Máster de Formación Permanente

Pentesting y Red Team

MPRT

tech universidad tecnológica

tech universidad tecnológica

Máster de Formación Permanente

Pentesting y Red Team

- Modalidad: **online**
- Duración: **7 meses**
- Titulación: **TECH Universidad Tecnológica**
- Acreditación: **60 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**
- Dirigido a: **Graduados, Diplomados y Licenciados universitarios que hayan realizado previamente cualquiera de las titulaciones del campo de las Ciencias Sociales y Jurídicas, Administrativas y Empresariales**

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

Índice

01

Bienvenida

En la actualidad, los ataques cibernéticos han tomado un protagonismo y una fuerza considerables, preocupando a la población y a las propias compañías. De esta manera, las empresas han sufrido estas amenazas de manera exponencial, teniendo que instaurar la protección máxima de las bases de datos y la información sensible de sus clientes. Así, este sector se encuentra en búsqueda constante de expertos altamente cualificados en ciberseguridad, por lo que TECH ha diseñado este programa académico, contando con recursos tecnológicos y otras novedades en torno a las tácticas, técnicas y procedimientos utilizados por actores malintencionados. Todo ello, mediante la metodología *Relearning* y una completísima plataforma 100% online, la cual ofrece flexibilidad y comodidad horaria.

Máster de Formación Permanente en Pentesting y Red Team
TECH Universidad Tecnológica

Gracias a este programa 100% online, te especializarás en promover prácticas éticas y legales en la ejecución de ataques y pruebas en sistemas Windows"

02

¿Por qué estudiar en TECH?

TECH es la mayor escuela de negocio 100% online del mundo. Se trata de una Escuela de Negocios de élite, con un modelo de máxima exigencia académica. Un centro de alto rendimiento internacional y de entrenamiento intensivo en habilidades directivas.

TECH es una universidad de vanguardia tecnológica, que pone todos sus recursos al alcance del alumno para ayudarlo a alcanzar el éxito empresarial"

En TECH Universidad Tecnológica

Innovación

La universidad ofrece un modelo de aprendizaje en línea que combina la última tecnología educativa con el máximo rigor pedagógico. Un método único con el mayor reconocimiento internacional que aportará las claves para que el alumno pueda desarrollarse en un mundo en constante cambio, donde la innovación debe ser la apuesta esencial de todo empresario.

"Caso de Éxito Microsoft Europa" por incorporar en los programas un novedoso sistema de multivídeo interactivo.

Máxima exigencia

El criterio de admisión de TECH no es económico. No se necesita realizar una gran inversión para estudiar en esta universidad. Eso sí, para titularse en TECH, se podrán a prueba los límites de inteligencia y capacidad del alumno. El listón académico de esta institución es muy alto...

95% | **de los alumnos de TECH finaliza sus estudios con éxito**

Networking

En TECH participan profesionales de todos los países del mundo, de tal manera que el alumno podrá crear una gran red de contactos útil para su futuro.

+100.000
directivos capacitados cada año

+200
nacionalidades distintas

Empowerment

El alumno crecerá de la mano de las mejores empresas y de profesionales de gran prestigio e influencia. TECH ha desarrollado alianzas estratégicas y una valiosa red de contactos con los principales actores económicos de los 7 continentes.

+500 | **acuerdos de colaboración con las mejores empresas**

Talento

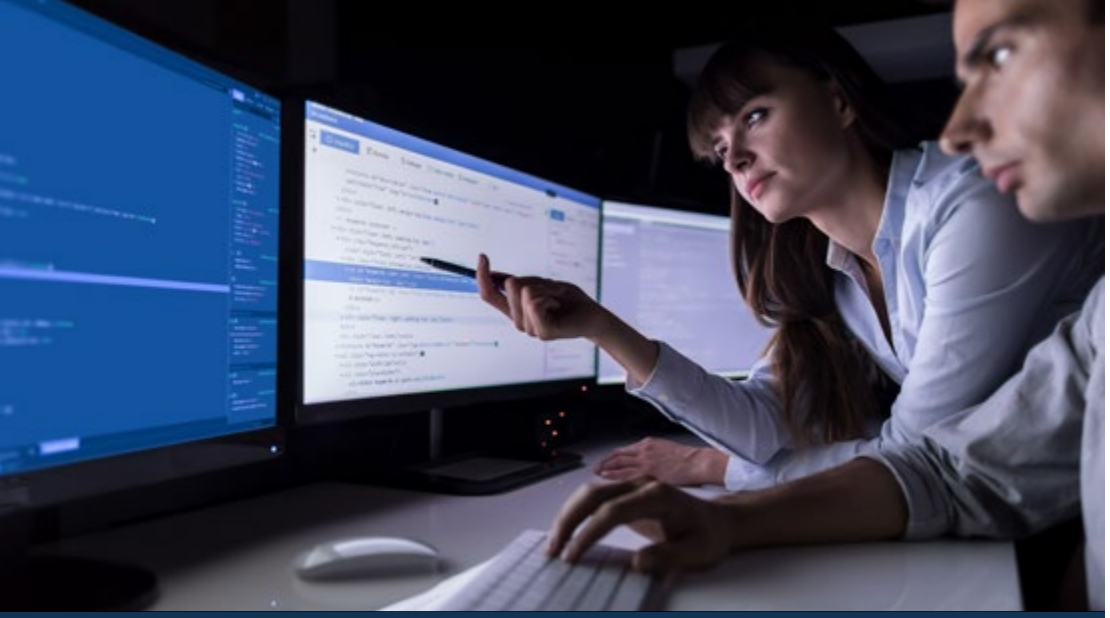
Este programa es una propuesta única para sacar a la luz el talento del estudiante en el ámbito empresarial. Una oportunidad con la que podrá dar a conocer sus inquietudes y su visión de negocio.

