Experto Universitario
Hacking Web Avanzado

tech universidad

tech universidad

Experto Universitario
Hacking Web Avanzado

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

Acceso web: **www.techtitute.com/informatica/experto-universitario/experto-hacking-web-avanzado**

Índice

01

Presentación

A medida que las instituciones se expanden digitalmente, cada vez emplean más la tecnología para almacenar datos confidenciales. Así, el *Hacking* Avanzado se convierte en una grave amenaza para las instituciones. Si los *hackers* acceden a sus sitios web, las consecuencias pueden ser nefastas, acarreando desde el robo de identidad hasta el fraude financiero y el chantaje. Por eso, es importante que las compañías cuenten con expertos en medidas de seguridad avanzadas, para la implementación de medidas como *firewalls*. Ante esto, TECH lanza un innovador programa para que el alumnado domine las técnicas más eficaces en materia de ciberseguridad. Además, se basa en una modalidad 100% online, garantizando la comodidad y la flexibilidad horaria.

Transformarás cualquier empresa en un entorno seguro, libre de amenazas cibernéticas, gracias a este Experto Universitario”

Los especialistas informáticos son un valioso intangible para las organizaciones actuales. Uno de los principales motivos es que las auditorías que realizan regularmente contribuyen a identificar y abordar posibles vulnerabilidades anticipadamente. De esta forma, se adelantan a los delitos que puedan cometer los *hackers*, mientras convierten los entornos virtuales en zonas seguras.

De esta forma, los usuarios tienen la garantía de navegar con seguridad y libremente por su red y adquirir tanto sus bienes como servicios. Sin embargo, en vista del incremento de estas prácticas, los informáticos se enfrentan al desafío de actualizar sus conocimientos constantemente, implementando las técnicas más revolucionarias para afrontarlos.

En este contexto, TECH ha desarrollado el Experto Universitario en *Hacking Web* Avanzado más completo del mercado académico. Mediante esta programación, los egresados estarán a la vanguardia en ciberseguridad y dispondrán de un amplio abanico de tácticas para proteger la información restringida. Además, se profundizará en las estrategias de explotación de vulnerabilidades sofisticadas.

Asimismo, el profesional se centrará en instaurar medidas de seguridad efectivas, como los sistemas de detección de intrusiones. También se enfatizará en el *switching* para interconectar los equipos de todas las secciones del organigrama en una misma red. Igualmente, se brindarán las claves para la redacción de reportes técnicos y ejecutivos. En este sentido, se ahondará en cómo exponer los datos sensibles, enfocando el informe a los clientes. Finalmente, se indagará en diversas metodologías, destinadas a la medición de la seguridad operativa real.

Para afianzar el dominio de los contenidos, esta capacitación aplica el innovador sistema *Relearning*, que promueve la asimilación de conceptos complejos a través de la reiteración natural y progresiva de los mismos. De igual forma, el programa se nutre de materiales en diversos formatos, como las infografías o los vídeos explicativos. Todo ello en una cómoda modalidad 100% online, que permite ajustar los horarios de cada persona a sus responsabilidades.

Este **Experto Universitario en Hacking Web Avanzado** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en Hacking Web Avanzado
- 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

Descifrarás contraseñas que se han almacenado en los equipos y anticiparás los ataques de hackers"

Explorarás el modelo OSI y entenderás los procesos de comunicación en los sistemas de redes. ¡Y en tan solo 6 meses!"

Profundizarás en las vulnerabilidades de DOM e impedirás los ataques avanzados con las estrategias más efectivas.

¡Olvídate de memorizar! Con la metodología 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 presente plan de estudio profundizará en las técnicas avanzadas de hacking dirigidas a servicios web, permitiendo a los profesionales aplicar las estrategias más eficaces, antes de que se produzcan los ataques informáticos. Para conseguirlo, se analizarán los principios fundamentales del diseño de redes y se identificarán las debilidades comunes. De este modo, los egresados ofrecerán las soluciones más innovadoras y destacarán en un sector digital que avanza a pasos agigantados.

¿Quieres asegurar la red y los datos transmitido en ella? Domina el switching con la mejor universidad digital del mundo, según Forbes"

Objetivos generales

- 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

Aplicarás las medidas de seguridad más afectivas y evitarás vulnerabilidades como el Broken Authentication. ¡Matricúlate ahora!"

