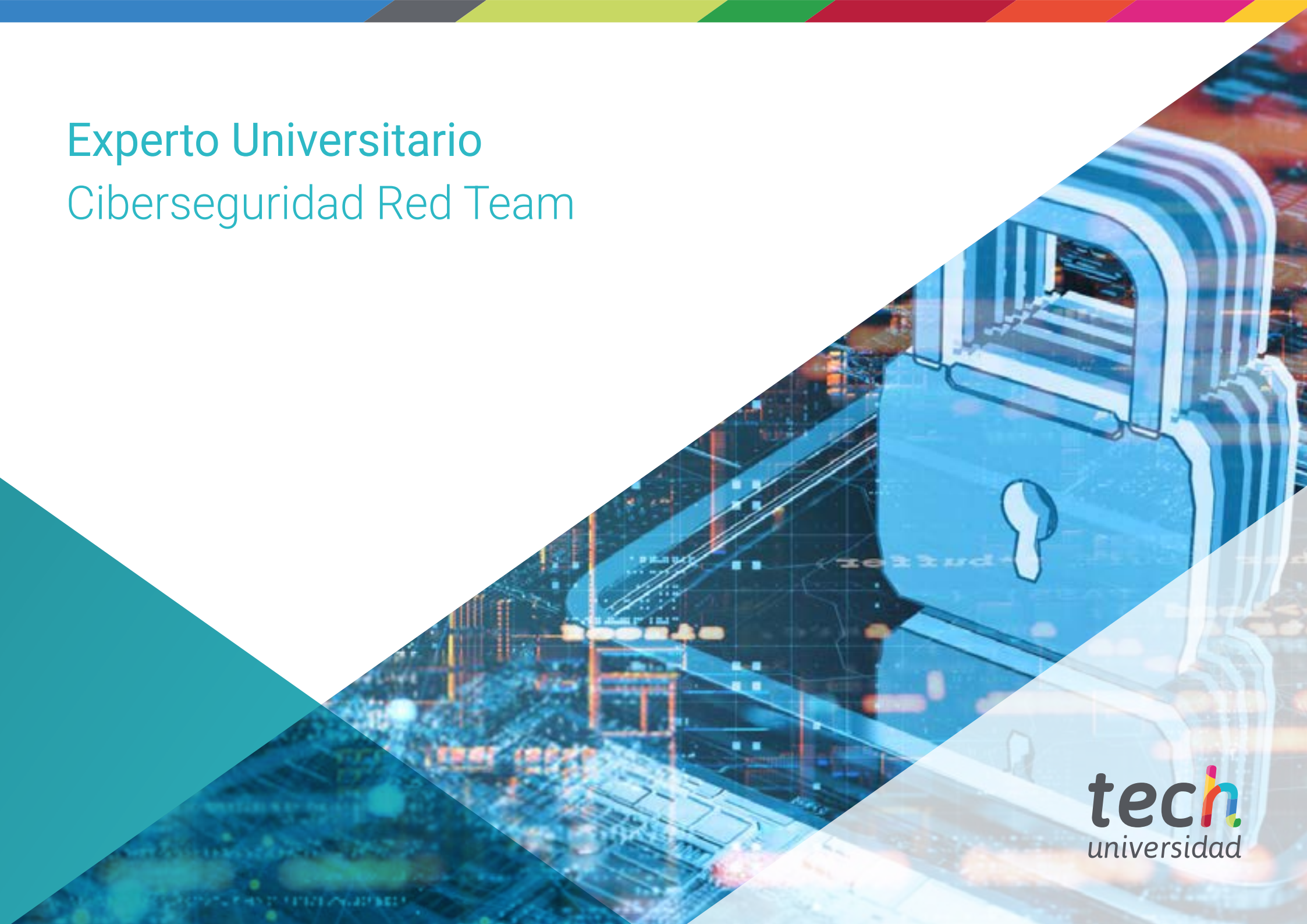
Experto Universitario
Ciberseguridad Red Team



tech universidad

tech universidad

Experto Universitario
Ciberseguridad Red Team

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

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

Índice

01

Presentación

La Ciberseguridad se ha convertido un pilar fundamental en la era digital, mientras que la creciente interconexión de sistemas ha intensificado la amenaza de ciberataques. La demanda de profesionales altamente capacitados en este campo es más evidente que nunca, especialmente considerando el aumento exponencial de la ciberdelincuencia y los ataques sofisticados. En este contexto, este programa se presenta como una respuesta estratégica para equipar a los profesionales con las habilidades necesarias para enfrentar amenazas cibernéticas. A lo largo del temario, los estudiantes se sumergirán en la simulación de amenazas avanzadas. La metodología del plan de estudios, 100% online, ofrece flexibilidad y accesibilidad, con una gran variedad de contenidos multimedia y la aplicación del método *Relearning*.