TECH ayuda al alumno a enseñar al mundo su talento al finalizar este programa.

Contexto Multicultural

Estudiando en TECH el alumno podrá disfrutar de una experiencia única. Estudiará en un contexto multicultural. En un programa con visión global, gracias al cual podrá conocer la forma de trabajar en diferentes lugares del mundo, recopilando la información más novedosa y que mejor se adapta a su idea de negocio.

Los alumnos de TECH provienen de más de 200 nacionalidades.



Aprende con los mejores

El equipo docente de TECH explica en las aulas lo que le ha llevado al éxito en sus empresas, trabajando desde un contexto real, vivo y dinámico. Docentes que se implican al máximo para ofrecer una especialización de calidad que permita al alumno avanzar en su carrera y lograr destacar en el ámbito empresarial.

Profesores de 20 nacionalidades diferentes.

En TECH tendrás acceso a los análisis de casos más rigurosos y actualizados del panorama académico"

TECH busca la excelencia y, para ello, cuenta con una serie de características que hacen de esta una universidad única:

Análisis

En TECH se explora el lado crítico del alumno, su capacidad de cuestionarse las cosas, sus competencias en resolución de problemas y sus habilidades interpersonales.

Excelencia académica

En TECH se pone al alcance del alumno la mejor metodología de aprendizaje online. La universidad combina el método *Relearning* (metodología de aprendizaje de posgrado con mejor valoración internacional) con el Estudio de Caso. Tradición y vanguardia en un difícil equilibrio, y en el contexto del más exigente itinerario académico.

Economía de escala

TECH es la universidad online más grande del mundo. Tiene un portfolio de más de 10.000 posgrados universitarios. Y en la nueva economía, **volumen + tecnología = precio disruptivo**. De esta manera, se asegura de que estudiar no resulte tan costoso como en otra universidad.

03

¿Por qué nuestro programa?

Realizar el programa de TECH supone multiplicar las posibilidades de alcanzar el éxito profesional en el ámbito de la alta dirección empresarial.

Es todo un reto que implica esfuerzo y dedicación, pero que abre las puertas a un futuro prometedor. El alumno aprenderá de la mano del mejor equipo docente y con la metodología educativa más flexible y novedosa.

Contamos con el más prestigioso cuadro docente y el temario más completo del mercado, lo que nos permite ofrecerte una capacitación de alto nivel académico”

Este programa aportará multitud de ventajas laborales y personales, entre ellas las siguientes:

01

Dar un impulso definitivo a la carrera del alumno

Estudiando en TECH el alumno podrá tomar las riendas de su futuro y desarrollar todo su potencial. Con la realización de este programa adquirirá las competencias necesarias para lograr un cambio positivo en su carrera en poco tiempo.

El 70% de los participantes de esta especialización logra un cambio positivo en su carrera en menos de 2 años.

02

Desarrollar una visión estratégica y global de la empresa

TECH ofrece una profunda visión de dirección general para entender cómo afecta cada decisión a las distintas áreas funcionales de la empresa.

Nuestra visión global de la empresa mejorará tu visión estratégica.

03

Consolidar al alumno en la alta gestión empresarial

Estudiar en TECH supone abrir las puertas de hacia panorama profesional de gran envergadura para que el alumno se posicione como directivo de alto nivel, con una amplia visión del entorno internacional.

Trabajarás más de 100 casos reales de alta dirección.

04

Asumir nuevas responsabilidades

Durante el programa se muestran las últimas tendencias, avances y estrategias, para que el alumno pueda llevar a cabo su labor profesional en un entorno cambiante.

El 45% de los alumnos consigue ascender en su puesto de trabajo por promoción interna.

05

Acceso a una potente red de contactos

TECH interrelaciona a sus alumnos para maximizar las oportunidades. Estudiantes con las mismas inquietudes y ganas de crecer. Así, se podrán compartir socios, clientes o proveedores.

Encontrarás una red de contactos imprescindible para tu desarrollo profesional.

06

Desarrollar proyectos de empresa de una forma rigurosa

El alumno obtendrá una profunda visión estratégica que le ayudará a desarrollar su propio proyecto, teniendo en cuenta las diferentes áreas de la empresa.

El 20% de nuestros alumnos desarrolla su propia idea de negocio.

07

Mejorar *soft skills* y habilidades directivas

TECH ayuda al estudiante a aplicar y desarrollar los conocimientos adquiridos y mejorar en sus habilidades interpersonales para ser un líder que marque la diferencia.

Mejora tus habilidades de comunicación y liderazgo y da un impulso a tu profesión.

08

Formar parte de una comunidad exclusiva

El alumno formará parte de una comunidad de directivos de élite, grandes empresas, instituciones de renombre y profesores cualificados procedentes de las universidades más prestigiosas del mundo: la comunidad TECH Universidad Tecnológica.

Te damos la oportunidad de especializarte con un equipo de profesores de reputación internacional.

04

Objetivos

Esta titulación universitaria le facilitará al alumnado innovadoras actualizaciones referentes a las normativas y el cumplimiento en proyectos de ciberseguridad en el área del *Pentesting*, aportando más valor a su carrera profesional. En este sentido, TECH proporcionará recursos didácticos durante todo el desarrollo del programa, potenciando competencias relacionadas con la detección de anomalías y los comportamientos sospechosos. De esta manera, al finalizar este programa, el egresado habrá ampliado sus conocimientos sobre *Pentesting y Red Team*. Todo esto, a lo largo de 7 meses de capacitación online.

