

Experto Universitario

Ciberseguridad Ofensiva



Experto Universitario Ciberseguridad Ofensiva

- » Modalidad: online
- » Duración: 6 meses
- » Titulación: TECH Universidad
- » Horario: a tu ritmo
- » Exámenes: online

Acceso web: www.techtitute.com/informatica/experto-universitario/experto-ciberseguridad-ofensiva

Índice

01

Presentación

pág. 4

02

Objetivos

pág. 8

03

Dirección del curso

pág. 12

04

Estructura y contenido

pág. 16

05

Metodología

pág. 22

06

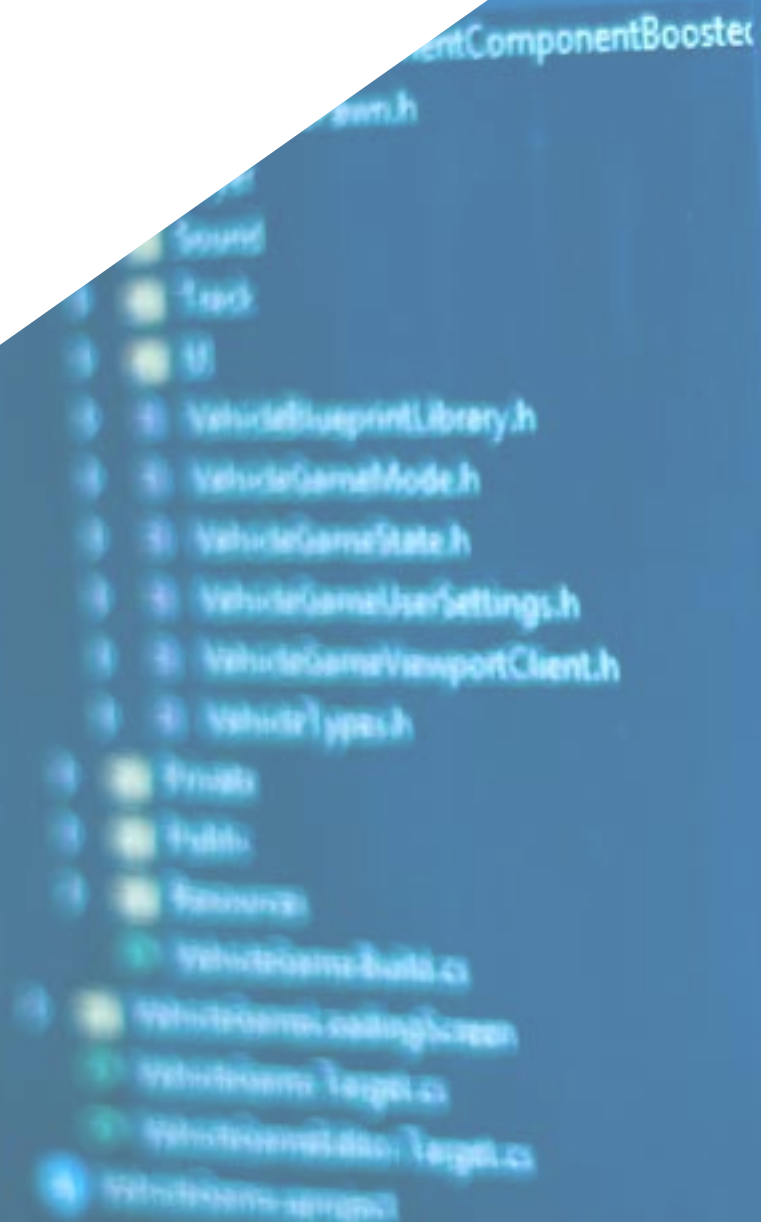
Titulación

pág. 30

01

Presentación

La ciberseguridad constituye un aspecto esencial para que las instituciones protejan sus activos digitales, mantengan su reputación social y se salvaguarden del espionaje de sus competidores. De ahí que cada vez más compañías soliciten la incorporación de expertos informáticos en sus organigramas, con el fin de evitar consecuencias que incluso podrían afectar a sus capacidades financieras. En este contexto, dichos especialistas necesitan actualizar su conocimientos y destrezas constantemente para estar al día de las técnicas de ciberdelincuencia. Por este motivo, TECH ha desarrollado un innovador Experto Universitario, en el que se identificarán y mitigarán amenazas. Cabe destacar que toda la programación se impartirá en una modalidad 100% online, para garantizar que los estudiantes cuenten con una mayor comodidad y flexibilidad.



```
GENERATED_UCLASS_BODY()

// Begin Actor overrides
virtual void PostInitializeComponents() override;
virtual void Tick(float DeltaSeconds) override;
virtual void ReceiveHit(class UPrimitiveComponent*, class FVector HitLocation, class FVector Impulse, class UDamageType* DamageType, bool bIsSelf) override;
virtual void FellOutOfWorld(const class UDamageType* DamageType) override;
// End Actor overrides

// Begin Pawn overrides
virtual void SetupPlayerInputComponent(class UInputComponent*) override;
virtual float TakeDamage(float Damage, class FVector DamageLocation, class UDamageType* DamageType, class AActor* Instigator) 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 network
 * UFUNCTION()
 * void OnRep_Dying()
 */

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



Profundizarás en el protocolo de Kerberos y protegerás la información en entornos de red”

