos de ciberseguridad para optimizar la defensa contra amenazas cibernéticas
- Planificar y ejecutar proyectos de seguridad, garantizando la protección de infraestructuras críticas
- Analizar y prevenir ataques a redes y sistemas Windows, mejorando la seguridad
- Desarrollar competencias en *hacking* web avanzado para identificar y neutralizar vulnerabilidades en entornos web
- Diseñar arquitecturas seguras en redes, implementando medidas preventivas contra ataques
- Analizar y desarrollar *malware*, mejorando las capacidades defensivas ante amenazas avanzadas
- Aplicar fundamentos forenses y DFIR para investigar y responder eficazmente a incidentes de seguridad



Objetivos específicos

Módulo 1. La seguridad ofensiva

- Desarrollar habilidades para aplicar metodologías de seguridad ofensiva, como PTES y OWASP, en entornos de prueba controlados
- Adquirir conocimientos sobre el uso de herramientas y sistemas operativos para *hacking*, como *Metasploit* y C2, en auditorías de seguridad
- Analizar y categorizar vulnerabilidades utilizando estándares como CVE, CWE y CVSS, para mejorar la capacidad de respuesta ante amenazas
- Comprender los principios éticos del *hacking*, diferenciando entre prácticas éticas y maliciosas, y evaluando sus implicaciones legales

Módulo 2. Gestión de equipos de ciberseguridad

- Desarrollar competencias para identificar roles y delegar responsabilidades de manera efectiva dentro de un equipo de ciberseguridad
- Implementar estrategias de liderazgo y motivación, adaptando estilos para potenciar el rendimiento del equipo
- Aplicar técnicas de gestión del talento, centradas en la identificación, desarrollo y retención de profesionales en ciberseguridad
- Integrar herramientas y tecnologías para mejorar la comunicación y coordinación en equipos, optimizando la gestión de proyectos y la colaboración

Módulo 3. Gestión de proyectos de seguridad

- Desarrollar competencias para gestionar el ciclo completo de proyectos de ciberseguridad, desde la definición de objetivos hasta la evaluación final
- Aplicar técnicas de planificación y estimación de recursos, optimizando la asignación de recursos humanos y técnicos en proyectos de seguridad
- Implementar estrategias de comunicación efectiva para la elaboración de informes y la interacción con clientes y la dirección en proyectos de ciberseguridad
- Identificar, analizar y mitigar riesgos en proyectos de seguridad, garantizando el cumplimiento de normativas y la gestión efectiva de auditorías

Módulo 4. Ataques a redes y sistemas Windows

- Comprender los fundamentos de Windows y directorio activo, incluyendo su historia, arquitectura y funciones clave en la gestión de redes
- Aplicar técnicas de autenticación y autorización en directorio activo, con énfasis en el manejo de credenciales y la seguridad de los procesos de autenticación
- Desarrollar habilidades avanzadas en Kerberos, desde su funcionamiento básico hasta la identificación de ataques comunes y sus mitigaciones
- Implementar estrategias de auditoría en directorio activo, utilizando herramientas de diagnóstico para detectar anomalías y responder de manera eficaz a incidentes de seguridad

Módulo 5. *Hacking* web avanzado

- Investigar el funcionamiento de las peticiones web y cómo visualizar detalles con *Burp Suite* para identificar posibles vulnerabilidades
- Profundizar en los tipos de ataques *Cross Site Scripting* (XSS) y su explotación, incluyendo técnicas avanzadas como XSLeaks
- Examinar los riesgos de inyecciones a bases de datos, abarcando SQLi, Blind SQLi y NoSQLi, para obtener acceso no autorizado a la información
- Evaluar las vulnerabilidades asociadas a la carga de archivos, como *Remote Code Execution* (RCE) y XSS en subidas de ficheros, y sus posibles impactos en la seguridad

Módulo 6. Arquitectura y seguridad en redes

- Analizar los conceptos clave de redes LAN, WAN y el modelo OSI/TCP - IP
- Configurar VLANs y aplicar medidas para mitigar ataques a capa 2
- Gestionar el direccionamiento IP y realizar enrutamiento estático y dinámico
- Implementar medidas de seguridad en redes, incluyendo *firewalls* y *Zero Trust Network Access*