Contribuirás a mejorar la Ciberseguridad y evitarás que se produzcan grandes delitos digitales. ¡No pierdas esta oportunidad e inscríbete ya!"

En el complejo escenario de la Ciberseguridad, tener un experto en este campo se presenta como una necesidad imperante para las organizaciones que buscan fortalecer sus defensas contra amenazas en constante evolución. Este enfoque proactivo, fundamental para mejorar continuamente la postura de seguridad, resalta la necesidad crítica de expertos.

La implementación de medidas proactivas es esencial y la capacitación especializada en Red Team ofrece a los profesionales la capacidad de anticipar, identificar y mitigar activamente vulnerabilidades en sistemas y redes. En este Experto Universitario, el alumno adquirirá habilidades en pruebas de penetración y simulaciones, abordando la identificación y explotación de vulnerabilidades. En este sentido, no solo desarrollará competencias técnicas avanzadas, sino que también fomentará la colaboración efectiva con los equipos de seguridad, integrando estrategias contra amenazas de *malware*.

Además, los egresados adquirirán conocimientos sólidos sobre los principios fundamentales de la investigación forense digital (DFIR), aplicables en la resolución de incidentes cibernéticos. Asimismo, este enfoque integral del temario garantizará que los profesionales se equipen con destrezas de vanguardia en el campo de la Ciberseguridad.

Este itinerario académico se distingue, no solo por su contenido, sino también por su metodología avanzada. Y es que estará a disposición de los estudiantes de manera totalmente online, otorgando la flexibilidad que necesitan para avanzar en sus carreras sin comprometer sus responsabilidades laborales.

Asimismo, la aplicación del *Relearning*, consistente en la repetición de conceptos clave, se emplea para fijar conocimientos y facilitar un aprendizaje efectivo. Esta combinación de accesibilidad y enfoque pedagógico robusto hace que este Experto Universitario no solo sea una opción educativa avanzada, sino también un impulsor significativo para aquellos que buscan destacar en el ámbito de la Ciberseguridad.

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

- El desarrollo de casos prácticos presentados por expertos en Ciberseguridad Red Team
- 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

Destacarás en un sector con gran proyección gracias a este exclusivo programa universitario de TECH”

Ahondarás en la elaboración de informes forenses detallados en la universidad mejor valorada del mundo por sus alumnos, según la plataforma Trustpilot (4,9/5)"

Desarrollarás habilidades para evaluar y seleccionar herramientas de seguridad anti-malware.

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

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.

02

Objetivos

El Experto Universitario en Ciberseguridad *Red Team* tiene como objetivo principal capacitar a los alumnos en el desarrollo de competencias en la simulación de amenazas avanzadas. A lo largo del programa, los egresados se sumergirán en la replicación de tácticas, técnicas y procedimientos (TTP), utilizados por actores malintencionados. En este contexto, el enfoque especializado no solo fortalecerá las habilidades técnicas de los profesionales, sino que también los capacitará para enfrentar desafíos del mundo real en este ámbito. Asimismo, el empleo de la metodología *Relearning* facilitará el aprendizaje, fijando conceptos clave con poco esfuerzo.

Identificarás puntos débiles y vulnerabilidades en las infraestructuras cibernéticas de las empresas. ¡Alcanza tus metas con TECH!"