Cada día se reportan en los medios de comunicación casos que tienen como protagonistas a piratas informáticos, que perjudican a las instituciones accediendo a sus bases de datos. Las consecuencias de estos ataques son graves, ya que interrumpen las operaciones e impiden que las empresas funcionen de manera efectiva. De hecho, puede impactar directamente en su economía al acarrear multas por incumplimiento de regulaciones y limitación de ingresos.

En este sentido, TECH ha creado una titulación vanguardista para detectar las técnicas de intrusión más empleadas, así como las estrategias más óptimas para hacerles frente. Bajo la dirección de un claustro docente experimentado en la materia, el temario establecerá las bases esenciales para entender cómo piensan los hackers. Asimismo, brindará diversas soluciones, destinadas a proporcionar infraestructuras seguras para la administración de certificados digitales en una red empresarial.

Igualmente, los profesionales abordarán una óptima preparación de los entornos virtuales, gracias a la configuración de máquinas virtuales o snapshots. Además, se analizarán los malware, indagando en las llamadas con API Monitor y observando con TCPView las peticiones en red. Los egresados aprenderán conceptos teóricos en entornos simulados, preparándose así para los desafíos del mundo real en Ciberseguridad Ofensiva. Por último, se hará hincapié en la ética y la responsabilidad social que debe caracterizar a los expertos en este ámbito.

Para afianzar el dominio de todos esos contenidos, el Experto Universitario aplica el innovador sistema Relearning. TECH es pionera en el uso de este modelo de enseñanza, el cual promueve la asimilación de conceptos complejos a través de la reiteración natural y progresiva de los mismos. El programa también se nutre de materiales en diversos formatos, como los vídeos explicativos, los resúmenes interactivos y las infografías. Todo ello en una cómoda modalidad 100% online, que permite ajustar los horarios de cada persona a sus responsabilidades y disponibilidad.

Este **Experto Universitario en Ciberseguridad Ofensiva** contiene el programa universitario más completo y actualizado del mercado. Sus características más destacadas son:

- ♦ El desarrollo de casos prácticos presentados por expertos en Ciberseguridad Ofensiva
- ♦ Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que está concebido recogen una información completa 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