Tras este Máster de Formación Permanente, te pondrás al día en la utilidad de la Investigación Forense Digital (DFIR) para resolver delitos cibernéticos"

TECH hace suyos los objetivos de sus alumnos
Trabajan conjuntamente para conseguirlos

El **Máster de Formación Permanente en Pentesting y Red Team** capacitará al alumno para:

01 Estudiar y comprender las tácticas, técnicas y procedimientos utilizados por los actores malintencionados, permitiendo la identificación y simulación de amenazas

02 Aplicar conocimientos teóricos en escenarios prácticos y simulaciones, enfrentándose a desafíos reales para fortalecer habilidades de *Pentesting*

03 Aprender a asignar eficientemente recursos dentro de un equipo de ciberseguridad, considerando las habilidades individuales y maximizando la productividad en proyectos

04 Mejorar habilidades de comunicación específicas para entornos técnicos, facilitando la comprensión y coordinación entre los miembros del equipo

05 Aprender técnicas de seguimiento y control de proyectos, identificando desviaciones y tomando acciones correctivas según sea necesario

06 Desarrollar competencias para evaluar y mejorar las configuraciones de seguridad en sistemas Windows, asegurando la implementación de medidas eficaces

07 Promover prácticas éticas y legales en la ejecución de ataques y pruebas en sistemas Windows, considerando los principios éticos de la ciberseguridad

08 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

09 Fomentar la colaboración efectiva con equipos de seguridad, integrando estrategias y esfuerzos para proteger la infraestructura de red

10 Promover prácticas éticas y legales en el análisis y desarrollo de malware, garantizando la integridad y responsabilidad en todas las actividades

11 Aplicar conocimientos teóricos en entornos simulados, participar en ejercicios prácticos para entender y contrarrestar ataques maliciosos

12 Adquirir conocimientos sólidos sobre los principios fundamentales de la Investigación Forense Digital (DFIR) y su aplicación en la resolución de incidentes cibernéticos

13 Aprender a elaborar informes detallados que documenten los hallazgos, metodologías utilizadas y recomendaciones derivadas de ejercicios de *Red Team* avanzados

14 Desarrollar habilidades para formular recomendaciones accionables y prácticas, orientadas a mitigar vulnerabilidades y mejorar la postura de seguridad

15 Familiarizar al alumno con las mejores prácticas para la presentación ejecutiva de informes, adaptando la información técnica para audiencias no técnicas

05

Competencias

Esta propuesta académica le proporcionará al egresado una visión actual sobre el *Pentesting*. Esto le dará la oportunidad de aumentar sus habilidades, asumiendo roles de dirección, enfrentando situaciones desafiantes y cambiantes, e incluso trabajando de la mano y de forma efectiva con otras compañías del sector informático. De esta forma, el profesional tendrá a su disposición múltiples herramientas, como infografías y vídeos, las cuales presentarán una perspectiva más práctica en este campo de estudio.

Potencia tus destrezas para la detección y prevención efectiva de malware, solucionando las situaciones más desafiantes en el sector informático"

01 Adquirir habilidades de *coaching* para el desarrollo profesional de los miembros del equipo, fomentando el crecimiento y la mejora

02 Desarrollar habilidades para la toma de decisiones estratégicas en situaciones de ciberseguridad, considerando el impacto a corto y largo plazo en la seguridad organizacional

03 Adquirir competencias en la identificación, evaluación y mitigación de riesgos específicos de proyectos de seguridad cibernética

04 Desarrollar habilidades para implementar medidas de defensa activa, fortaleciendo la seguridad de sistemas y redes basadas

05 Aprender técnicas de análisis de tráfico web para identificar patrones y comportamientos anómalos, facilitando la detección de posibles amenazas

06 Adquirir competencias en el análisis forense aplicado a entornos de red, permitiendo la identificación y respuesta efectiva a incidentes cibernéticos

07 Aprender estrategias para la detección y prevención efectiva de malware, incluyendo el despliegue de soluciones de seguridad avanzadas

08 Desarrollar habilidades en la identificación de indicadores de compromiso (IoC) durante la investigación forense, facilitando la detección y respuesta a incidentes

09 Adquirir habilidades para la planificación estratégica de ejercicios de *Red Team*, considerando objetivos, alcance, recursos y escenarios realistas

10 Adquirir competencias en la identificación y priorización de vulnerabilidades, destacando aquellas que representan mayores riesgos para la seguridad

06

Estructura y contenido

El programa en Pentesting y Red Team es un programa enfocado esencialmente en que el egresado adquiera las competencias relacionadas con la informática forense en la ciberseguridad. De esa manera, esta titulación académica está encaminada hacia una estructura teórica-práctica, acompañada de la amplia experiencia y el gran bagaje de un equipo de expertos altamente especializado.

Sin horarios predefinidos ni evaluaciones continuas: así TECH te garantiza el acceso más rápido y flexible a sus contenidos académicos"

Plan de estudios

Esta titulación universitaria consta de un aprendizaje continuo, mediante una enseñanza de los más altos estándares, gracias a la cual el egresado conseguirá los mejores puestos en el sector informático y empresarial. De este modo, el alumnado sobrepasará los diversos obstáculos que impone el entorno laboral. Esta titulación facilitará múltiples habilidades que abordan técnicas avanzadas en Kerberos, mitigaciones y protecciones.

