# Diplomado
## Hacking Ético



tech universidad tecnológica



tech universidad tecnológica

# Diplomado

## Hacking Ético

Modalidad: **Online**
Duración: **6 semanas**
Titulación: **TECH Universidad Tecnológica**
Horas lectivas: **150 h.**
Acceso web: **www.techtitute.com/informatica/curso-universitario/hacking-etico**

# Índice


01 Presentación — pág. 4

02 Objetivos — pág. 8

03 Dirección de curso — pág. 12

04 Estructura y contenido — pág. 16

05 Metodología — pág. 20

06 Titulación — pág. 28

01

# Presentación

La ciberprotección se ha convertido en una prioridad para particulares y empresas. Cuanto más innovadoras y desarrolladas son las funcionalidades de los dispositivos, más sofisticadas y peligrosas son las amenazas que afectas a los mismos y, por consecuencia, los datos de sus usuarios. Generar herramientas que se vayan adaptando a las variaciones de la amenaza implica el uso de tecnologías, *hacking* y planteamientos que proporcionen una cobertura de seguridad adecuada. Este programa es la forma más completa y de mayor calidad del mercado docente online para conseguir la capacitación más amplia en este campo de actuación.





*Aprende a detectar las vulnerabilidades de un sistema realizando ataques preventivos que demuestren las brechas y consigue datos de inestimable valor en ciberseguridad”*

En la actualidad ninguna empresa está exenta de sufrir un ciberataque y, por tanto, padecer las diferentes consecuencias que implica. Independientemente del tamaño de la misma, está expuesta a robos de información, chantajes, sabotajes, etc.

Es necesario realizar un estudio de vulnerabilidades y determinar la superficie de ataque, por lo que cada vez más se van a realizar estudios periódicos de vulnerabilidades y riesgos. Cada empresa tendrá que ver si cumple con las normas y legislación del país conde está ubicada y ser consciente de los daños ocasionados tanto monetarios como otros daños inmateriales, por ejemplo, su reputación.

En este módulo se presentan las distintas herramientas y metodologías para hacer frente a esta necesidad y, por tanto, proporciona un conjunto extenso de conocimientos especializados para llevar a cabo este trabajo.

Este **Diplomado de Hacking Ético** contiene el programa más completo y actualizado del mercado. Las características más destacadas son:

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

*Las formas más innovadoras y eficientes de crear sistemas de protección que garanticen la ciberseguridad en los dispositivos”*

*Estudia a través de un Diplomado centrado en la práctica impulsando tu capacidad hasta el nivel de un especialista"*

*Conoce a fondo las principales amenazas y las herramientas más innovadoras y actualizadas en la lucha contra los ciberataques a través de este excepcional programa.*

*Un proceso de alta capacitación creado para ser asumible y flexible, con la metodología más interesante de la docencia online.*

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 programa académico. Para ello, contará con la ayuda de un novedoso sistema de vídeos interactivos realizados por reconocidos expertos.