Desarrolla tus habilidades como auditor ofensivo y embárcate en un nuevo reto profesional en las empresas digitales más prestigiosas"

“

Conseguirás tus objetivos a través de las herramientas didácticas de TECH, entre las que destacan los vídeos explicativos y los 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.

¿Quieres convertirte en Big Bounty Hunter? Captarás cualquier vulnerabilidad en Internet gracias a este programa.

En tan solo 6 meses dominarás la gestión de identidades en Azure AD. ¡Matricúlate ahora!



02

Objetivos

El diseño del presente programa ofrece una experiencia educativa única, que destaca por su enfoque práctico e innovador en Ciberseguridad. De esta forma, el alumnado abordará, desde el análisis de vulnerabilidades, hasta las técnicas avanzadas de intrusión. En esta línea, se ofrecerán las medidas óptimas para evaluar y fortalecer los diferentes sistemas cibernéticos. Además, se enfatizará tanto la responsabilidad legal como en la ética que deben adoptar los expertos de esta materia.



“

Reduce las amenazas de malware con la mejor universidad digital del mundo, según Forbes”



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



Objetivos específicos

Módulo 1. La Seguridad Ofensiva

- ♦ 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*

Módulo 2. Ataques a Redes y Sistemas Windows

- ♦ Desarrollar habilidades para identificar y evaluar vulnerabilidades específicas en sistemas operativos Windows
- ♦ Aprender tácticas avanzadas utilizadas por atacantes para infiltrarse y persistir en redes basadas en entornos Windows
- ♦ Adquirir competencias en estrategias y herramientas para mitigar amenazas específicas dirigidas a sistemas operativos Windows
- ♦ Familiarizar al egresado con técnicas de análisis forense aplicadas a sistemas Windows, facilitando la identificación y respuesta a incidentes

- ♦ Aplicar conocimientos teóricos en entornos simulados, participando en ejercicios prácticos para entender y contrarrestar ataques específicos a sistemas Windows
- ♦ Aprender estrategias específicas para asegurar entornos empresariales que utilizan sistemas operativos Windows, considerando las complejidades de infraestructuras empresariales
- ♦ Desarrollar competencias para evaluar y mejorar las configuraciones de seguridad en sistemas Windows, asegurando la implementación de medidas eficaces