Objetivos específicos

Módulo 1. Hacking Web Avanzado

- Desarrollar habilidades para identificar y evaluar vulnerabilidades en aplicaciones web, incluyendo inyecciones SQL, Cross-Site Scripting (XSS) y otros vectores de ataque comunes
- Aprender a realizar pruebas de seguridad en aplicaciones web modernas
- Adquirir competencias en técnicas avanzadas de hacking web, explorando estrategias de evasión de medidas de seguridad y explotación de vulnerabilidades sofisticadas
- 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
- Desarrollar habilidades para implementar medidas de mitigación efectivas en aplicaciones web, reduciendo la exposición a ataques y fortaleciendo la seguridad
- Participar en simulaciones prácticas para evaluar la seguridad en entornos web complejos, aplicando conocimientos en situaciones del mundo real
- Desarrollar competencias en la formulación de estrategias de defensa efectivas para proteger aplicaciones web contra amenazas cibernéticas
- Aprender a lineal las prácticas de hacking web avanzado con las normativas y estándares de seguridad relevantes, asegurando la adhesión a marcos legales y éticos
- Fomentar la colaboración efectiva entre equipos de desarrollo y seguridad

Módulo 2. Arquitectura y Seguridad en Redes

- Adquirir conocimientos avanzados sobre la arquitectura de redes, incluyendo topologías, protocolos y componentes clave
- Desarrollar habilidades para identificar y evaluar vulnerabilidades específicas en infraestructuras de red, considerando amenazas potenciales
- Aprender a implementar medidas de seguridad efectivas en redes, incluyendo firewalls, sistemas de detección de intrusiones (IDS) y segmentación de red
- Familiarizar al estudiante con tecnologías emergentes en redes, como redes definidas por software (SDN), y comprender su impacto en la seguridad
- Desarrollar habilidades para asegurar las comunicaciones en redes, incluyendo la protección contra amenazas como sniffing y ataques de intermediarios
- Aprender a evaluar y mejorar las configuraciones de seguridad en entornos de redes empresariales, garantizando la protección adecuada
- Desarrollar habilidades para implementar medidas de mitigación efectivas contra amenazas en redes empresariales, desde ataques internos hasta amenazas externas
- Fomentar la colaboración efectiva con equipos de seguridad, integrando estrategias y esfuerzos para proteger la infraestructura de red
- Promover prácticas éticas y legales en la implementación de medidas de seguridad en redes, asegurando la adhesión a principios éticos en todas las actividades

Módulo 3. Reporte Técnico y Ejecutivo

- Desarrollar habilidades para elaborar informes técnicos detallados, presentando de manera clara y completa los hallazgos, metodologías utilizadas y recomendaciones
- Aprender a comunicar de manera efectiva con audiencias técnicas, utilizando un lenguaje preciso y adecuado para transmitir información técnica compleja
- Desarrollar habilidades para formular recomendaciones accionables y prácticas, orientadas a mitigar vulnerabilidades y mejorar la postura de seguridad
- Aprender a evaluar el impacto potencial de las vulnerabilidades identificadas, considerando aspectos técnicos, operativos y estratégicos
- Familiarizar al alumno con las mejores prácticas para la presentación ejecutiva de informes, adaptando la información técnica para audiencias no técnicas
- Desarrollar competencias para alinear los hallazgos y recomendaciones con los objetivos estratégicos y operativos de la organización
- Aprender a utilizar herramientas de visualización de datos para representar gráficamente la información contenida en los informes, facilitando la comprensión
- Promover la inclusión de información relevante sobre el cumplimiento de normativas y estándares en los informes, garantizando la adhesión a requisitos legales
- Fomentar la colaboración efectiva entre equipos técnicos y ejecutivos, asegurando la comprensión y apoyo para las acciones de mejora propuestas en el informe

03

Dirección del curso

Con el objetivo de ofrecer la excelencia educativa, TECH ha reunido a un equipo docente con un amplio bagaje profesional en ciberseguridad. Con más de 13 años de experiencia, estos especialistas ofrecerán el enfoque más integral y las herramientas más novedosas para desarrollar entornos virtuales seguros. De esta manera, los estudiantes contarán con las garantías que requieren para especializarse en un sector digital que ofrece múltiples oportunidades.