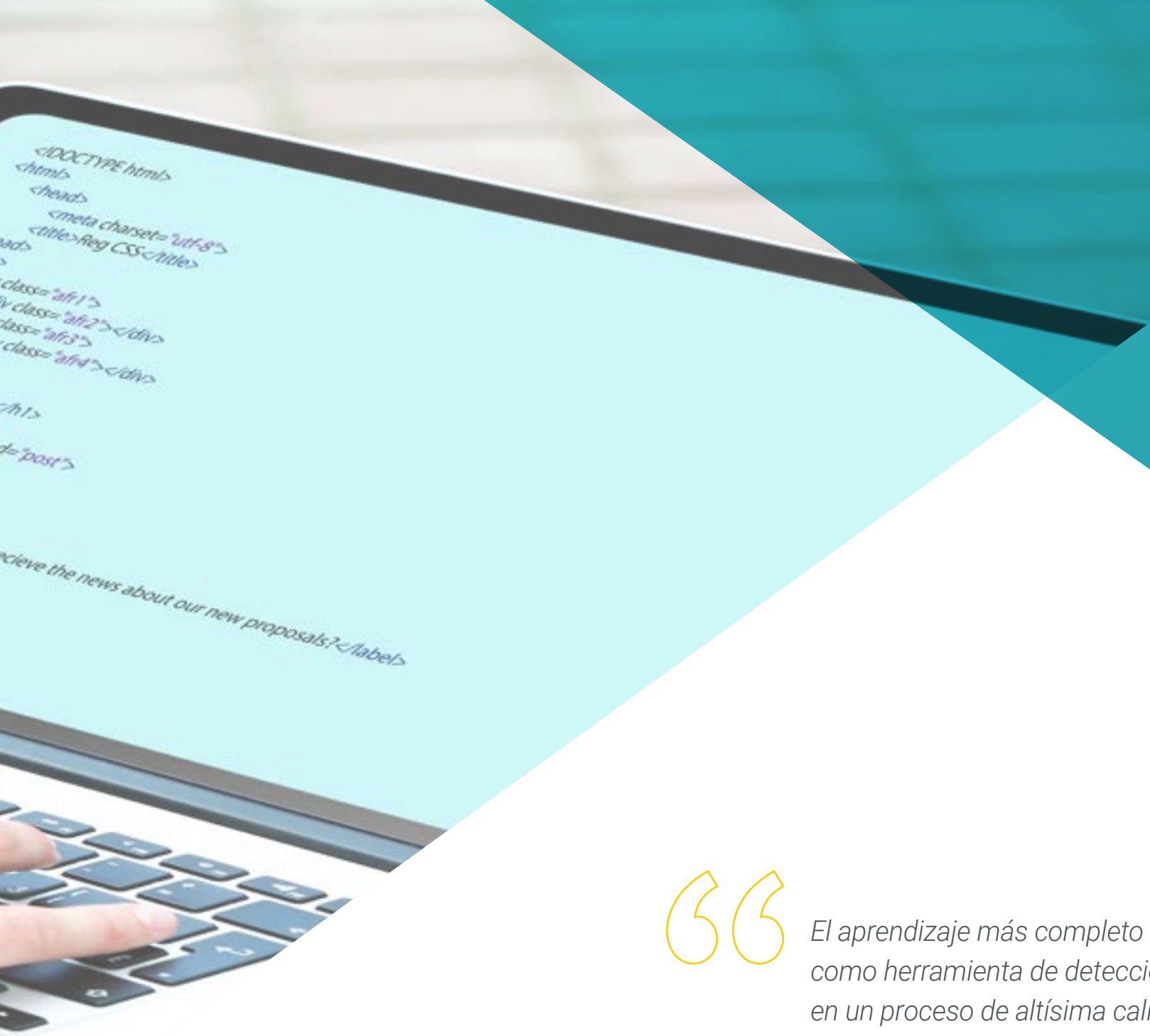


02

# Objetivos

El Diplomado en Hacking Ético, proporciona capacidad de trabajo en este campo del alumnado, de forma rápida y sencilla. Con objetivos realistas y de alto interés, este proceso de estudio se ha configurado para llevar al alumnado, de forma progresiva a la adquisición de los conocimientos teóricos y prácticos necesarios para intervenir con calidad desarrollando, además, competencias transversales que permitirán afrontar situaciones complejas elaborando respuestas ajustadas y precisas.






*El aprendizaje más completo acerca del hacking ético como herramienta de detección de vulnerabilidades, en un proceso de altísima calidad"*

## Objetivos generales

- Analizar los diferentes sistemas existentes
- Evaluar la información obtenida y desarrollar mecanismos de prevención y *hacking*
- Establecer prioridades en el estudio y resolución de las vulnerabilidades
- Demostrar que un sistema es vulnerable, atacarlo con fines preventivos y solventar dichos problemas







## Objetivos específicos

- Examinar los métodos de IOSINT
- Recopilar la información disponible en medios públicos
- Escanear redes para obtener información de modo activo

*Pensando en el alumno, este Diplomado pone en marcha los sistemas de apoyo al estudio más interesantes del momento"*

03

# Dirección del curso

Los docentes que imparten este programa han sido seleccionados por su excepcional competencia en este campo. Combinan la experiencia técnica y práctica con la docente, ofreciendo al alumnado un apoyo de primer nivel en la consecución de sus metas. A través de ellos, el Diplomado ofrece la visión más directa e inmediata de las características reales de la intervención en este campo consiguiendo una visión contextual del máximo interés.