- ♦ Promover prácticas éticas y legales en la ejecución de ataques y pruebas en sistemas Windows, considerando los principios éticos de la ciberseguridad
- ♦ Mantener al día al alumno con las últimas tendencias y amenazas en ataques a sistemas Windows, garantizando la relevancia y efectividad constante de las habilidades adquiridas

Módulo 3. Análisis y Desarrollo de *Malware*

- ♦ Adquirir conocimientos avanzados sobre la naturaleza, funcionalidad y comportamiento del *malware*, comprendiendo sus diversas formas y objetivos
- ♦ Desarrollar habilidades en el análisis forense aplicado al *malware*, permitiendo la identificación de indicadores de compromiso (IoC) y patrones de ataque
- ♦ Aprender estrategias para la detección y prevención efectiva de *malware*, incluyendo el despliegue de soluciones de seguridad avanzadas
- ♦ Familiarizar al alumno con el desarrollo de *malware* con propósitos educativos y defensivos, permitiendo la comprensión profunda de las tácticas utilizadas por los atacantes
- ♦ Promover prácticas éticas y legales en el análisis y desarrollo de *malware*, garantizando la integridad y responsabilidad en todas las actividades

- ♦ Aplicar conocimientos teóricos en entornos simulados, participar en ejercicios prácticos para entender y contrarrestar ataques maliciosos
- ♦ Desarrollar habilidades para evaluar y seleccionar herramientas de seguridad *anti-malware*, considerando su eficacia y adaptabilidad a entornos específicos
- ♦ Aprender a implementar de mitigación efectiva contra amenazas maliciosas, reduciendo el impacto y la propagación del *malware* en sistemas y redes
- ♦ Fomentar la colaboración efectiva con equipos de seguridad, integrando estrategias y esfuerzos para proteger contra amenazas de *malware*
- ♦ Mantener al día al egresado con las últimas tendencias y técnicas utilizadas en el análisis y desarrollo de *malware*, asegurando la relevancia y eficacia constante de las habilidades adquiridas



*¡Olvídate de memorizar!
Con el sistema Relearning
integrarás los conceptos de
manera natural y progresiva”*

03

Dirección del curso

En su compromiso por ofrecer la excelencia educativa, TECH cuenta con un claustro docente de prestigio. Cabe destacar que dichos especialistas cuentan con un amplio bagaje profesional, tras formar parte de reconocidas empresas dedicadas a la Ciberseguridad Ofensiva. Por este motivo, el itinerario académico contará con los recursos y las tecnologías más avanzadas en esta materia. Además, se ofrecerá enfoque integral para cumplir con las expectativas que demanda el egresado para especializarse en un ámbito que le brindará muchas oportunidades.