Profundizarás en los límites del Pentester con el respaldo del mejor cuadro docente. ¡Tus actividades serán 100% legales!"

Dirección

D. Gómez Pintado, Carlos

- Gerente de Ciberseguridad y Red Team Cipherbit en Grupo Oesía
- Gerente *Advisor & Investo*r 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. 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

Adquirirás conocimientos sin limitaciones geográficas o timing preestablecido"

04

Estructura y contenido

El presente programa abarca 3 completos módulos: *Hacking Web* Avanzado; Arquitectura y Seguridad en Redes; y Reporte Técnico y Ejecutivo. Con el apoyo de un veterano claustro docente, se abordarán tácticas avanzadas para asegurar las redes empresariales mediante la implementación de *firewalls*. También se profundizará en la detección de intrusiones, entre las que sobresale el HHTP *Request Smuggling*. Asimismo, se analizará la importancia de contar con VLANs para separar el tráfico de datos en un mismo entorno virtual, y se indagará en el proceso de reporte, con el fin de presentar informes de forma precisa y detallada.

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. Hacking Web Avanzado

1.1. Funcionamiento de una web
- 1.1.1. La URL y sus partes
- 1.1.2. Los métodos HTTP
- 1.1.3. Las cabeceras
- 1.1.4. Cómo ver peticiones web con Burp Suite

1.2. Sesiones
- 1.2.1. Las *cookies*
- 1.2.2. *Tokens* JWT
- 1.2.3. Ataques de robo de sesión
- 1.2.4. Ataques a JWT

1.3. *Cross Site Scripting* (XSS)
- 1.3.1. Qué es un XSS
- 1.3.2. Tipos de XSS
- 1.3.3. Explotando un XSS
- 1.3.4. Introducción a los *XSLeaks*

1.4. Inyecciones a bases de datos
- 1.4.1. Qué es una *SQL Injection*
- 1.4.2. Exfiltrando información con *SQLi*
- 1.4.3. *SQLi Blind, Time-Based y Error-Based*
- 1.4.4. Inyecciones NoSQLi

1.5. Path Traversal y Local File Inclusion
- 1.5.1. Qué son y sus diferencias
- 1.5.2. Filtros comunes y cómo saltarlos
- 1.5.3. *Log Poisoning*
- 1.5.4. LFIs en PHP

1.6. *Broken Authentication*
- 1.6.1. *User Enumeration*
- 1.6.2. *Password Bruteforce*
- 1.6.3. *2FA Bypass*
- 1.6.4. *Cookies* con información sensible y modificable

1.7. *Remote Command Execution*
- 1.7.1. *Command Injection*
- 1.7.2. *Blind Command Injection*
- 1.7.3. *Insecure Deserialization* PHP
- 1.7.4. *Insecure Deserialization* Java

1.8. *File Uploads*
- 1.8.1. RCE mediante *webshells*
- 1.8.2. XSS en subidas de ficheros
- 1.8.3. XML *External Entity* (XXE) *Injection*
- 1.8.4. *Path traversal* en subidas de fichero

1.9. *Broken Acess Control*
- 1.9.1. Acceso a paneles sin restricción
- 1.9.2. *Insecure Direct Object References* (IDOR)
- 1.9.3. *Bypass* de filtros
- 1.9.4. Métodos de autorización insuficientes

1.10. Vulnerabilidades de DOM y ataques más avanzados
- 1.10.1. *Regex Denial of Service*
- 1.10.2. DOM *Clobbering*
- 1.10.3. *Prototype Pollution*
- 1.10.4. HTTP *Request Smuggling*

Módulo 2. Arquitectura y Seguridad en Redes

2.1. Las redes informáticas
- 2.1.1. Conceptos básicos: Protocolos LAN, WAN, CP, CC
- 2.1.2. Modelo OSI y TCP/IP
- 2.1.3. *Switching:* Conceptos básicos
- 2.1.4. *Routing:* Conceptos básicos

2.2. *Switching*
- 2.2.1. Introducción a VLAN's
- 2.2.2. STP
- 2.2.3. *EtherChannel*
- 2.2.4. Ataques a capa 2

2.3. VLAN´s
- 2.3.1. Importancia de las VLAN's
- 2.3.2. Vulnerabilidades en VLAN's
- 2.3.3. Ataques comunes en VLAN's
- 2.3.4. Mitigaciones