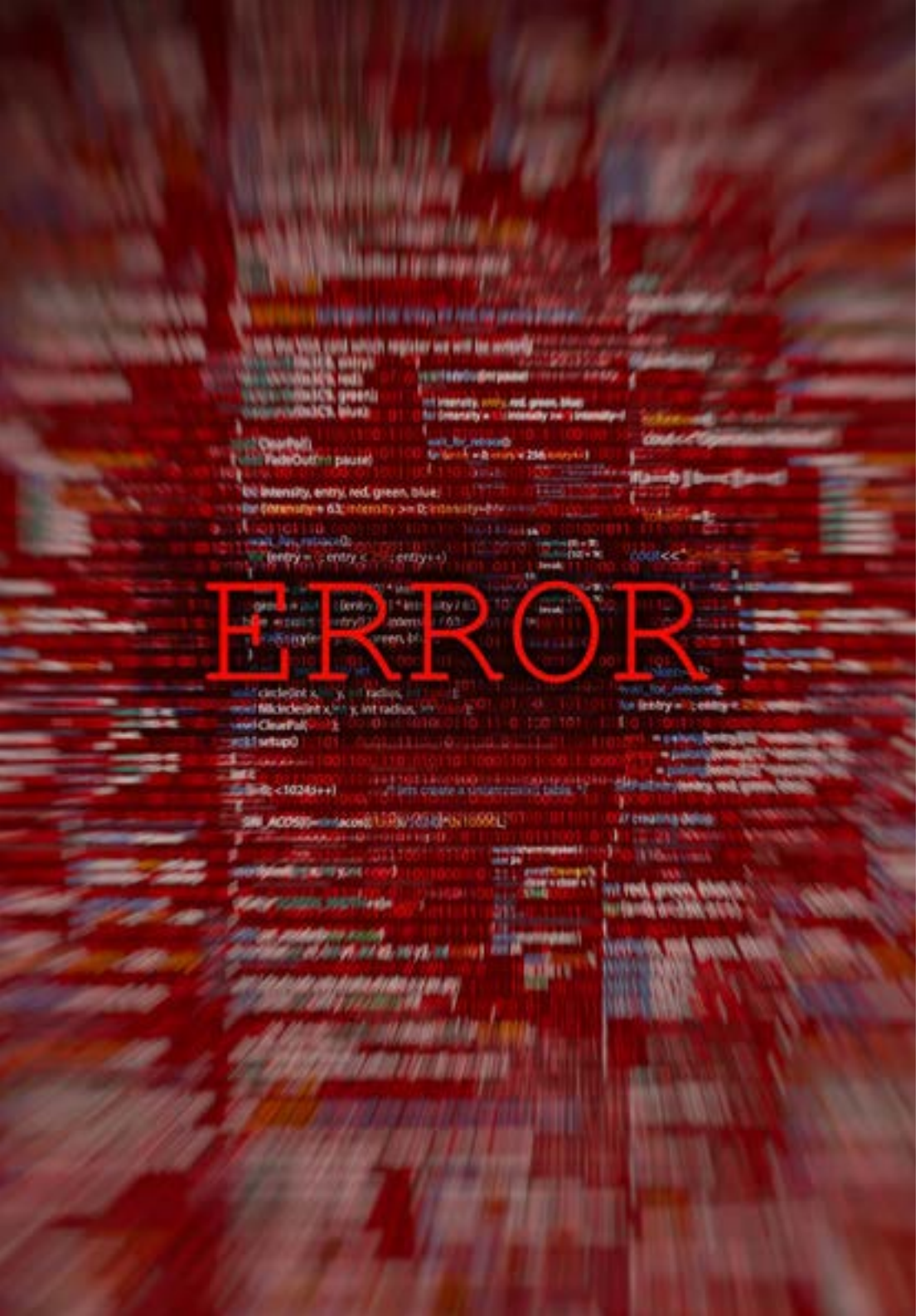
*Docentes expertos en Hacking Ético te dotarán de la visión amplia y contextual que necesitas para trabajar con precisión en ciberseguridad”*