Módulo 7. Análisis y desarrollo de *malware*

- Investigar la evolución y clasificación de los diferentes tipos de *malware*
- Configurar y utilizar herramientas para el análisis y desarrollo de *malware*
- Aplicar técnicas intermedias de *malware*, como la manipulación de claves del registro y el uso de salvapantallas
- Realizar análisis dinámico y estático de *malware* utilizando herramientas como *Process Hacker* y Ghidra

Módulo 8. Fundamentos forenses y DFIR

- Aplicar la cadena de custodia y los procesos de adquisición de evidencia digital en investigaciones forenses
- Realizar análisis forenses en sistemas operativos Windows, Linux y macOS
- Utilizar herramientas de análisis de disco y recuperar datos de medios dañados
- Responder a incidentes de seguridad mediante la creación de un plan y coordinación con equipos de seguridad

Módulo 9. Ejercicios de *Red Team* avanzados

- Realizar la enumeración avanzada de subdominios y aplicar técnicas de Google Dorking
- Ejecutar campañas de *phishing* avanzadas, incluyendo el uso de *Reverse Proxy Phishing* y 2FA *Bypass* con *Evilginx*
- Utilizar técnicas avanzadas de persistencia como *Golden Tickets* y *Silver Tickets*
- Aplicar técnicas avanzadas de evasión, como el *Bypass* de AMSI y la ofuscación de *PowerShell*

Módulo 10. Reporte técnico y ejecutivo

- Desarrollar la estructura de un reporte técnico y ejecutivo, diferenciando los enfoques según el público
- Aplicar las metodologías OSSTMM y LINCE en el proceso de evaluación y elaboración de informes
- Identificar y evitar errores comunes al reportar vulnerabilidades, y cuantificar el alcance de los hallazgos
- Ajustar el informe ejecutivo al contexto del cliente, destacando soluciones, mitigaciones y ejemplos prácticos

05

Salidas profesionales

Las oportunidades profesionales que brindará esta titulación universitaria son amplias y desafiantes. Gracias a las herramientas adquiridas, los profesionales estarán capacitados para asumir roles fundamentales en el ámbito de la ciberseguridad, específicamente en *Pentesting* y *Red Team*. De hecho, podrán desempeñarse en empresas de tecnología, agencias o consultoras de seguridad, liderando equipos encargados de identificar y mitigar amenazas. Con un enfoque en técnicas avanzadas, estarán preparados para enfrentar los retos más exigentes en la protección de infraestructuras digitales, convirtiéndose en actores clave en la defensa contra ciberataques.

¿Buscas desempeñarte como Red Team Operator? Lógralo mediante esta completísima titulación universitaria"

Perfil del egresado

El egresado estará preparado para enfrentar los retos de un entorno digital en constante evolución. Con una sólida base en ciberseguridad avanzada, dominará técnicas de evasión, análisis forense y metodologías de ataque en profundidad. Además, tendrá habilidades estratégicas para gestionar incidentes de seguridad, diseñar planes de contingencia y liderar equipos de respuesta ante emergencias cibernéticas. También, destacará por su aptitud en la implementación de medidas proactivas de protección, contribuyendo a la resiliencia digital de las organizaciones. Como resultado, su capacidad de adaptación y liderazgo será clave para anticiparse a amenazas emergentes y garantizar sistemas seguros.

> *Forjarás la resiliencia digital de organizaciones frente a los retos de un entorno en constante evolución, aplicando una sólida base en ciberseguridad.*

- **Pensamiento analítico:** Competencia para descomponer problemas complejos en componentes más pequeños para entender cómo funcionan
- **Gestión de riesgos:** Destreza que permite identificar, evaluar y priorizar riesgos, y desarrollar estrategias efectivas para mitigarlos
- **Habilidad para trabajar bajo presión:** Aptitud de enfrentar situaciones de alta presión, como la respuesta a incidentes de seguridad. Esta habilidad les permite tomar decisiones rápidas y precisas en situaciones críticas
- **Conocimiento de herramientas y técnicas de hacking ético:** Habilidad para dominar herramienta de penetración para identificar y corregir vulnerabilidades en sistemas informáticos