2.4. *Routing*
- 2.4.1. Direccionamiento IP- IPv4 e IPv6
- 2.4.2. Enrutamiento: Conceptos Clave
- 2.4.3. Enrutamiento Estático
- 2.4.4. Enrutamiento Dinámico: Introducción

2.5. Protocolos IGP
- 2.5.1. RIP
- 2.5.2. OSPF
- 2.5.3. RIP vs OSPF
- 2.5.4. Análisis de necesidades de la topología

2.6. Protección perimetral
- 2.6.1. DMZs
- 2.6.2. *Firewalls*
- 2.6.3. Arquitecturas comunes
- 2.6.4. Zero Trust Network Access

2.7. IDS e IPS
- 2.7.1. Características
- 2.7.2. Implementación
- 2.7.3. SIEM y SIEM CLOUDS
- 2.7.4. Detección basada en *HoneyPots*

2.8. TLS y VPN´s
- 2.8.1. SSL/TLS
- 2.8.2. TLS: Ataques comunes
- 2.8.3. VPNs con TLS
- 2.8.4. VPNs con IPSEC

2.9. Seguridad en redes inalámbricas
- 2.9.1. Introducción a las redes inalámbricas
- 2.9.2. Protocolos
- 2.9.3. Elementos claves
- 2.9.4. Ataques comunes

2.10. Redes empresariales y cómo afrontarlas
- 2.10.1. Segmentación lógica
- 2.10.2. Segmentación física
- 2.10.3. Control de acceso
- 2.10.4. Otras medidas a tomar en cuenta

Módulo 3. Reporte Técnico y Ejecutivo

3.1. Proceso de reporte
- 3.1.1. Estructura de un reporte
- 3.1.2. Proceso de reporte
- 3.1.3. Conceptos clave
- 3.1.4. Ejecutivo vs Técnico

3.2. Guías
- 3.2.1. Introducción
- 3.2.2. Tipos de Guías
- 3.2.3. Guías nacionales
- 3.2.4. Casos de uso

3.3. Metodologías
- 3.3.1. Evaluación
- 3.3.2. *Pentesting*
- 3.3.3. Repaso de metodologías comunes
- 3.3.4. Introducción a metodologías nacionales

3.4. Enfoque técnico de la fase de reporte
- 3.4.1. Entendiendo los límites del *pentester*
- 3.4.2. Uso y claves del lenguaje
- 3.4.3. Presentación de la información
- 3.4.4. Errores comunes

3.5. Enfoque ejecutivo de la fase de reporte
- 3.5.1. Ajustando el informe al contexto
- 3.5.2. Uso y claves del lenguaje
- 3.5.3. Estandarización
- 3.5.4. Errores comunes

3.6. OSSTMM
- 3.6.1. Entendiendo la metodología
- 3.6.2. Reconocimiento
- 3.6.3. Documentación
- 3.6.4. Elaboración del informe

3.7. LINCE
- 3.7.1. Entendiendo la metodología
- 3.7.2. Reconocimiento
- 3.7.3. Documentación
- 3.7.4. Elaboración del informe

3.8. Reportando vulnerabilidades
- 3.8.1. Conceptos clave
- 3.8.2. Cuantificación del alcance
- 3.8.3. Vulnerabilidades y evidencias
- 3.8.4. Errores comunes

3.9. Enfocando el informe al cliente
- 3.9.1. Importancia de las pruebas de trabajo
- 3.9.2. Soluciones y mitigaciones
- 3.9.3. Datos sensibles y relevantes
- 3.9.4. Ejemplos prácticos y casos

3.10. Reportando *retakes*
- 3.10.1. Conceptos claves
- 3.10.2. Entendiendo la información heredada
- 3.10.3. Comprobación de errores
- 3.10.4. Añadiendo información

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 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 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