## Dirección



### Dña. Fernández Sapena, Sonia

- Formadora de Seguridad Informática y Hacking Ético. Centro de Referencia Nacional de Getafe en Informática y Telecomunicaciones. Madrid
- Instructora certificada E-Council. Madrid
- Formadora en las siguientes certificaciones: EXIN Ethical Hacking Foundation y EXIN Cyber & IT Security Foundation. Madrid
- Formadora acreditada experta por la CAM de los siguientes certificados de profesionalidad: Seguridad Informática (IFCT0190), Gestión de Redes de Voz y datos (IFCM0310), Administración de Redes departamentales (IFCT0410), Gestión de Alarmas en redes de telecomunicaciones (IFCM0410), Operador de Redes de voz y datos (IFCM0110), y Administración de servicios de internet (IFCT0509)
- Colaboradora externa CSO/SSA (Chief Security Officer/Senior Security Architect). Universidad de las Islas Baleares
- Ingeniera en Informática. Universidad de Alcalá de Henares. Madrid
- Máster en DevOps: Docker and Kubernetes. Cas-Training. Madrid
- Microsoft Azure Security Techonologies. E-Council. Madrid




*Amplía tus estudios de la mano de los mejores especialistas en la materia”*

04

# Estructura y contenido

A lo largo del desarrollo de los diferentes temas de este Diplomado el alumno podrá adquirir todos los conocimientos que el uso del hacking Ético necesita para ser utilizado como herramienta. Para ello se ha estructurado con vistas a la adquisición eficiente de aprendizajes complementarios, que propicien la penetración de los aprendizajes y consoliden lo estudiado dotando al alumnado de capacidad de intervención de la manera más rápida posible. Un recorrido de alta intensidad y enorme calidad creado para capacitar a los mejores del sector.





*Un Diplomado desarrollado de forma estructurada a través de un planteamiento de estudio centrado en la eficiencia"*

## **Módulo 1.** Hacking Ético

1.1. Entorno de trabajo
- 1.1.1. Distribuciones Linux
  - 1.1.1.1. Kali Linux - Offensive Security
  - 1.1.1.2. Parrot OS
  - 1.1.1.3. Ubuntu
- 1.1.2. Sistemas de virtualización
- 1.1.3. Sandbox
- 1.1.4. Despliegue de laboratorios

1.2. Metodologías
- 1.2.1. OSSTMM
- 1.2.2. OWASP
- 1.2.3. NIST
- 1.2.4. PTES
- 1.2.5. ISSAF

1.3. Footprinting
- 1.3.1. Inteligencia de fuentes abiertas (OSINT)
- 1.3.2. Búsqueda de brechas y vulnerabilidades de datos
- 1.3.3. Uso de herramientas pasivas

1.4. Escaneo de redes
- 1.4.1. Herramientas de escaneo
  - 1.4.1.1. Nmap
  - 1.4.1.2. Hping3
  - 1.4.1.3. Otras herramientas de escaneo
- 1.4.2. Técnicas de escaneo
- 1.4.3. Técnicas de evasión de *firewall* e IDS
- 1.4.4. Banner *grabbing*
- 1.4.5. Diagramas de red

1.5. Enumeración
- 1.5.1. Enumeración SMTP
- 1.5.2. Enumeración DNS
- 1.5.3. Enumeración de NetBIOS y Samba
- 1.5.4. Enumeración de LDAP
- 1.5.5. Enumeración de SNMP
- 1.5.6. Otras técnicas de Enumeración