“

Tendrás el apoyo de un cuadro docente formado por distinguidos profesionales en Ciberguridad Ofensiva”

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. 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. 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. 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

04

Estructura y contenido

El presente programa se estructura en 3 módulos: Seguridad Ofensiva, Ataque a Redes o Sistemas Windows, y Análisis y Desarrollo de *Malware*. A lo largo del plan de estudio, se aportará una perspectiva práctica orientada a la detección de las primeras amenazas. En este sentido, se fomentará la creatividad de los alumnos para superar los desafíos mediante soluciones innovadoras. Además, se profundizará en la categorización de vulnerabilidades, entre las que sobresale la CVE. Asimismo, se indagará en técnicas avanzadas de análisis de *malware*, con el fin de fortalecer la seguridad en entornos cibernéticos.

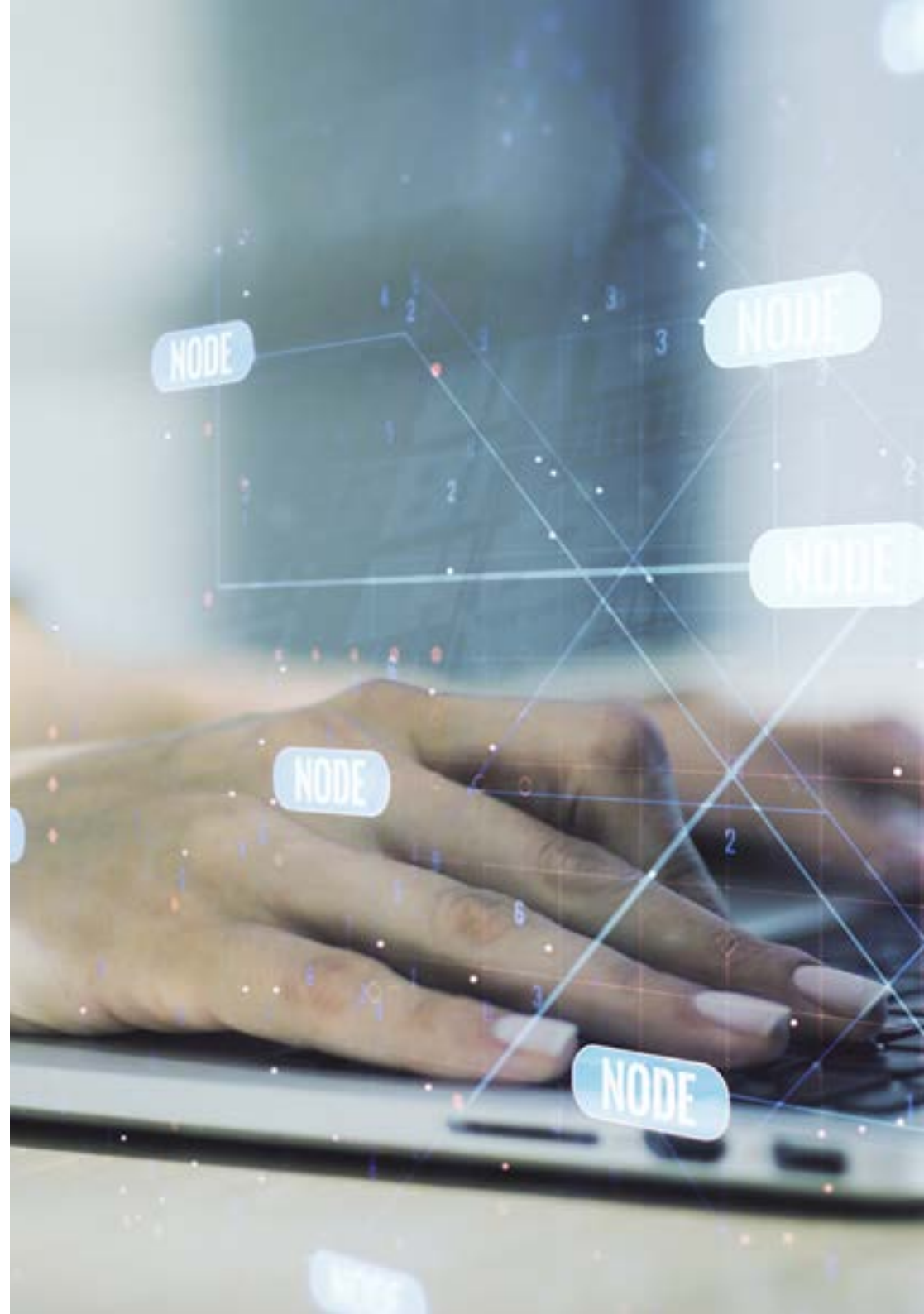


“

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

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. Ataques a Redes y Sistemas Windows

- 2.1. Windows y Directorio Activo
 - 2.1.1. Historia y evolución de Windows
 - 2.1.2. Conceptos básicos de Directorio Activo
 - 2.1.3. Funciones y servicios del Directorio Activo
 - 2.1.4. Arquitectura general del Directorio Activo
- 2.2. Redes en entornos de Directorio Activo
 - 2.2.1. Protocolos de red en Windows
 - 2.2.2. DNS y su funcionamiento en el Directorio Activo
 - 2.2.3. Herramientas de diagnóstico de red
 - 2.2.4. Implementación de redes en Directorio Activo
- 2.3. Autenticación y autorización en Directorio Activo
 - 2.3.1. Proceso y flujo de autenticación
 - 2.3.2. Tipos de credenciales
 - 2.3.3. Almacenamiento y gestión de credenciales
 - 2.3.4. Seguridad en la autenticación
- 2.4. Permisos y políticas en Directorio Activo
 - 2.4.1. GPOs
 - 2.4.2. Aplicación y gestión de GPOs
 - 2.4.3. Administración de permisos en Directorio Activo
 - 2.4.4. Vulnerabilidades y mitigaciones en permisos

- 2.5. Fundamentos de Kerberos
 - 2.5.1. ¿Qué es Kerberos?
 - 2.5.2. Componentes y funcionamiento