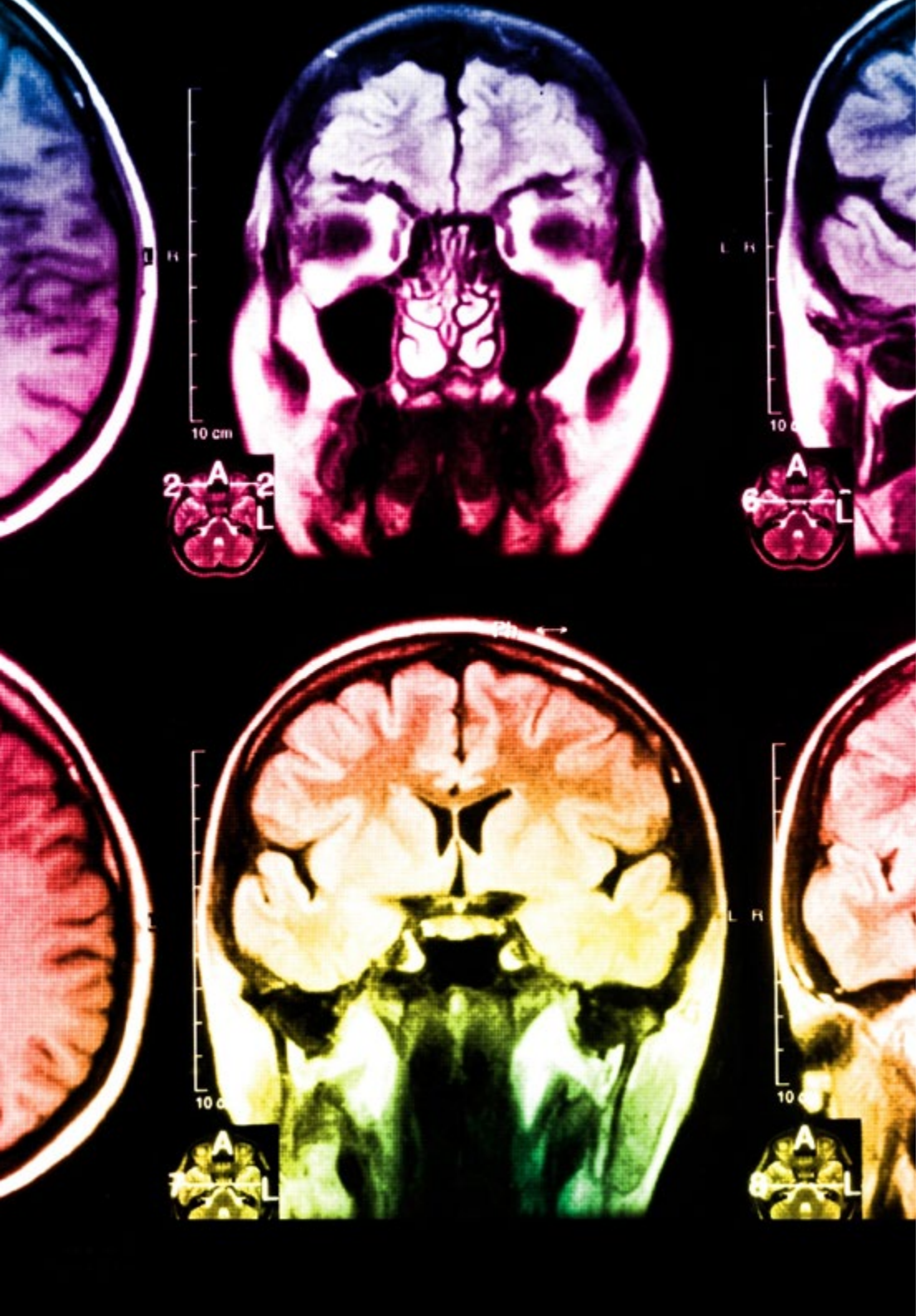
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

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.

