

# Curso Universitario

## Gestión de Equipos de pentesting



## Curso Universitario Gestión de Equipos de pentesting

- » Modalidad: **online**
- » Duración: **6 semanas**
- » Titulación: **TECH Global University**
- » Acreditación: **6 ECTS**
- » Horario: **a tu ritmo**
- » Exámenes: **online**

Acceso web: [www.techtitute.com/informatica/curso-universitario/gestion-equipos-pentesting](http://www.techtitute.com/informatica/curso-universitario/gestion-equipos-pentesting)

# Índice

01

Presentación

---

*pág. 4*

02

Objetivos

---

*pág. 8*

03

Dirección del curso

---

*pág. 12*

04

Estructura y contenido

---

*pág. 16*

05

Metodología

---

*pág. 20*

06

Titulación

---

*pág. 28*

# 01 Presentación

La gestión de equipos de pentesting es un aspecto fundamental para las instituciones. El motivo es que permite aprovechar al máximo los recursos humanos y tecnológicos disponibles, realizando pruebas de penetración. Así pues, las compañías demandan cada vez más la incorporación de expertos en ciberseguridad para la identificación y resolución de problemas de manera óptima. Ante el aumento del del *hacking* informático, estos profesionales deben actualizar sus conocimientos habitualmente y aplicar las herramientas más modernas con el fin de prevenir los ataques informáticos. Por esto, TECH lanza un innovador programa para que el alumnado implemente las tácticas más vanguardistas en *pentesting*. Además, este programa se basa en una modalidad 100% online, garantizando así la comodidad y flexibilidad del alumnado.



```
// Begin Actor overrides
virtual void PostInitializeComponents() override;
virtual void Tick(float DeltaSeconds) override;
virtual void ReceiveHit(class UPrimitiveComponent* Component, FVector ImpactLocation) override;
virtual void FellOutOfWorld(const class UDamageEvent* DamageEvent) override;
// End Actor overrides

// Begin Pawn overrides
virtual void SetupPlayerInputComponent(class UInputComponent* InputComponent) override;
virtual float TakeDamage(float Damage, struct FDamageEvent* DamageEvent, class AActor* Instigator, class UPrimitiveComponent* Component) override;
virtual void TurnOff() override;
// End Pawn overrides

/** Identifies if pawn is in its dying state.
UPROPERTY(VisibleAnywhere, BlueprintReadWrite)
uint32 bIsDying:1;

/** replicating death on server
UFUNCTION()
void OnRep_Dying() override;

/** Returns true if the pawn is in its dying state.
virtual bool IsDying() const override;
```

“

Cuenta con el arsenal más potente del auditor ofensivo a través de 150 horas de la mejor enseñanza digital”

Gracias a las auditorías realizadas por expertos en gestión de equipos, las entidades son conscientes de sus posibles obstáculos, riesgos y problemas antes de que sea demasiado tarde. En este sentido, con pentesters facilita la comunicación entre los miembros de los equipos, permitiéndoles compartir tanto sus conocimientos como informaciones. Asimismo, se hace un seguimiento de los recursos y se aplican estrategias de control para el cumplimiento de los objetivos trazados por las organizaciones (tanto a corto como a largo plazo).

Consciente de esta realidad, TECH ha desarrollado una pionera capacitación que comprende desde el análisis de vulnerabilidades hasta técnicas avanzadas de intrusión. El temario profundizará en una serie de metodologías orientadas a la seguridad ofensiva, entre las que sobresale el Cyber Security Kill Chain. Además, fomentará la creatividad mediante la técnica del think outside the box e impulsará así las soluciones innovadoras para diferenciarse del resto. También explorará los diferentes roles de los *pentestings*, enfatizando la necesidad de realizar investigaciones profundas. A su vez, ahondará en la herramienta del Metasploit, con el objetivo de realizar ataques simulados de forma controlada. Por último, se expondrán los principales desafíos que afectan a la seguridad ofensiva y se incentiva a convertirlos en oportunidades para que los egresados demuestren todo su potencial e ingenio.