1.6. Análisis de vulnerabilidades
- 1.6.1. Soluciones de Análisis de vulnerabilidades
  - 1.6.1.1. Qualys
  - 1.6.1.2. Nessus
  - 1.6.1.3. CFI LanGuard
- 1.6.2. Sistemas de puntuación de Vulnerabilidades
  - 1.6.2.1. CVSS
  - 1.6.2.2. CVE
  - 1.6.2.3. NVD

1.7. Ataques a redes inalámbrica
- 1.7.1. Metodología de *hacking* en redes inalámbricas
  - 1.7.1.1. Wifi *discovery*
  - 1.7.1.2. Análisis de tráfico
  - 1.7.1.3. Ataques del *aircrack*
    - 1.7.1.3.1. Ataques WEP
    - 1.7.1.3.2. Ataques WPA/WPA2
  - 1.7.1.4. Ataques de Evil Twin
  - 1.7.1.5. Ataques a WPS
  - 1.7.1.6. *Jamming*
- 1.7.2. Herramientas para la seguridad inalámbrica

1.8. Hackeo de servidores webs
- 1.8.1. *Cross site scripting*
- 1.8.2. CSRF
- 1.8.3. *Session hijacking*
- 1.8.4. SQL *injection*

1.9. Explotación de vulnerabilidades
- 1.9.1. Uso de *exploits* conocidos
- 1.9.2. Uso de *metasploit*
- 1.9.3. Uso de *malware*
  - 1.9.3.1. Definición y alcance
  - 1.9.3.2. Generación de *malware*
  - 1.9.3.3. Bypass de soluciones antivirus

1.10. Persistencia
- 1.10.1. Instalación de *rootkits*
- 1.10.2. Uso de Ncat
- 1.10.3. Uso de tareas programadas para *Backdoors*
- 1.10.4. Creación de usuarios
- 1.10.5. Detección de HIDS

*Todo lo que el profesional de la ciberseguridad tiene que saber esta organizado en un temario completo que impulsará tu capacidad de forma progresiva y constante hasta el máximo nivel”*

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.