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

1. ***Tester* de Penetración:** Encargado de evaluar la seguridad de sistemas simulando ataques para identificar vulnerabilidades y ayudar a mejorar la protección.
2. ***Red Team Leader*:** Ejecuta simulaciones de ataques cibernéticos, coordinando un equipo que replica las tácticas de atacantes para evaluar la seguridad organizacional.
3. **Analista de Vulnerabilidades:** Se centra en identificar y clasificar vulnerabilidades en sistemas para ayudar a prevenir posibles explotaciones.
4. **Ingeniero de Seguridad:** Dedicado al diseño e implementación de estrategias para proteger redes y sistemas contra amenazas cibernéticas.
5. **Consultor en Ciberseguridad:** Asesora a organizaciones sobre cómo mejorar su seguridad digital a través de auditorías y recomendaciones.
6. **Analista de Incidentes de Seguridad:** Focalizado en investigar y responder a incidentes de seguridad, tomando acciones para mitigar el impacto de las amenazas.
7. **Especialista en Forense Digital:** Su labor consiste en la recopilación de evidencia digital para investigar delitos cibernéticos y apoyar en procesos legales.
8. **Arquitecto de Seguridad Cibernética:** Encargado de implementar soluciones de seguridad para proteger la infraestructura tecnológica de una organización.
9. **Administrador de Sistemas de Seguridad:** gestor de herramientas de seguridad para garantizar su correcto funcionamiento y protección.
10. ***Chief Information Security Officer*:** Centrado en supervisar la seguridad de la información en una organización, estableciendo políticas y estrategias de protección.

06

Licencias de software incluidas

TECH es referencia en el mundo universitario por combinar la última tecnología con las metodologías docentes para potenciar el proceso de enseñanza-aprendizaje. Para ello, ha establecido una red de alianzas que le permite tener acceso a las herramientas de software más avanzadas del mundo profesional.

Al matricularte recibirás, de forma completamente gratuita, las credenciales de uso académico de las siguientes aplicaciones de software profesional”

TECH ha establecido una red de alianzas profesionales en la que se encuentran los principales proveedores de software aplicado a las diferentes áreas profesionales. Estas alianzas permiten a TECH tener acceso al uso de centenares de aplicaciones informáticas y licencias de software para acercarlas a sus estudiantes.

Las licencias de software para uso académico permitirán a los estudiantes utilizar las aplicaciones informáticas más avanzadas en su área profesional, de modo que podrán conocerlas y aprender su dominio sin tener que incurrir en costes. TECH se hará cargo del procedimiento de contratación para que los alumnos puedan utilizarlas de modo ilimitado durante el tiempo que estén estudiando el programa de Máster de Formación Permanente en Pentesting y Red Team, y además lo podrán hacer de forma completamente gratuita.

TECH te dará acceso gratuito al uso de las siguientes aplicaciones de software:

Google Career Launchpad

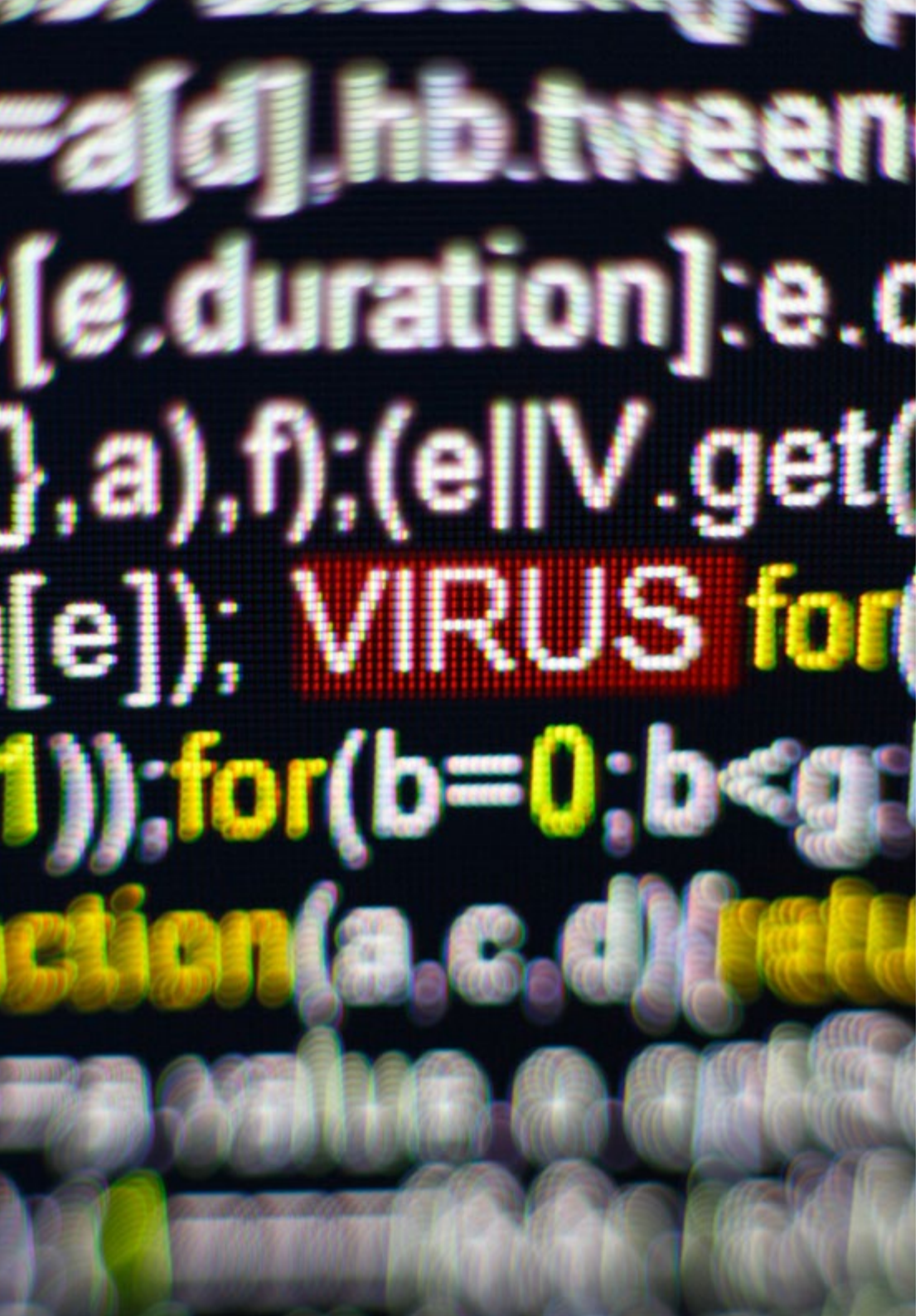
Google Career Launchpad es una solución para desarrollar habilidades digitales en tecnología y análisis de datos. Con un valor estimado de **5.000 dólares**, se incluye de forma **gratuita** en el programa universitario de TECH, brindando acceso a laboratorios interactivos y certificaciones reconocidas en el sector.

Esta plataforma combina capacitación técnica con casos prácticos, usando tecnologías como BigQuery y Google AI. Ofrece entornos simulados para experimentar con datos reales, junto a una red de expertos para orientación personalizada.

Funcionalidades destacadas:

- **Cursos especializados:** contenido actualizado en cloud computing, machine learning y análisis de datos
- **Laboratorios en vivo:** prácticas con herramientas reales de Google Cloud sin configuración adicional
- **Certificaciones integradas:** preparación para exámenes oficiales con validez internacional
- **Mentorías profesionales:** sesiones con expertos de Google y partners tecnológicos
- **Proyectos colaborativos: retos basados en problemas reales de empresas líderes**

En conclusión, **Google Career Launchpad** conecta a los usuarios con las últimas tecnologías del mercado, facilitando su inserción en áreas como inteligencia artificial y ciencia de datos con credenciales respaldadas por la industria.



Gracias a TECH podrás utilizar gratuitamente las mejores aplicaciones de software de tu área profesional”

07

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.