Por otro lado, el equipo docente ha desarrollado un exclusivo temario, que incorpora 10 módulos, con el propósito de que el estudiante adquiera competencias fundamentales referentes a la evaluación de la seguridad en APIs y servicios web, identificando posibles puntos de vulnerabilidad.

Asimismo, el profesional ahondará en las recomendaciones accionables y prácticas, orientadas a mitigar vulnerabilidades y mejorar la postura de seguridad. En ese sentido, se convertirán en importantes especialistas en materia de métodos de medición y prevención de conflictos.

Para este programa académico, los empresarios se apoyarán en la exclusiva metodología *Relearning*, a través de la cual podrán examinar conceptos complejos y asimilar su aplicación cotidiana de una manera fluida. A su vez, la titulación se impartirá desde una innovadora plataforma de aprendizaje 100% online, la cual no está sujeta a horarios fijos ni cronogramas evaluativos continuos.

Este Máster de Formación Permanente se desarrolla a lo largo de 7 meses y se divide en 10 módulos:

Módulo 1	La Seguridad Ofensiva
Módulo 2	Gestión de Equipos de Ciberseguridad
Módulo 3	Gestión de Proyectos de Seguridad
Módulo 4	Ataques a Redes y Sistemas Windows
Módulo 5	***Hacking Web*** Avanzado
Módulo 6	Arquitectura y Seguridad en Redes
Módulo 7	Análisis y Desarrollo de ***Malware***
Módulo 8	Fundamentos Forenses y DFIR
Módulo 9	Ejercicios de ***Red Team*** Avanzados
Módulo 10	Reporte Técnico y Ejecutivo

¿Dónde, cuándo y cómo se imparte?

TECH ofrece la posibilidad de desarrollar este Máster de Formación Permanente en Pentesting y Red Team de manera totalmente online. Durante los 7 meses que dura la especialización, el alumno podrá acceder a todos los contenidos de este programa en cualquier momento, lo que le permitirá autogestionar su tiempo de estudio.

Una experiencia educativa única, clave y decisiva para impulsar tu desarrollo profesional y dar el salto definitivo.

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 Acess 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

07

Metodología

Este programa de capacitación ofrece una forma diferente de aprender. Nuestra metodología se desarrolla a través de un modo de aprendizaje de forma cíclica: ***el Relearning***.

Este sistema de enseñanza es utilizado, por ejemplo, en las facultades de medicina más prestigiosas del mundo y se ha considerado uno de los más eficaces por publicaciones de gran relevancia como el ***New England Journal of Medicine.***

Descubre el Relearning, un sistema que abandona el aprendizaje lineal convencional para llevarte a través de sistemas cíclicos de enseñanza: una forma de aprender que ha demostrado su enorme eficacia, especialmente en las materias que requieren memorización"

TECH Business School emplea el Estudio de Caso para contextualizar todo el contenido

Nuestro programa ofrece un método revolucionario de desarrollo de habilidades y conocimientos. Nuestro objetivo es afianzar competencias en un contexto cambiante, competitivo y de alta exigencia.

Con TECH podrás experimentar una forma de aprender que está moviendo los cimientos de las universidades tradicionales de todo el mundo"

Este programa te prepara para afrontar retos empresariales en entornos inciertos y lograr el éxito de tu negocio.

Nuestro programa te prepara para afrontar nuevos retos en entornos inciertos y lograr el éxito en tu carrera.

Un método de aprendizaje innovador y diferente

El presente programa de TECH es una enseñanza intensiva, creada desde 0 para proponerle al directivo retos y decisiones empresariales de máximo nivel, ya sea en el ámbito nacional o internacional. Gracias a esta metodología se impulsa el crecimiento personal y profesional, dando un paso decisivo para conseguir el éxito. El método del caso, técnica que sienta las bases de este contenido, garantiza que se sigue la realidad económica, social y empresarial más vigente.

> *Aprenderás, mediante actividades colaborativas y casos reales, la resolución de situaciones complejas en entornos empresariales reales"*

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

Ante una determinada situación, ¿qué debería hacer un profesional? Esta es la pregunta a la que nos enfrentamos en el método del caso, un método de aprendizaje orientado a la acción. A lo largo del programa, los estudiantes se enfrentarán a múltiples casos reales. Deberán integrar todos sus conocimientos, investigar, argumentar y defender sus ideas y decisiones.