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

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

Objetivos específicos

Módulo 1. 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

Módulo 2. Fundamentos Forenses y DFIR

- Adquirir conocimientos sólidos sobre los principios fundamentales de la investigación forense digital (DFIR) y su aplicación en la resolución de incidentes cibernéticos
- Desarrollar habilidades en la adquisición segura y forense de evidencia digital, garantizando la preservación de la cadena de custodia
- Aprender a realizar análisis forenses de sistemas de archivos
- Familiarizar al estudiante con técnicas avanzadas para el análisis de registros y bitácoras, permitiendo la reconstrucción de eventos en entornos digitales
- Aprender a aplicar metodologías de investigación forense digital en la resolución de casos, desde la identificación hasta la documentación de hallazgos
- Familiarizar al alumno con el análisis de evidencia digital y la aplicación de técnicas forenses en entornos de *Pentesting*
- Desarrollar habilidades en la elaboración de informes forenses detallados y claros, presentando hallazgos y conclusiones de manera comprensible
- Fomentar la colaboración efectiva con equipos de respuesta a incidentes (IR), optimizando la coordinación en la investigación y mitigación de amenazas
- Promover prácticas éticas y legales en la investigación forense digital, asegurando la adhesión a normativas y estándares de conducta en Ciberseguridad

Módulo 3. Ejercicios de Red Team Avanzados

- Desarrollar competencias en la simulación de amenazas avanzadas, replicando tácticas, técnicas y procedimientos (TTP) utilizados por actores malintencionados atractivos
- Aprender a identificar puntos débiles y vulnerabilidades en la infraestructura mediante ejercicios realistas de *Red Team*, fortaleciendo la postura de seguridad
- Familiarizar al egresado con técnicas avanzadas de evasión de medidas de seguridad, permitiendo evaluar la resistencia de la infraestructura ante ataques deseables
- Desarrollar habilidades de coordinación y colaboración efectiva entre los miembros del equipo de *Red Team*, optimizando la ejecución de tácticas y estrategias para evaluar comprehensivamente la seguridad de la organización
- Aprender a simular escenarios de amenazas actuales, como ataques de *ransomware* o campañas de *phishing* avanzadas, para evaluar la capacidad de respuesta de la organización
- Familiarizar al estudiante con técnicas de análisis post-ejercicio, evaluando el desempeño del equipo de *Red Team* y extrayendo lecciones aprendidas para la mejora continua
- Desarrollar habilidades para evaluar la resiliencia organizacional ante ataques simulados, identificando áreas de mejora en políticas y procedimientos
- Aprender a elaborar informes detallados que documenten los hallazgos, metodologías utilizadas y recomendaciones derivadas de ejercicios de *Red Team* avanzados
- Promover prácticas éticas y legales en la realización de ejercicios de *Red Team*, asegurando la adhesión a normativas y estándares éticos en Ciberseguridad

03

Dirección del curso

Para este programa universitario, TECH ha reunido a un distinguido claustro docente, compuesto por los mejores especialistas en el campo. En este sentido, cada miembro del cuerpo docente posee un extenso y reconocido bagaje profesional, forjado en empresas líderes del sector de la Ciberseguridad. Asimismo, seleccionados cuidadosamente por su experiencia y conocimientos especializados, estos profesionales no solo garantizarán la calidad académica del plan de estudios, sino que también aportarán una perspectiva práctica y actualizada, enriqueciendo la formación de los participantes con insights valiosos provenientes de su experiencia real en el ámbito del Red Team.

Actualízate con las últimas técnicas de cifrado de Shellcode (XQR) de la mano de los mejores expertos en Ciberseguridad. ¡Lanza tu carrera profesional con TECH!"

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 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 plan de estudios ofrecerá al alumno una inmersión especializada en el análisis forense aplicado al *malware*, destacando el desarrollo de habilidades clave para la identificación de indicadores de compromiso (IoC) y patrones de ataque. A lo largo del temario, los egresados se sumergirán en metodologías avanzadas, proporcionándoles las herramientas y conocimientos necesarios para enfrentar amenazas cibernéticas sofisticadas. Asimismo, este programa, estructurado de manera rigurosa, garantizará una formación integral en el ámbito del *Red Team*, preparando a los profesionales para analizar y contrarrestar las complejas estrategias utilizadas por actores malintencionados.