Cabe destacar que, para afianzar el dominio de los contenidos, esta capacitación aplica el vanguardista sistema *Relearning*. TECH es pionera en el uso de ese modelo de enseñanza, que promueve la asimilación de conceptos complejos a través de la reiteración natural y progresiva de los mismos. En esta línea, también el programa se nutre de materiales en diversos formatos como infografías, resúmenes interactivos o vídeos explicativos. Todo ello en una cómoda modalidad 100% online, que permite a los alumnos ajustar los horarios en función de sus responsabilidades y circunstancias personales.

Este **Curso Universitario en Gestión de Equipos de pentesting** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

- ♦ El desarrollo de casos prácticos presentados por expertos en Gestión de Equipos de pentesting
- ♦ Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que está concebido recogen una información actualizada 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
- ♦ 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



*¿Quieres experimentar un salto profesional en tu carrera? Conviértete en un experto de Inteligencia en fuentes abiertas gracias a esta capacitación”*

“

*Conseguirás tus objetivos gracias a las herramientas didácticas de TECH, entre las que destacan vídeos explicativos y resúmenes interactivos”*

El programa incluye en su cuadro docente a profesionales del sector que vierten en esta capacitación la experiencia de su trabajo, además de reconocidos especialistas de sociedades de referencia y universidades de prestigio.

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

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

*Profundizarás en el researching para realizar las investigaciones más exhaustivas y diferenciarte así del resto.*

*Domina el programa Metasploit en la mejor universidad digital del mundo según Forbes.*



# 02

## Objetivos

El diseño del presente programa proporcionará una inmersión profunda en las tácticas y técnicas empleadas por los profesionales de seguridad ofensiva. En esta línea, se enfocará en el desarrollo de habilidades de pruebas de penetración y estrategias para explotar vulnerabilidades tanto en sistemas como redes. De esta manera, se ofrecerán conocimientos sólidos para realizar evaluaciones de seguridad de manera efectiva y ética. Los alumnos realizarán sesiones prácticas para aprender conceptos teóricos en entornos simulados, preparándose para enfrentar los desafíos del mundo real en *Red Team*.



“

*¿Buscas implementar las medidas de seguridad ofensiva más innovadoras? Lógralo gracias a este programa en solo 6 semanas”*



## Objetivos generales

---

- ♦ Adquirir habilidades avanzadas en pruebas de penetración y simulaciones de Red Team, abordando la identificación y explotación de vulnerabilidades en sistemas y redes
- ♦ Desarrollar capacidades de liderazgo para coordinar equipos especializados en ciberseguridad ofensiva, optimizando la ejecución de proyectos de Pentesting y Red Team
- ♦ Desarrollar habilidades en el análisis y desarrollo de malware, comprendiendo su funcionalidad y aplicando estrategias defensivas y educativas
- ♦ Perfeccionar habilidades de comunicación mediante la elaboración de informes técnicos y ejecutivos detallados, presentando hallazgos de manera efectiva a audiencias técnicas y ejecutivas
- ♦ Promover una práctica ética y responsable en el ámbito de la ciberseguridad, considerando los principios éticos y legales en todas las actividades
- ♦ Mantener actualizado al alumnado con las tendencias y tecnologías emergentes en ciberseguridad



*Durante tu proceso de aprendizaje, contarás con el respaldo de los mejores profesionales en Ciberseguridad”*





## Objetivos específicos

---

- ♦ Familiarizar al egresado con las metodologías de pruebas de penetración, incluyendo fases clave como la recolección de información, análisis de vulnerabilidades, explotación y documentación
- ♦ Desarrollar competencias prácticas en el uso de herramientas especializadas de Pentesting para identificar y evaluar vulnerabilidades en sistemas y redes
- ♦ Estudiar y comprender las tácticas, técnicas y procedimientos utilizados por los actores malintencionados, permitiendo la identificación y simulación de amenazas
- ♦ Aplicar conocimientos teóricos en escenarios prácticos y simulaciones, enfrentándose a desafíos reales para fortalecer habilidades de Pentesting
- ♦ Desarrollar habilidades de documentación efectiva, creando informes detallados que reflejan hallazgos, metodologías utilizadas y recomendaciones para la mejora de la seguridad
- ♦ Practicar la colaboración efectiva en equipos de seguridad ofensiva, optimizando la coordinación y ejecución de actividades de Pentesting