Relearning Methodology

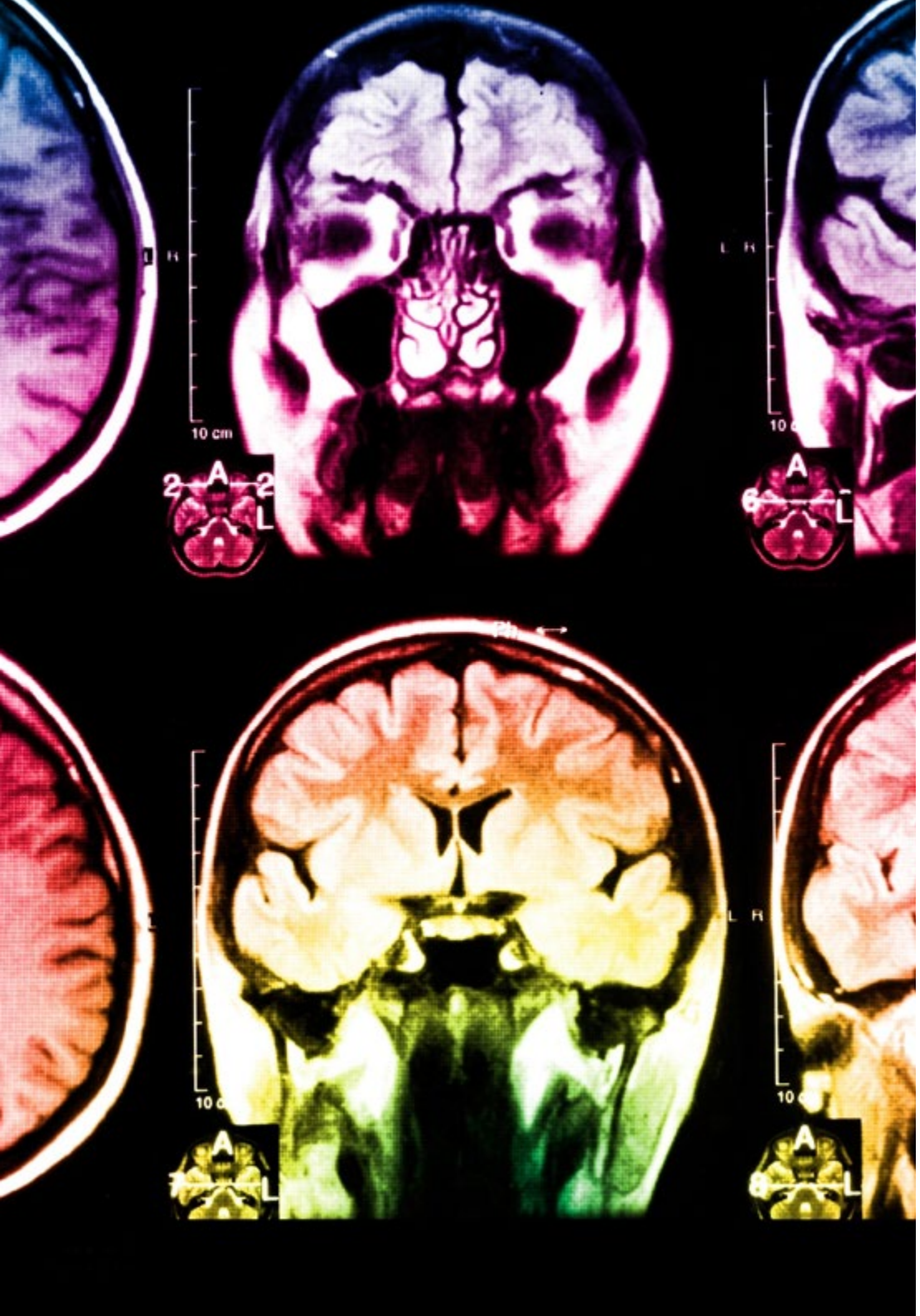
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el Relearning.

Nuestro sistema online te permitirá organizar tu tiempo y tu ritmo de aprendizaje, adaptándolo a tus horarios. Podrás acceder a los contenidos desde cualquier dispositivo fijo o móvil con conexión a internet.

En TECH aprenderás con una metodología vanguardista concebida para capacitar a los directivos del futuro. Este método, a la vanguardia pedagógica mundial, se denomina Relearning.

Nuestra escuela de negocios es la única en habla hispana licenciada para emplear este exitoso método. En 2019, conseguimos mejorar los niveles de satisfacción global de nuestros alumnos (calidad docente, calidad de los materiales, estructura del curso, objetivos…) con respecto a los indicadores de la mejor universidad online en español.



En nuestro programa, el aprendizaje no es un proceso lineal, sino que sucede en espiral (aprender, desaprender, olvidar y reaprender). Por eso, combinamos cada uno de estos elementos de forma concéntrica. Con esta metodología se han capacitadomás de 650.000 graduados universitarios con un éxito sin precedentes en ámbitos tan distintos como la bioquímica, la genética, la cirugía, el derecho internacional, las habilidades directivas, las ciencias del deporte, la filosofía, el derecho, la ingeniería, el periodismo, la historia o los mercados e instrumentos financieros. Todo ello en un entorno de alta exigencia, con un alumnado universitario de un perfil socioeconómico alto y una media de edad de 43,5 años.

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.

A partir de la última evidencia científica en el ámbito de la neurociencia, no solo sabemos organizar la información, las ideas, las imágenes y los recuerdos, sino que sabemos que el lugar y el contexto donde hemos aprendido algo es fundamental para que seamos capaces de recordarlo y almacenarlo en el hipocampo, para retenerlo en nuestra memoria a largo plazo.

De esta manera, y en lo que se denomina Neurocognitive context-dependent e-learning, los diferentes elementos de nuestro programa están conectados con el contexto donde el participante desarrolla su práctica profesional.

Este programa ofrece los mejores materiales educativos, preparados a conciencia para los profesionales:

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, para crear el método de trabajo online de TECH. Todo ello, con las técnicas más novedosas que ofrecen piezas de gran calidad en todos y cada uno los materiales que se ponen a disposición del alumno.