Profundizarás en técnicas avanzadas de post-explotación y te posicionarás como un destacado Red Teamer”

Módulo 1. Análisis y Desarrollo de *Malware*

1.1. Análisis y desarrollo de *malware*
- 1.1.1. Historia y evolución del *malware*
- 1.1.2. Clasificación y tipos de *malware*
- 1.1.3. Análisis de *malware*
- 1.1.4. Desarrollo de *malware*

1.2. Preparando el entorno
- 1.2.1. Configuración de Máquinas Virtuales y *Snapshots*
- 1.2.2. Herramientas para análisis de *malware*
- 1.2.3. Herramientas para desarrollo de *malware*

1.3. Fundamentos de Windows
- 1.3.1. Formato de fichero PE (*Portable Executable*)
- 1.3.2. Procesos y *Threads*
- 1.3.3. Sistema de archivos y registro
- 1.3.4. *Windows Defender*

1.4. Técnicas de *malware* básicas
- 1.4.1. Generación de *shellcode*
- 1.4.2. Ejecución de *shellcode* en disco
- 1.4.3. Disco vs memoria
- 1.4.4. Ejecución de *shellcode* en memoria

1.5. Técnicas de *malware* intermedias
- 1.5.1. Persistencia en Windows
- 1.5.2. Carpeta de inicio
- 1.5.3. Claves del registro
- 1.5.4. Salvapantallas

1.6. Técnicas de *malware* avanzadas
- 1.6.1. Cifrado de *shellcode* (XOR)
- 1.6.2. Cifrado de *shellcode* (RSA)
- 1.6.3. Ofuscación de *strings*
- 1.6.4. Inyección de procesos

1.7. Análisis estático de *malware*
- 1.7.1. Analizando *packers* con DIE (*Detect It Easy*)
- 1.7.2. Analizando secciones con PE-Bear
- 1.7.3. Decompilación con Ghidra

1.8. Análisis dinámico de *malware*
- 1.8.1. Observando el comportamiento con Process Hacker
- 1.8.2. Analizando llamadas con API Monitor
- 1.8.3. Analizando cambios de registro con Regshot
- 1.8.4. Observando peticiones en red con TCPView

1.9. Análisis en .NET
- 1.9.1. Introducción a .NET
- 1.9.2. Decompilando con dnSpy
- 1.9.3. Depurando con dnSpy

1.10. Analizando un *malware* real
- 1.10.1. Preparando el entorno
- 1.10.2. Análisis estático del *malware*
- 1.10.3. Análisis dinámico del *malware*
- 1.10.4. Creación de reglas YARA

Módulo 2. Fundamentos Forenses y DFIR

2.1. Forense digital
- 2.1.1. Historia y evolución de la informática forense
- 2.1.2. Importancia de la informática forense en la ciberseguridad
- 2.1.3. Historia y evolución de la informática forense

2.2. Fundamentos de la informática forense
- 2.2.1. Cadena de custodia y su aplicación
- 2.2.2. Tipos de evidencia digital
- 2.2.3. Procesos de adquisición de evidencia

2.3. Sistemas de archivos y estructura de datos
- 2.3.1. Principales sistemas de archivos
- 2.3.2. Métodos de ocultamiento de datos
- 2.3.3. Análisis de metadatos y atributos de archivos

2.4. Análisis de Sistemas Operativos
- 2.4.1. Análisis forense de sistemas Windows
- 2.4.2. Análisis forense de sistemas Linux
- 2.4.3. Análisis forense de sistemas macOS

2.5. Recuperación de datos y análisis de disco
- 2.5.1. Recuperación de datos de medios dañados
- 2.5.2. Herramientas de análisis de disco
- 2.5.3. Interpretación de tablas de asignación de archivos

2.6. Análisis de redes y tráfico
- 2.6.1. Captura y análisis de paquetes de red
- 2.6.2. Análisis de registros de *firewall*
- 2.6.3. Detección de intrusiones en red

2.7. *Malware* y análisis de código malicioso
- 2.7.1. Clasificación de *malware* y sus características
- 2.7.2. Análisis estático y dinámico de *malware*
- 2.7.3. Técnicas de desensamblado y depuración

2.8. Análisis de registros y eventos
- 2.8.1. Tipos de registros en sistemas y aplicaciones
- 2.8.2. Interpretación de eventos relevantes
- 2.8.3. Herramientas de análisis de registros