 - 2.5.3. Tickets en Kerberos
 - 2.5.4. Kerberos en el contexto de Directorio Activo
- 2.6. Técnicas avanzadas en Kerberos
 - 2.6.1. Ataques comunes en Kerberos
 - 2.6.2. Mitigaciones y protecciones
 - 2.6.3. Monitorización del tráfico Kerberos
 - 2.6.4. Ataques avanzados en Kerberos
- 2.7. *Active Directory Certificate Services (ADCS)*
 - 2.7.1. Conceptos básicos de PKI
 - 2.7.2. Roles y componentes de ADCS
 - 2.7.3. Configuración y despliegue de ADCS
 - 2.7.4. Seguridad en ADCS
- 2.8. Ataques y defensas en *Active Directory Certificate Services (ADCS)*
 - 2.8.1. Vulnerabilidades comunes en ADCS
 - 2.8.2. Ataques y técnicas de explotación
 - 2.8.3. Defensas y mitigaciones
 - 2.8.4. Monitorización y auditoría de ADCS
- 2.9. Auditoría del Directorio Activo
 - 2.9.1. Importancia de la auditoría en el Directorio Activo
 - 2.9.2. Herramientas de auditoría
 - 2.9.3. Detección de anomalías y comportamientos sospechosos
 - 2.9.4. Respuesta a incidentes y recuperación
- 2.10. Azure AD
 - 2.10.1. Conceptos básicos de Azure AD
 - 2.10.2. Sincronización con el Directorio Activo local
 - 2.10.3. Gestión de identidades en Azure AD
 - 2.10.4. Integración con aplicaciones y servicios



Módulo 3. Análisis y Desarrollo de *Malware*

- 3.1. Análisis y desarrollo de *malware*
 - 3.1.1. Historia y evolución del *malware*
 - 3.1.2. Clasificación y tipos de *malware*
 - 3.1.3. Análisis de *malware*
 - 3.1.4. Desarrollo de *malware*
- 3.2. Preparando el entorno
 - 3.2.1. Configuración de Máquinas Virtuales y *Snapshots*
 - 3.2.2. Herramientas para análisis de *malware*
 - 3.2.3. Herramientas para desarrollo de *malware*
- 3.3. Fundamentos de Windows
 - 3.3.1. Formato de fichero PE (*Portable Executable*)
 - 3.3.2. Procesos y *Threads*
 - 3.3.3. Sistema de archivos y registro
 - 3.3.4. *Windows Defender*
- 3.4. Técnicas de *malware* básicas
 - 3.4.1. Generación de *shellcode*
 - 3.4.2. Ejecución de *shellcode* en disco
 - 3.4.3. Disco vs memoria
 - 3.4.4. Ejecución de *shellcode* en memoria
- 3.5. Técnicas de *malware* intermedias
 - 3.5.1. Persistencia en Windows
 - 3.5.2. Carpeta de inicio
 - 3.5.3. Claves del registro
 - 3.5.4. Salvapantallas
- 3.6. Técnicas de *malware* avanzadas
 - 3.6.1. Cifrado de *shellcode* (XOR)
 - 3.6.2. Cifrado de *shellcode* (RSA)
 - 3.6.3. Ofuscación de *strings*
 - 3.6.4. Inyección de procesos

- 3.7. Análisis estático de *malware*