Clases magistrales

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

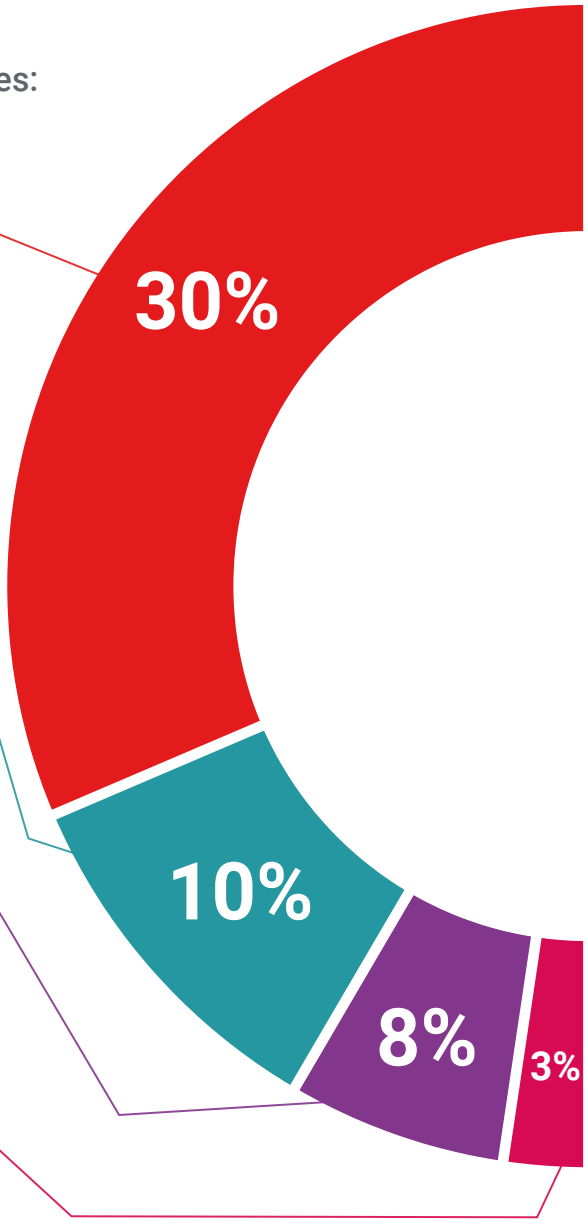
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

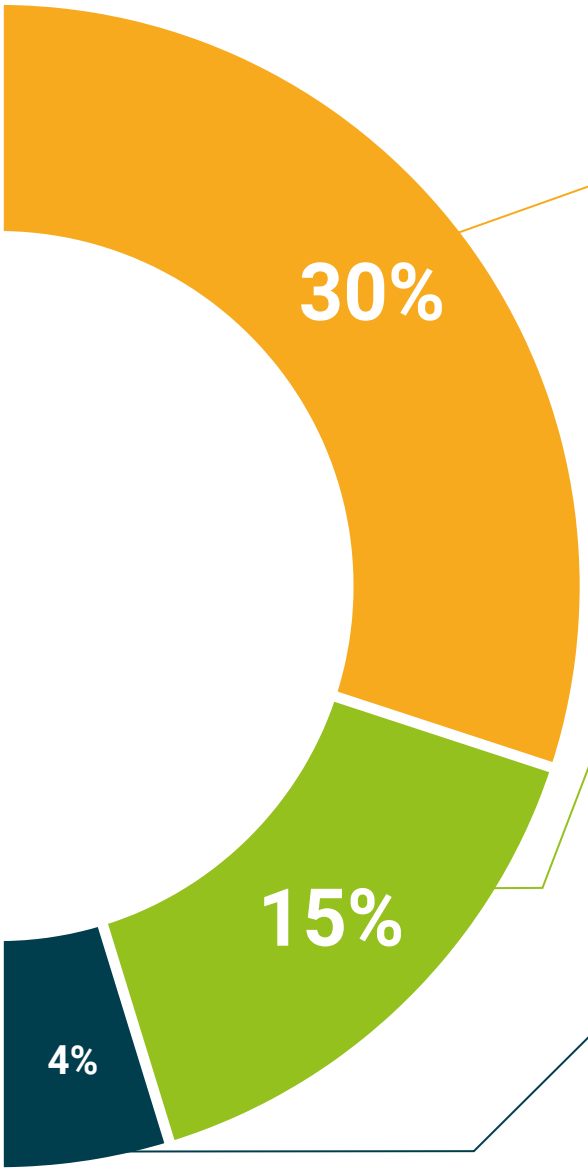
Prácticas de habilidades directivas

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

Lecturas complementarias

Artículos recientes, documentos de consenso y guías internacionales, entre otros. En la biblioteca virtual de TECH el estudiante tendrá acceso a todo lo que necesita para completar su capacitación.





Case studies

Completarán una selección de los mejores business cases que se emplean en Harvard Business School. Casos presentados, analizados y tutorizados por los mejores especialistas en alta dirección del panorama latinoamericano.

Resúmenes interactivos

El equipo de TECH presenta los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audios, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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

Testing & Retesting

Se evalúan y reevalúan periódicamente los conocimientos del alumno a lo largo del programa, mediante actividades y ejercicios evaluativos y autoevaluativos para que, de esta manera, el estudiante compruebe cómo va consiguiendo sus metas.

08

Perfil de nuestros alumnos

El programa está dirigido a Graduados, Diplomados y Licenciados universitarios que hayan realizado previamente cualquiera de las siguientes titulaciones en el campo de las Ciencias Sociales y Jurídicas, Administrativas y Económicas.

La diversidad de participantes con diferentes perfiles académicos y procedentes de múltiples nacionalidades conforma el enfoque multidisciplinar de este programa.