2.9. Responder a incidentes de seguridad
- 2.9.1. Proceso de respuesta a incidentes
- 2.9.2. Creación de un plan de respuesta a incidentes
- 2.9.3. Coordinación con equipos de seguridad

2.10. Presentación de evidencia y jurídico
- 2.10.1. Reglas de evidencia digital en el ámbito legal
- 2.10.2. Preparación de informes forenses
- 2.10.3. Comparecencia en juicio como testigo experto

Módulo 3. Ejercicios de *Red Team* Avanzados

3.1. Técnicas avanzadas de reconocimiento
- 3.1.1. Enumeración avanzada de subdominios
- 3.1.2. *Google Dorking* avanzado
- 3.1.3. Redes Sociales y theHarvester

3.2. Campañas de *phishing* avanzadas
- 3.2.1. Qué es *Reverse-Proxy Phishing*
- 3.2.2. *2FA Bypass* con Evilginx
- 3.2.3. Exfiltración de datos

3.3. Técnicas avanzadas de persistencia
- 3.3.1. *Golden Tickets*
- 3.3.2. *Silver Tickets*
- 3.3.3. Técnica *DCShadow*

3.4. Técnicas avanzadas de evasión
- 3.4.1. *Bypass* de AMSI
- 3.4.2. Modificación de herramientas existentes
- 3.4.3. Ofuscación de *Powershell*

3.5. Técnicas avanzadas de movimiento lateral
- 3.5.1. *Pass-the-Ticket* (PtT)
- 3.5.2. *Overpass-the-Hash (Pass-the-Key)*
- 3.5.3. NTLM Relay

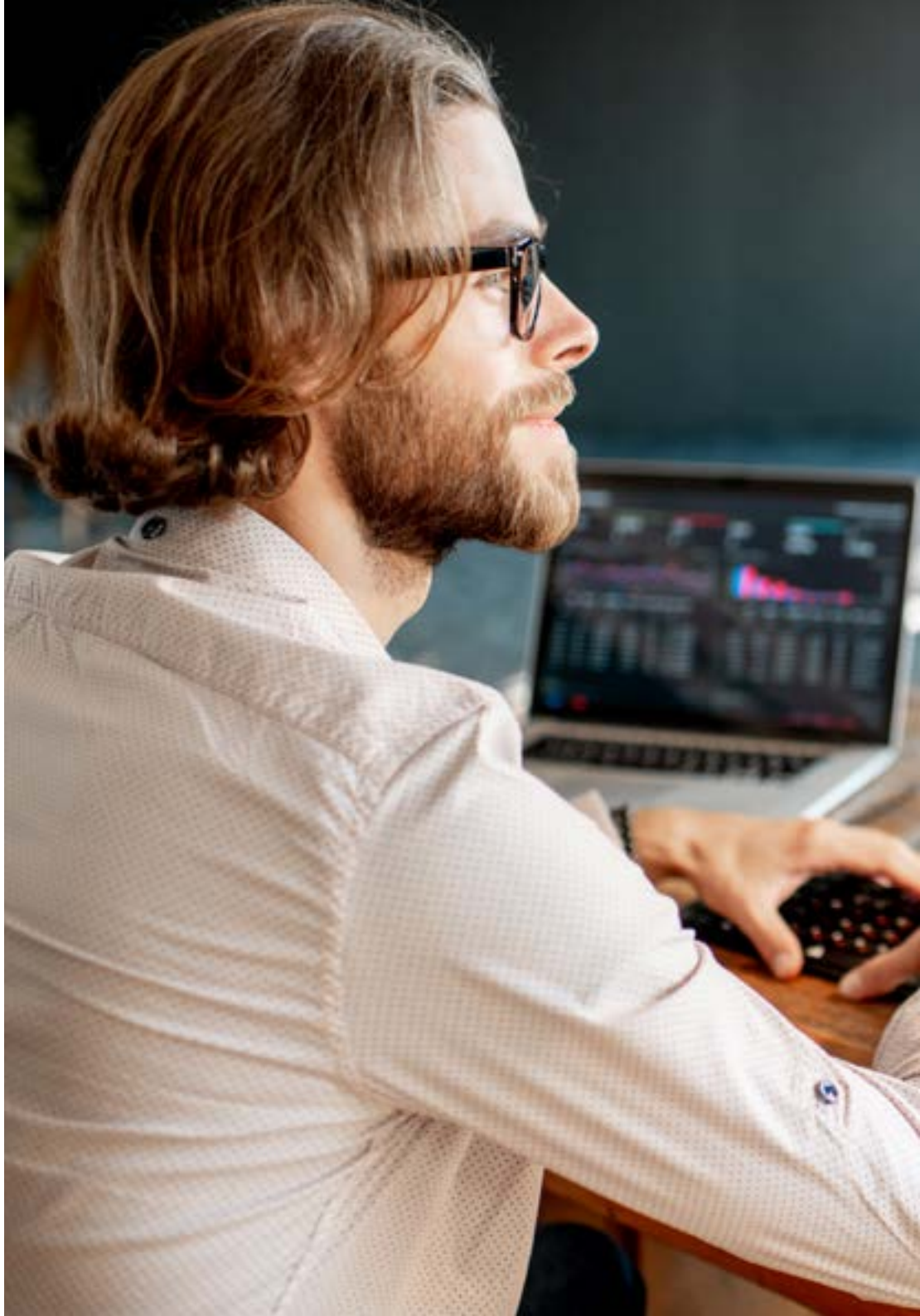
3.6. Técnicas avanzadas de post-explotación
- 3.6.1. *Dump* de LSASS
- 3.6.2. *Dump* de SAM
- 3.6.3. Ataque *DCSync*