# 03

## Dirección del curso

En su compromiso de ofrecer la máxima calidad educativa, TECH dispone de un claustro docente de primer nivel. A estos expertos les caracteriza un profundo conocimiento en materia de ciberseguridad, al mismo tiempo que cuentan con un amplio bagaje profesional. Por eso, el presente itinerario académico pone a disposición de los alumnos las mejores herramientas y tácticas para que adquieran múltiples destrezas durante el curso. Así pues, los estudiantes tienen las garantías que precisan para especializarse en un sector digital que ofrece numerosas oportunidades laborales.



“

*Accederás a un sistema de aprendizaje basado en la reiteración, con una enseñanza natural y progresiva a lo largo de todo el temario”*

## 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. 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



# 04

# Estructura y contenido

Este plan de estudios se aborda desde una perspectiva teórica-práctica, de la mano de un experimentado cuadro docente que sumerge al alumnado en el análisis de las estrategias más eficaces en seguridad ofensiva. Para adquirir una comprensión integral de cómo operan los actores malintencionados, se profundiza en la categorización de vulnerabilidades (CAPEC, CVSS, etc.) Asimismo, se enfatiza en el empleo del scripting con la meta de ejecutar secuencias de comandos que automatizan tareas en un sistema informático, entre los que destacan JavaScript. También se abordan los principios de la ética *hacker* con el fin de entender las implicaciones legales y consecuencias que pueden generarse durante las actividades. Para conseguirlo, se analizan casos de estudio reales donde se han aplicado éticas en ciberseguridad.