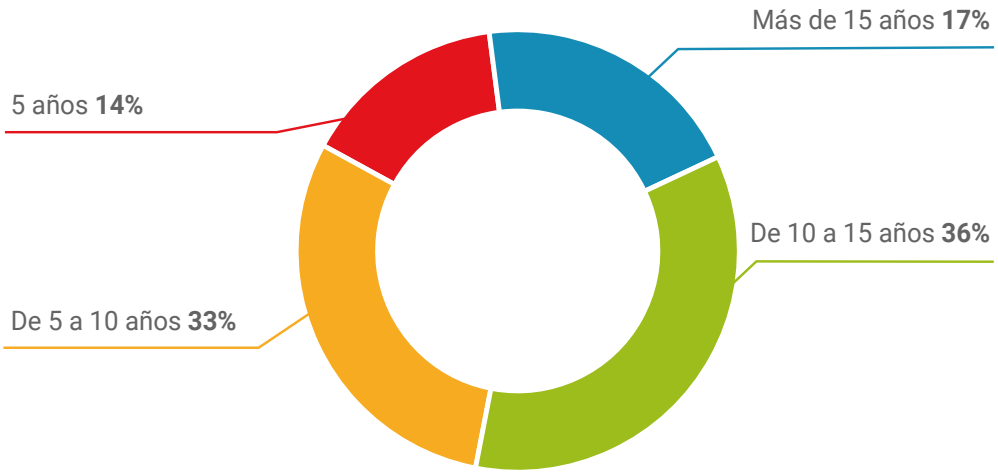
También podrán realizar el programa los profesionales que, siendo titulados universitarios en cualquier área, cuenten con una experiencia laboral de dos años en el campo de la informática.

Si tienes experiencia en Pentesting y Red Team, y buscas una interesante mejora en tu trayectoria mientras sigues trabajando, este es tu programa"

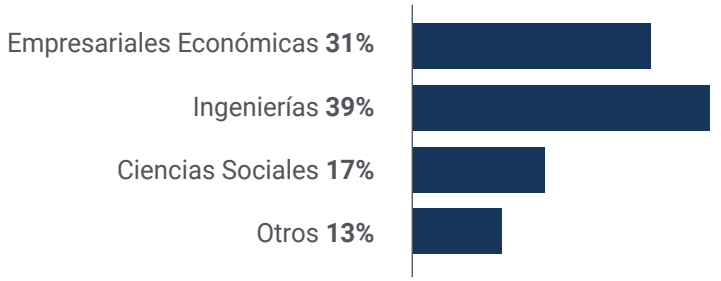
Edad media

Entre **35** y **45** años

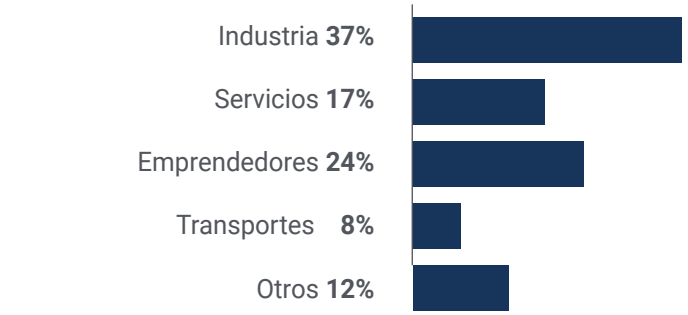
Años de experiencia



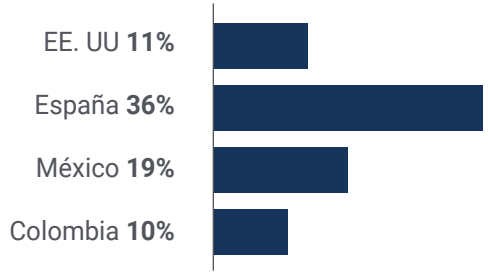
Formación



Perfil académico



Distribución geográfica



Salomón Galvis

Analista de seguridad de la información

"De esta titulación resalto que logré profundizar en la importancia de las evaluaciones regulares y lo esenciales para medir la seguridad cibernética. Una gran inversión que a futuro se verá reflejado, gracias a las herramientas clave que el equipo docente implanta en el desarrollo del programa"

09

Dirección del curso

Este Máster de Formación Permanente tiene a su disposición un equipo docente de gran reconocimiento internacional y con importantes conocimientos especializados en Software y Tecnologías de la Sociedad de la Información y Ciberseguridad en Integración Tecnológica Empresarial. Así, la educación de élite se ve reflejada en un enfoque dinámico e innovador del plan de estudios, implementando las más recientes tendencias en ciberseguridad. De este modo, se acoplan casos simulados y el análisis de situaciones reales para que el alumnado obtenga una praxis de primer nivel, permitiéndoles asumir los distintos retos profesionales en el ámbito laboral.

Grandes expertos en Pentesting y Red Team impartirán este innovador y riguroso programa”

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"

10

Impacto para tu carrera

Este programa universitario ha sido diseñado con la intención de orientar al egresado sobre los conocimientos que lo llevarán a afrontar cualquier situación en el campo de la ciberseguridad. De este modo, TECH se adentrará específicamente en la enseñanza de la más alta calidad, buscando eficiencia en cada una de sus titulaciones. Así, se le garantizará al profesional un aprendizaje especializado en *Pentesting* y *Red Team*.

Red Team y otros aspectos informáticos de ciberseguridad pueden integrarse al Pentesting a través de esta intensiva titulación"

Las técnicas avanzadas de pivoting son algunas de las habilidades que tendrás en tus manos tras este exhaustivo Máster de Formación Permanente de 7 meses de duración.