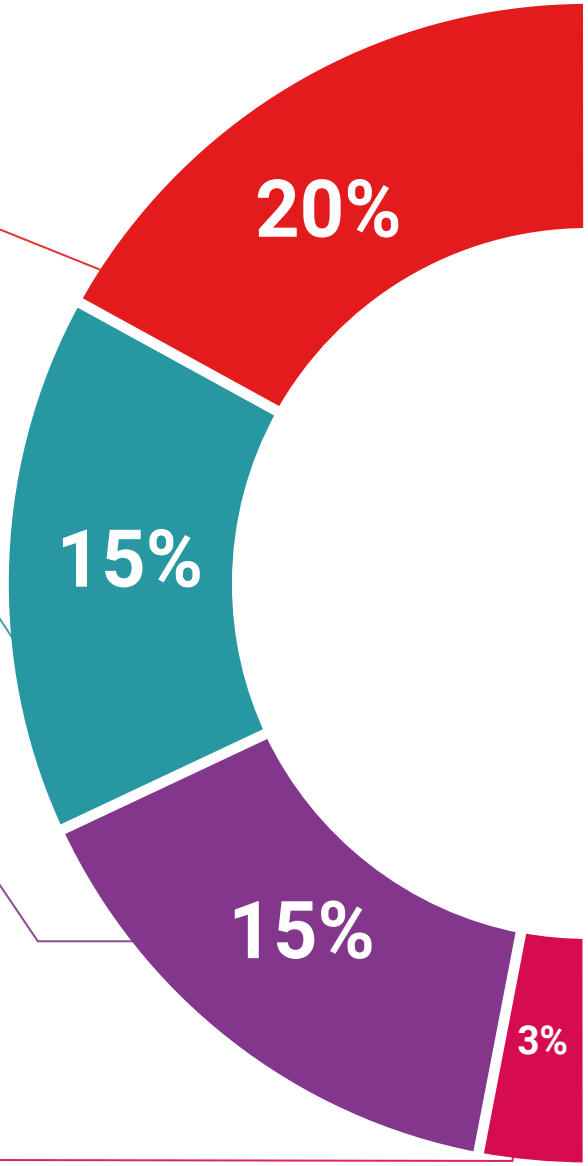
Resúmenes interactivos

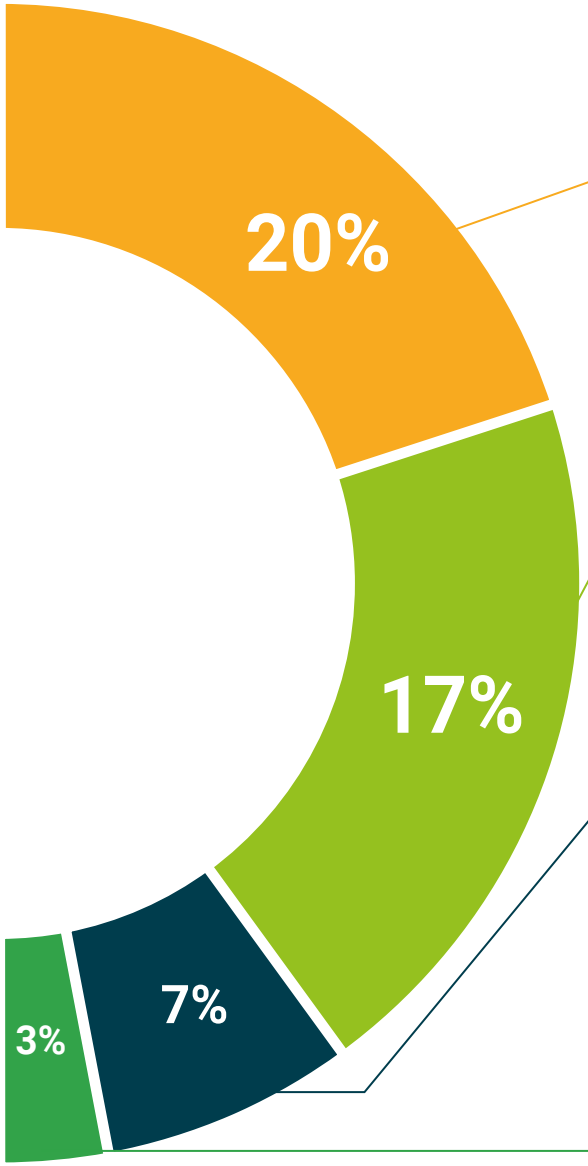
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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.

08

Cuadro docente

Para el diseño de este Máster de Formación Permanente en Pentesting y Red Team, TECH ha reunido a los mejores especialistas, que cuentan con un extenso y reconocido bagaje profesional en empresas líderes del sector. En este sentido, cada miembro del claustro docente aportará su experiencia práctica y sus conocimientos especializados, garantizando que los alumnos se beneficiarán de la enseñanza de profesionales altamente cualificados. Asimismo, la selección cuidadosa de estos expertos no solo asegurará la calidad académica, sino también la relevancia y aplicabilidad inmediata de los contenidos en el entorno dinámico de la ciberseguridad.

El equipo docente, especializado en Pentesting y Red Team, ha diseñado horas de contenido de alto nivel para que amplíes cada apartado del temario de manera personalizada"

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. 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

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

09

Titulación

Este programa en Pentesting y Red Team garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Máster de Formación Permanente expedido por TECH Universidad.