3.7. Técnicas avanzadas de *pivoting*
- 3.7.1. Qué es el *pivoting*
- 3.7.2. Túneles con SSH
- 3.7.3. *Pivoting* con Chisel

3.8. Intrusiones físicas
- 3.8.1. Vigilancia y reconocimiento
- 3.8.2. *Tailgating y Piggybacking*
- 3.8.3. *Lock-Picking*

3.9. Ataques Wi-Fi
- 3.9.1. Ataques a WPA/WPA2 PSK
- 3.9.2. Ataques de Rogue AP
- 3.9.3. Ataques a WPA2 *Enterprise*

3.10. Ataques RFID
- 3.10.1. Lectura de tarjetas RFID
- 3.10.2. Manipulación de tarjetas RFID
- 3.10.3. Creación de tarjetas clonadas



No dejes pasar esta oportunidad para impulsar tu carrera mediante este programa innovador. ¡Conviértete en un experto en Ciberseguridad!”

04

Metodología de estudio

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

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

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

El alumno: la prioridad de todos los programas de TECH

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

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

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

Los planes de estudios más exhaustivos a nivel internacional

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

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

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

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

Case studies o Método del caso

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

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

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

Método *Relearning*

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

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

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

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

Un Campus Virtual 100% online con los mejores recursos didácticos

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

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

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

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

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

La eficacia del método se justifica con cuatro logros fundamentales:

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

La metodología universitaria mejor valorada por sus alumnos

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

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

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

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

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

Material de estudio

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

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

Prácticas de habilidades y competencias

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

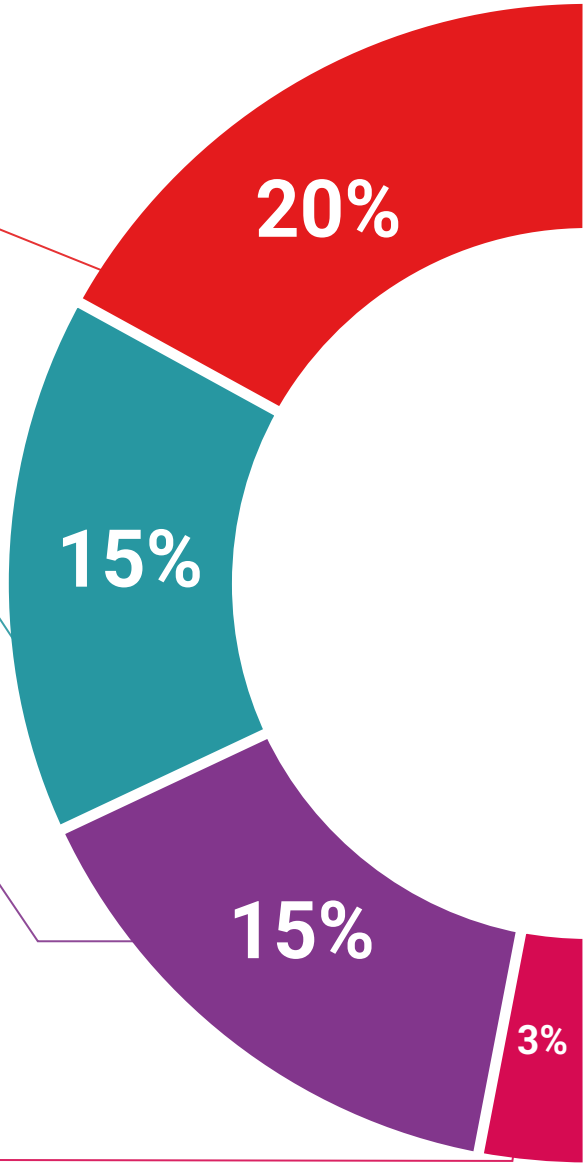
Resúmenes interactivos

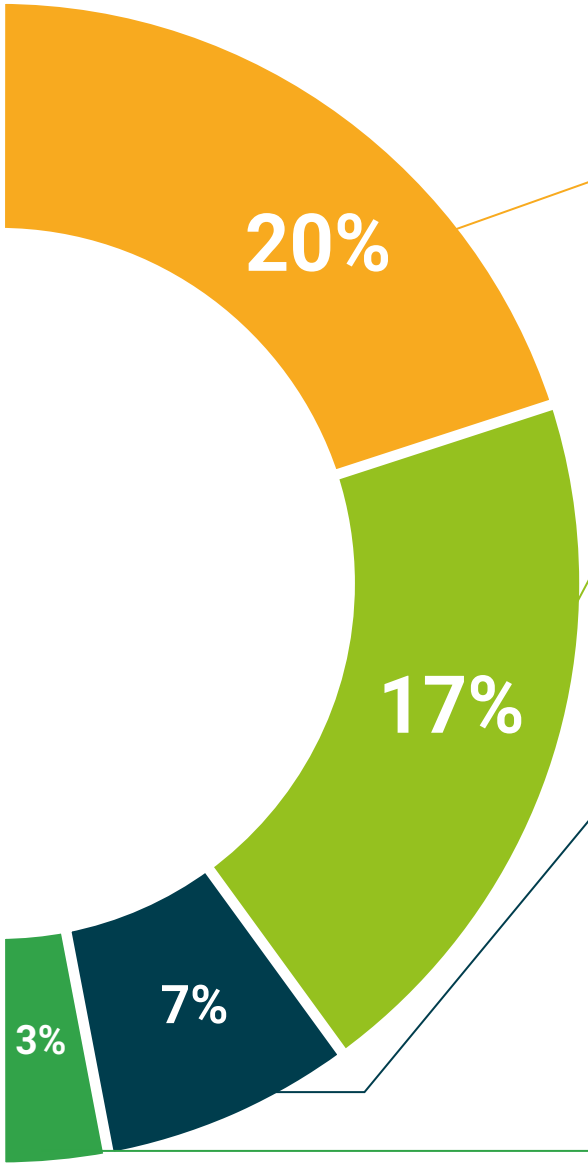
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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

Lecturas complementarias

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





Case Studies

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

Testing & Retesting

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

Clases magistrales

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

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

Guías rápidas de actuación

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

06

Titulación

El Experto Universitario en Ciberseguridad Red Team 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 Red Team** 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 Red Team**

Modalidad: **online**

Duración: **6 meses**


tech universidad

C. _____, con documento de identificación _____ ha superado con éxito y obtenido el título de:

Experto Universitario en Ciberseguridad Red Team

Se trata de un título propio de esta Universidad con una duración de 450 horas, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH es una Institución Particular de Educación Superior reconocida por la Secretaría de Educación Pública a partir del 28 de junio de 2018.

En Ciudad de México, a 31 de mayo de 2024

Mtro. Gerardo Daniel Orozco Martínez
Rector

código único TECH: AFWOR23S techtitute.com/titulos

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

tech universidad

Experto Universitario
Ciberseguridad Red Team

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

Experto Universitario
Ciberseguridad Red Team

tech universidad