¿Estás preparado para dar el salto? Una excelente mejora profesional te espera

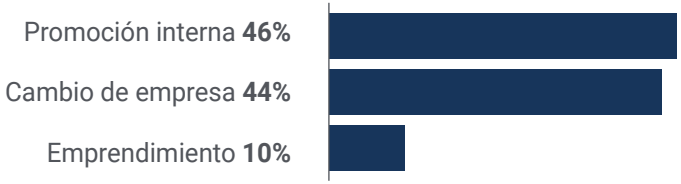
El Máster de Formación Permanente en Pentesting y Red Team de TECH es un programa intensivo que te prepara para afrontar retos y decisiones empresariales en el ámbito de la Informática. Su objetivo principal es favorecer tu crecimiento personal y profesional. Ayudarte a conseguir el éxito.

Si quieres superarte a ti mismo, conseguir un cambio positivo a nivel profesional y relacionarte con los mejores, este es tu sitio.

Aprovecha esta oportunidad rigurosa y exhaustiva de ampliar tus competencias en Pentesting por medio de TECH, la mejor universidad online del mundo según Forbes.

Momento del cambio

Tipo de cambio



Mejora salarial

La realización de este programa supone para nuestros alumnos un incremento salarial de más del **25,55%**

11

Beneficios para tu empresa

Este programa contribuye a elevar el talento de la organización a su máximo potencial mediante la instrucción de líderes de alto nivel.

Además, participar en esta opción universitaria supone una oportunidad única para acceder a una red de contactos potente en la que encontrar futuros socios profesionales, clientes o proveedores.

En la era digital, el directivo debe integrar nuevos procesos y estrategias que provoquen cambios significativos y desarrollo organizacional. Esto solo es posible a través de la capacitación y actualización universitaria"

Desarrollar y retener el talento en las empresas es la mejor inversión a largo plazo.

01

Crecimiento del talento y del capital intelectual

El profesional aportará a la empresa nuevos conceptos, estrategias y perspectivas que pueden provocar cambios relevantes en la organización.

02

Retención de directivos de alto potencial evitando la fuga de talentos

Este programa refuerza el vínculo de la empresa con el profesional y abre nuevas vías de crecimiento profesional dentro de la misma.

03

Construcción de agentes de cambio

Será capaz de tomar decisiones en momentos de incertidumbre y crisis, ayudando a la organización a superar los obstáculos.

04

Incremento de las posibilidades de expansión internacional

Gracias a este programa, la empresa entrará en contacto con los principales mercados de la economía mundial.

05

Desarrollo de proyectos propios

El profesional puede trabajar en un proyecto real o desarrollar nuevos proyectos en el ámbito de I + D o Desarrollo de Negocio de su compañía.

06

Aumento de la competitividad

Este programa dotará a sus profesionales de competencias para asumir los nuevos desafíos e impulsar así la organización.

12

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 Tecnológica.

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 Tecnológica.

TECH Universidad Tecnológica, 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: **100% Online**

Duración: **7 meses**

Créditos: **60 ECTS**


tech universidad tecnológica

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

Máster de Formación Permanente en Pentesting y Red Team

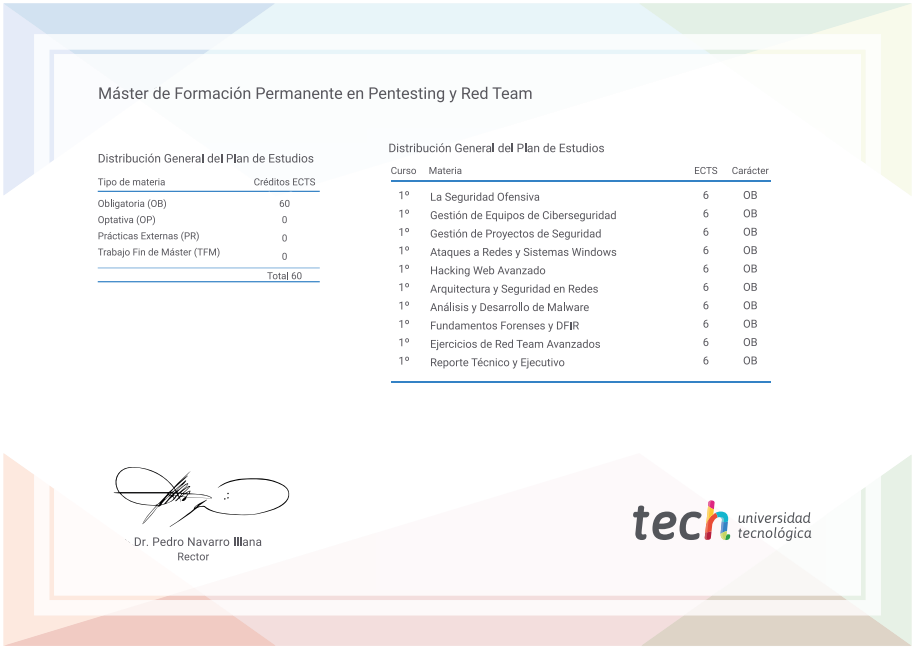
Se trata de un título propio de 1.500 horas de duración equivalente a 60 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH Universidad Tecnológica es una universidad oficial española que pertenece al Espacio Europeo de Educación Superior (EEES).

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 tecnológica

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

tech universidad tecnológica

Máster de Formación Permanente

Pentesting y Red Team

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

Máster de Formación Permanente

Pentesting y Red Team

tech universidad tecnológica