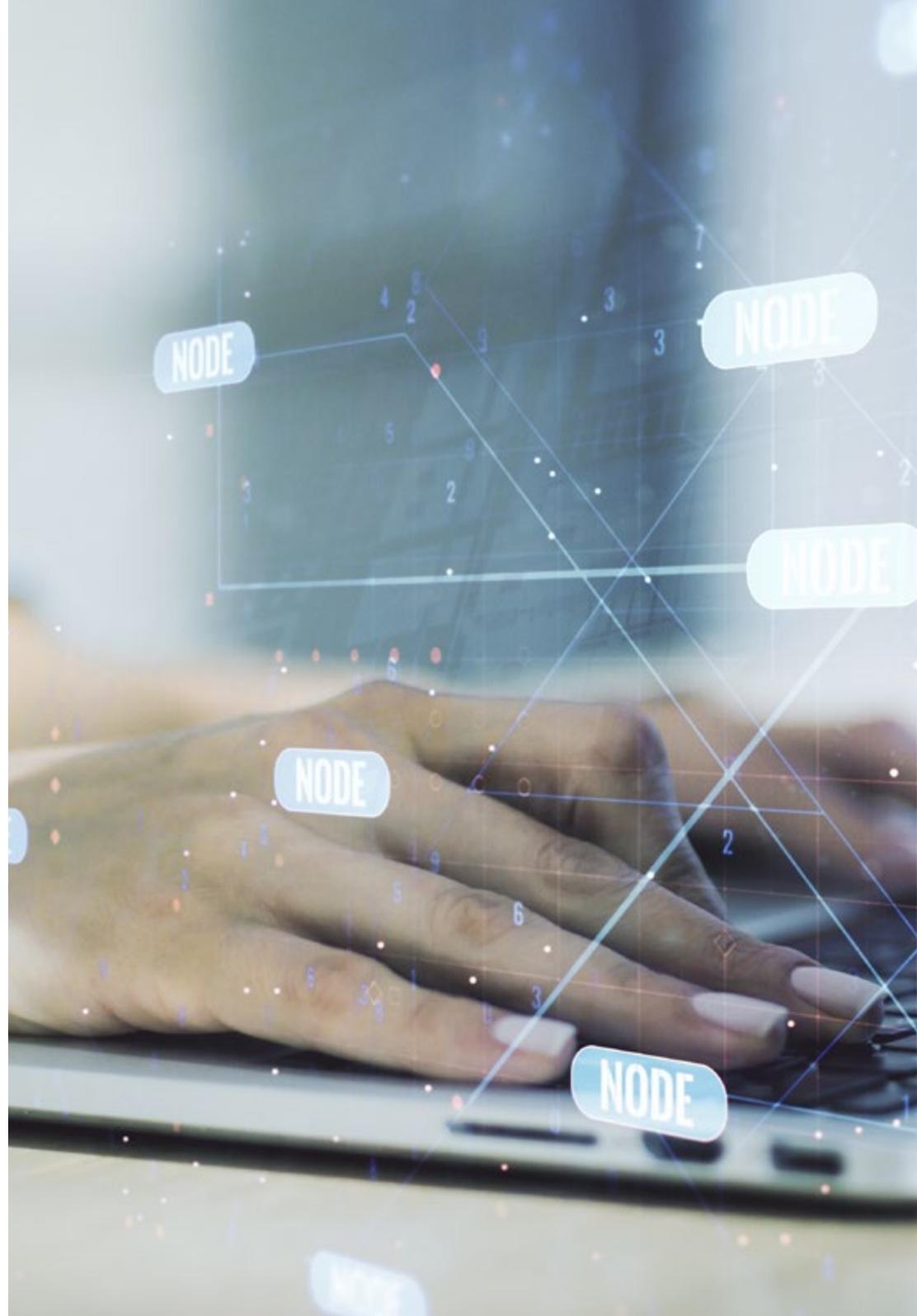


“

*Sin horarios ni cronogramas  
evaluativos preestablecidos: así  
es este programa de TECH”*

## 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

“ *Biblioteca atestada de recursos multimedia en diferentes formatos audiovisuales* ”

# 05 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”*

## 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”*



*Accederás a un sistema de aprendizaje basado en la reiteración, con una enseñanza natural y progresiva a lo largo de todo el temario.*



*El alumno aprenderá, mediante actividades colaborativas y casos reales, la resolución de situaciones complejas en entornos empresariales reales.*

## Un método de aprendizaje innovador y diferente

El presente programa de TECH es una enseñanza intensiva, creada desde 0, que propone los retos y decisiones más exigentes en este campo, 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 profesional más vigente.

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

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de Informática 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 tomaran decisiones y emitieran 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 te enfrentamos en el método del caso, un método de aprendizaje orientado a la acción. A lo largo del curso, 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.

*En 2019 obtuvimos los mejores resultados de aprendizaje de todas las universidades online en español en el mundo.*

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 universidad 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, se combinan cada uno de estos elementos de forma concéntrica. Con esta metodología se han capacitado más 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 capacitación, 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 y competencias

Realizarán 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.



#### 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 casos de estudio elegidos expresamente para esta titulación. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.



**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.



06

# Titulación

El Curso Universitario en Gestión de Equipos de pentesting garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Curso Universitario expedido por TECH Global University.



“

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

Este programa te permitirá obtener el título propio de **Curso Universitario en Gestión de Equipos de Pentesting** avalado por **TECH Global University**, la mayor Universidad digital del mundo.

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

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

Título: **Curso Universitario en Gestión de Equipos de Pentesting**

Modalidad: **online**

Duración: **6 semanas**

Acreditación: **6 ECTS**





## Curso Universitario Gestión de Equipos de pentesting

- » Modalidad: **online**
- » Duración: **6 semanas**
- » Titulación: **TECH Global University**
- » Acreditación: **6 ECTS**
- » Horario: **a tu ritmo**
- » Exámenes: **online**

# Curso Universitario

## Gestión de Equipos de pentesting