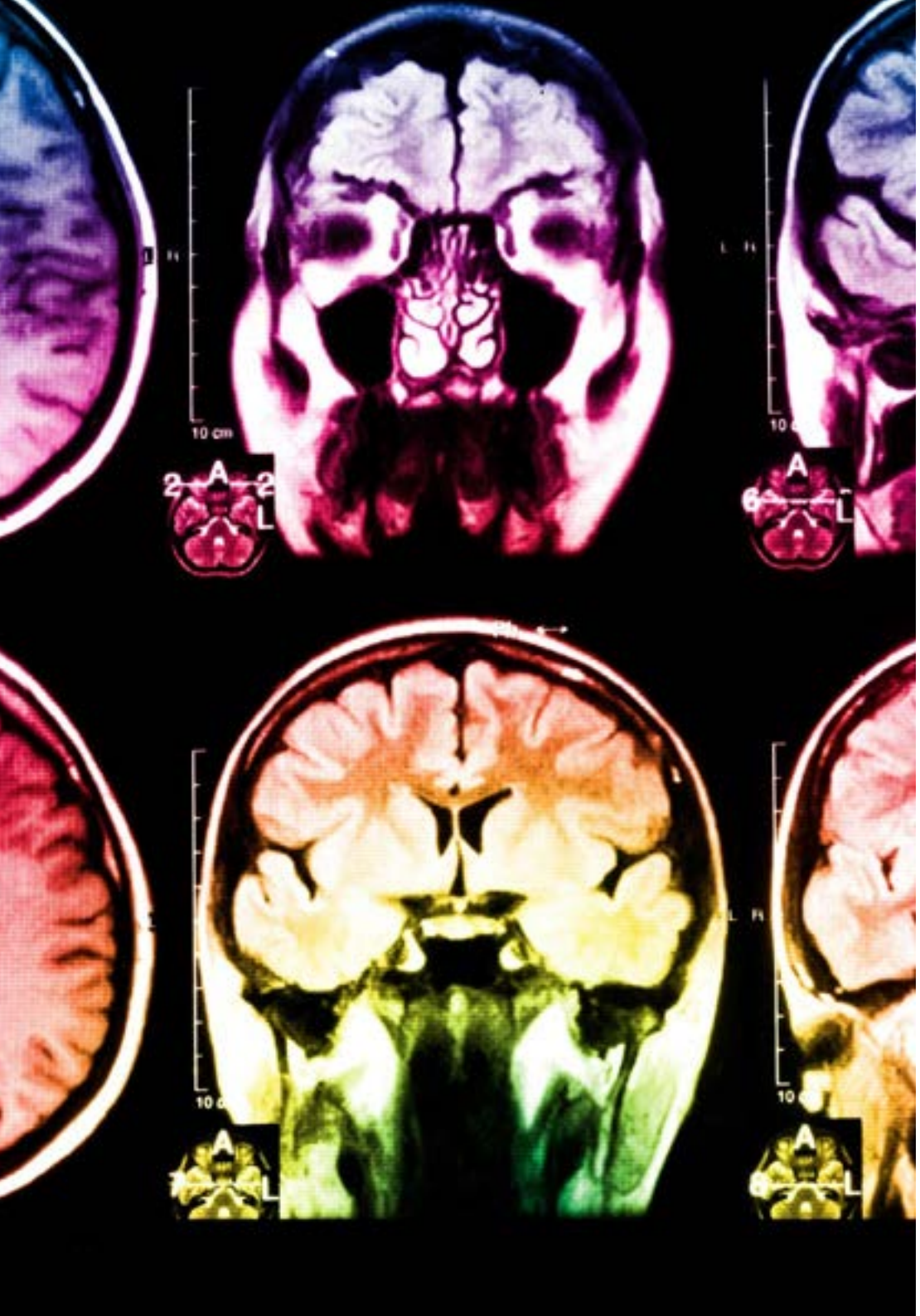
Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el Relearning.

*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.

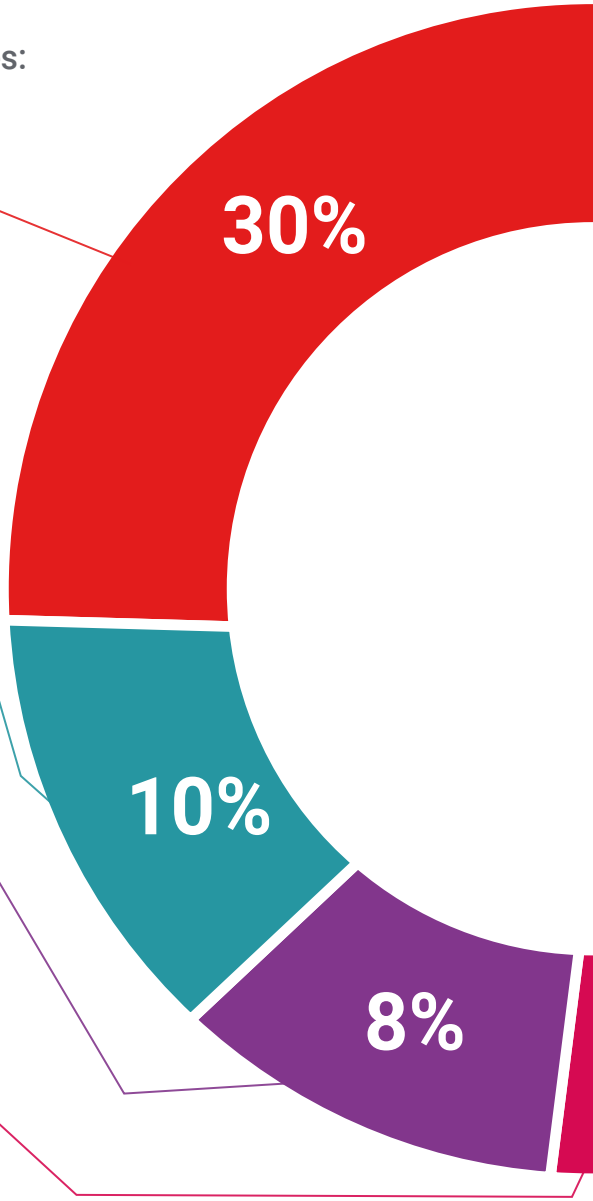
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