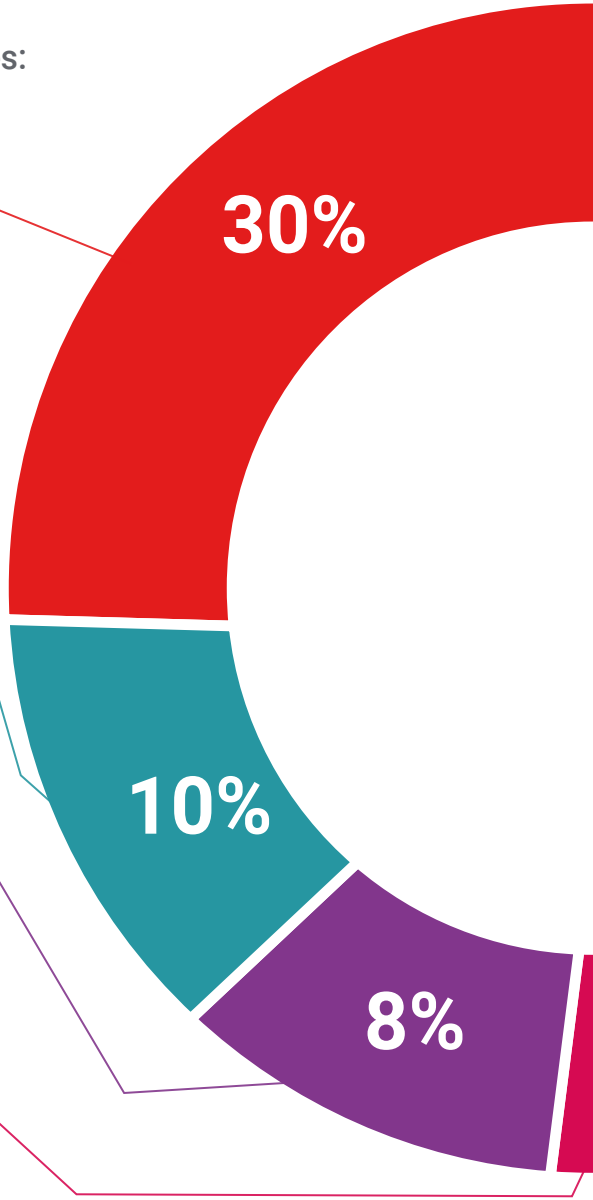
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

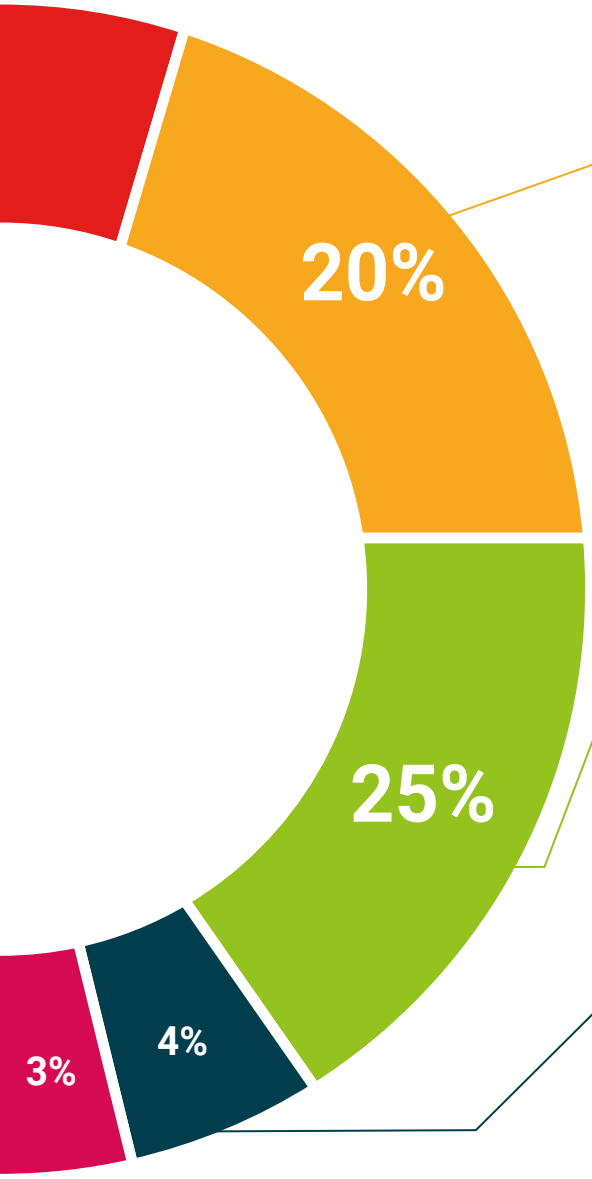
Prácticas de habilidades y competencias

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 Experto Universitario en Hacking Web Avanzado 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 Hacking Web Avanzado** contiene el programa científico 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 Hacking Web Avanzado**

Modalidad: **om+nline**

Duración: **6 meses**


tech universidad

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

Experto Universitario en Hacking Web Avanzado

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
Hacking Web Avanzado

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

Experto Universitario
Hacking Web Avanzado

tech universidad