 - 3.7.1. Analizando *packers* con DIE (*Detect It Easy*)
 - 3.7.2. Analizando secciones con PE-Bear
 - 3.7.3. Decompilación con Ghidra
- 3.8. Análisis dinámico de *malware*
 - 3.8.1. Observando el comportamiento con Process Hacker
 - 3.8.2. Analizando llamadas con API Monitor
 - 3.8.3. Analizando cambios de registro con Regshot
 - 3.8.4. Observando peticiones en red con TCPView
- 3.9. Análisis en .NET
 - 3.9.1. Introducción a .NET
 - 3.9.2. Decompilando con dnSpy
 - 3.9.3. Depurando con dnSpy
 - 3.10. Analizando un *malware* real
- 3.10.1. Preparando el entorno
 - 3.10.2. Análisis estático del *malware*
 - 3.10.3. Análisis dinámico del *malware*
 - 3.10.4. Creación de reglas YARA



Sin horarios ni cronogramas evaluativos preestablecidos. ¡Así es esta capacitación de TECH!”

05

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

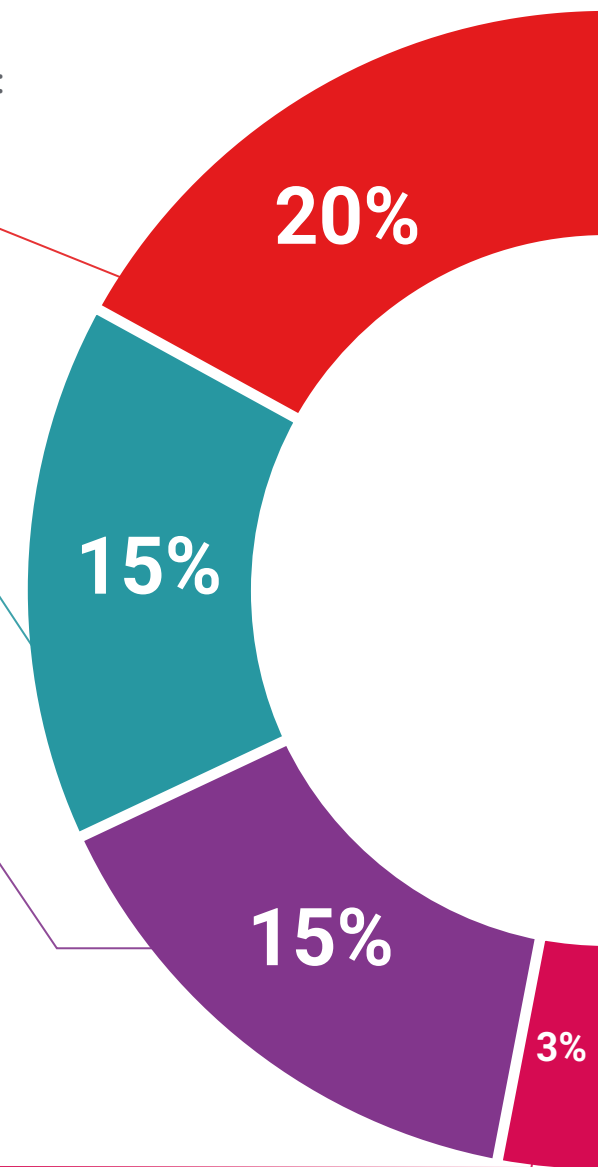
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

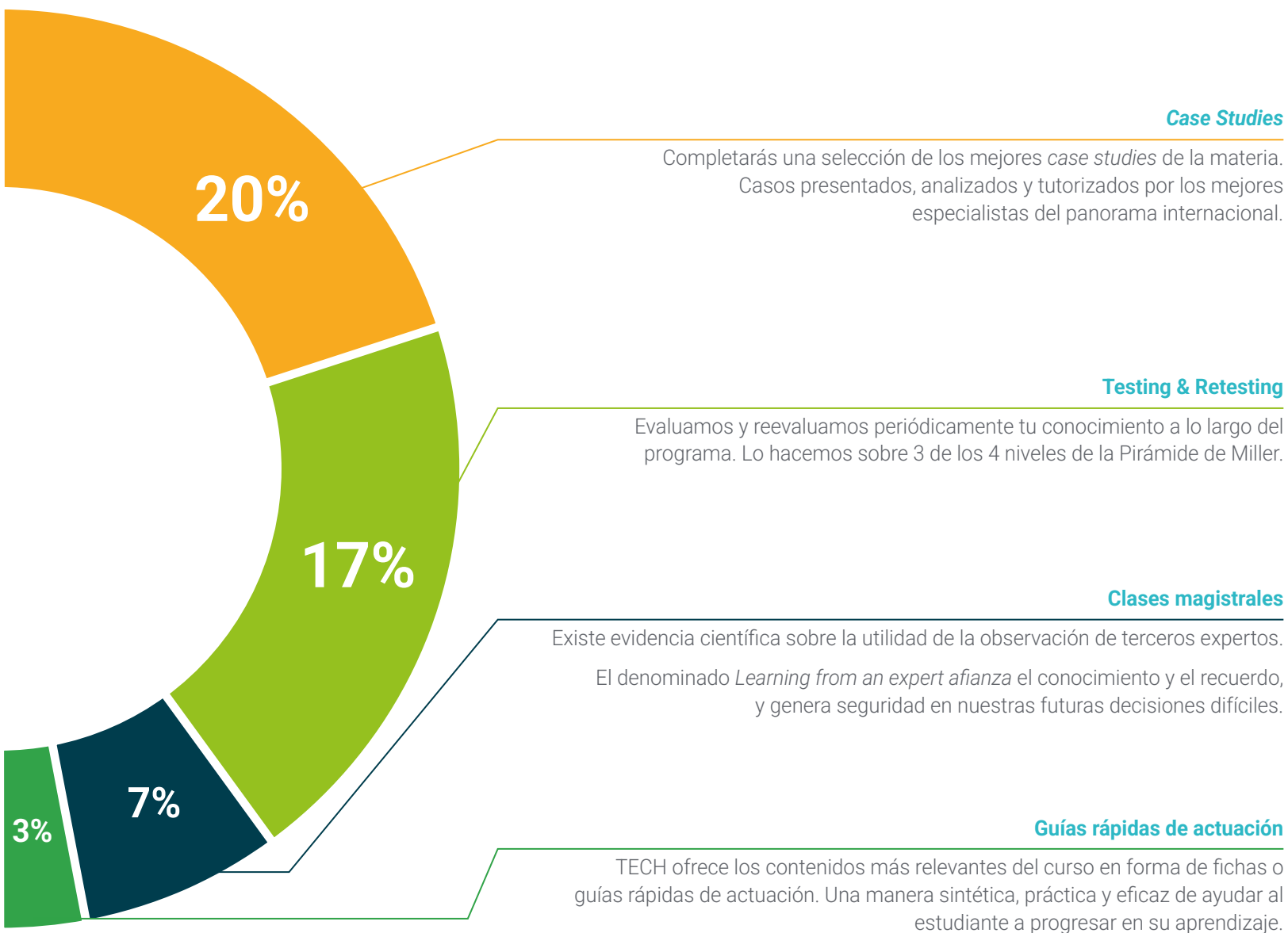
Este sistema exclusivo educativo para la presentación de contenidos multimedia fue premiado por Microsoft como "Caso de éxito en Europa".



Lecturas complementarias

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





06 Titulación

El Experto Universitario en Ciberseguridad Ofensiva garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Experto Universitario expedido por TECH Universidad.



“

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

Este **Experto Universitario en Ciberseguridad Ofensiva** contiene el programa universitario más completo y actualizado del mercado.

Tras la superación de la evaluación, el alumno recibirá por correo postal* con acuse de recibo su correspondiente título de **Experto Universitario** emitido por **TECH Universidad**.

Este título expedido por **TECH Universidad** expresará la calificación que haya obtenido en el Experto Universitario, y reunirá los requisitos comúnmente exigidos por las bolsas de trabajo, oposiciones y comités evaluadores de carreras profesionales.

Título: **Experto Universitario en Ciberseguridad Ofensiva**

Modalidad: **online**

Duración: **6 meses**



*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.



Experto Universitario Ciberseguridad Ofensiva

- » Modalidad: online
- » Duración: 6 meses
- » Titulación: TECH Universidad
- » Horario: a tu ritmo
- » Exámenes: online

Experto Universitario

Ciberseguridad Ofensiva