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

Este programa te permitirá obtener el título de **Máster de Formación Permanente en Pentesting y Red Team** emitido por TECH Universidad.

TECH es una Universidad española oficial, que forma parte del Espacio Europeo de Educación Superior (EEES). Con un enfoque centrado en la excelencia académica y la calidad universitaria a través de la tecnología.

Este título propio contribuye de forma relevante al desarrollo de la educación continua y actualización del profesional, garantizándole la adquisición de las competencias en su área de conocimiento y aportándole un alto valor curricular universitario a su formación. Es 100% válido en todas las Oposiciones, Carrera Profesional y Bolsas de Trabajo de cualquier Comunidad Autónoma española.

Además, el riguroso sistema de garantía de calidad de TECH asegura que cada título otorgado cumpla con los más altos estándares académicos, brindándole al egresado la confianza y la credibilidad que necesita para destacarse en su carrera profesional.

Título: **Máster de Formación Permanente en Pentesting y Red Team**

Modalidad: **online**

Duración: **7 meses**

Acreditación: **60 ECTS**

tech universidad

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

Máster de Formación Permanente en Pentesting y Red Team

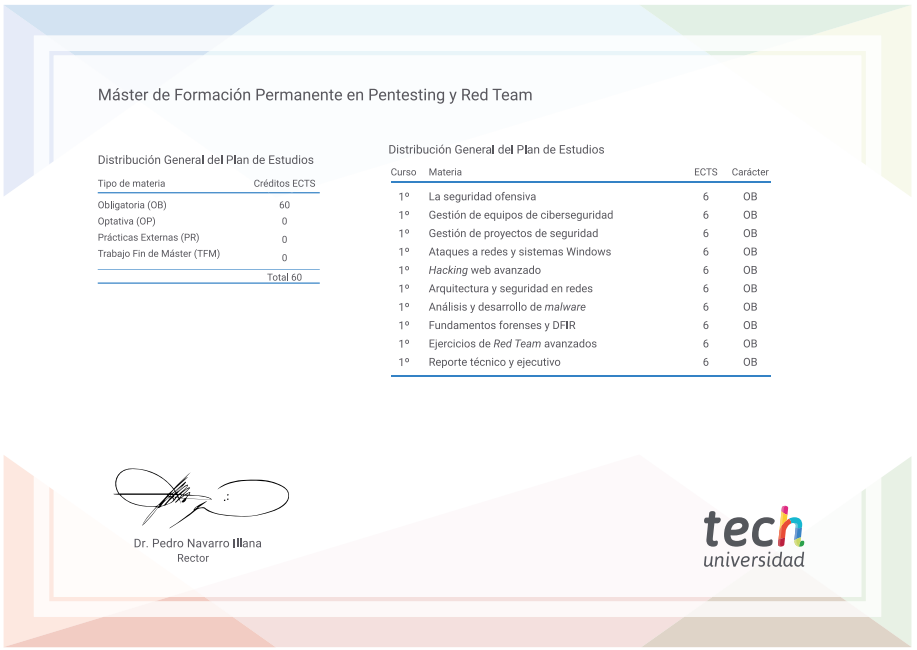
Se trata de un título propio de 1.500 horas de duración equivalente a 60 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH es una universidad Oficial Española legalmente reconocida mediante la Ley 1/2024, del 16 de abril, de la Comunidad Autónoma de Canarias, publicada en el Boletín Oficial del Estado (BOE) núm. 181, de 27 de julio de 2024 (pág. 96.369) e integrada en el Registro de Universidades, Centros y Títulos (RUCT) del Ministerio de Ciencia, Innovación y Universidades con el código 104.

En San Cristóbal de la Laguna, a 28 de febrero de 2024

Dr. Pedro Navarro Illana
Rector

código único TECH: AFWOR23S techtitute.com/titulos



Máster de Formación Permanente 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	La 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 *Red Team* avanzados	6	OB
1º	Reporte técnico y ejecutivo	6	OB

Dr. Pedro Navarro Illana
Rector

tech universidad

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

tech universidad

Máster de Formación Permanente

Pentesting y Red Team

- Modalidad: **online**
- Duración: **7 meses**
- Titulación: **TECH Universidad**
- Acreditación: **60 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Máster de Formación Permanente

Pentesting y Red Team

tech universidad