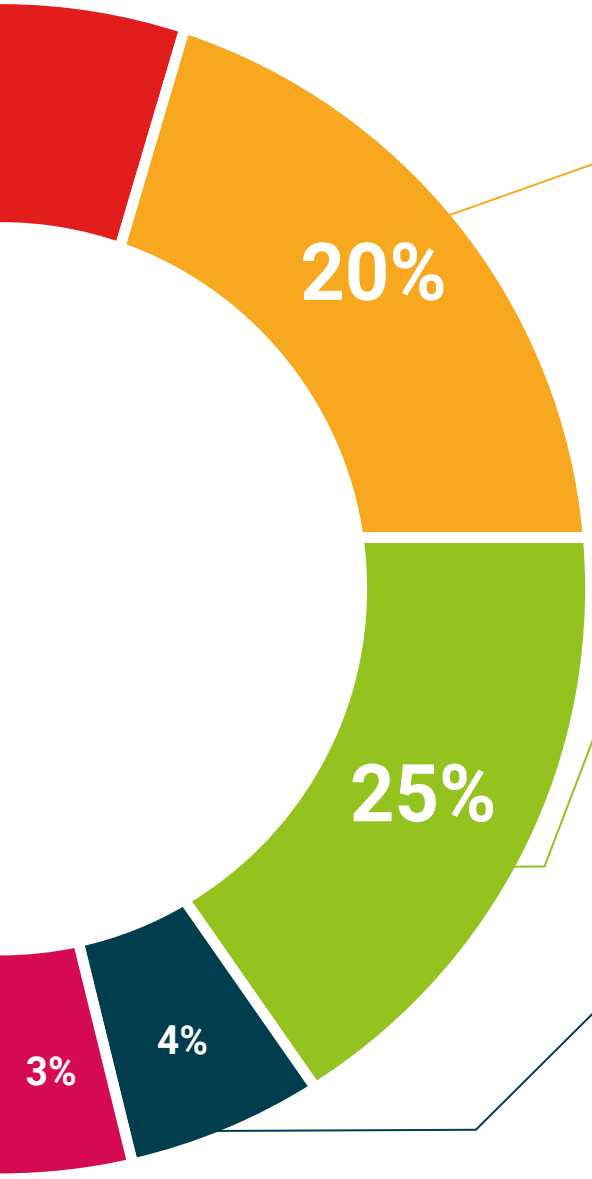
### Prácticas de habilidades y competencias

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 Diplomado en Hacking Ético garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Diplomado expedido por TECH Universidad Tecnológica.





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

Este **Diplomado en Hacking Ético** contiene el programa 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 **Diplomado** emitido por **TECH Universidad Tecnológica.**

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

Título: **Diplomado en Hacking Ético**

N.º Horas Oficiales: **150 h.**


tech universidad tecnológica

Otorga la presente

CONSTANCIA

a

C. _____, con documento de identificación nº_____

Por haber superado con éxito y acreditado el programa de

DIPLOMADO

en

Hacking Ético

Se trata de un título propio de esta Universidad con una duración de 150 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.

A 17 de junio de 2020

Mtra.Tere Guevara Navarro
Rectora

Este título propio se deberá acompañar siempre del título universitario habilitante expedido por la autoridad competente para ejercer profesionalmente en cada país. 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 EDUCATION realizará las gestiones oportunas para su obtención, con un coste adicional.



# Diplomado

## Hacking Ético

Modalidad: **Online**

Duración: **6 semanas**

Titulación: **TECH Universidad Tecnológica**

Horas lectivas: **150 h.**

# Diplomado
## Hacking Ético



tech universidad tecnológica