

Diplomado

Ataques a Redes  
y Sistemas Windows



**tech** universidad  
tecnológica

## Diplomado Ataques a Redes y Sistemas Windows

- » Modalidad: **online**
- » Duración: **6 semanas**
- » Titulación: **TECH Universidad Tecnológica**
- » Dedicación: **16h/semana**
- » Horario: **a tu ritmo**
- » Exámenes: **online**

Acceso web: [www.techtitute.com/informatica/curso-universitario/ataques-redes-sistemas-windows](http://www.techtitute.com/informatica/curso-universitario/ataques-redes-sistemas-windows)

# Índice

01

Presentación

---

*pág. 4*

02

Objetivos

---

*pág. 8*

03

Dirección del curso

---

*pág. 12*

04

Estructura y contenido

---

*pág. 16*

05

Metodología

---

*pág. 20*

06

Titulación

---

*pág. 28*

# 01 Presentación

Ante la creciente dependencia de las instituciones a las tecnologías y entornos virtuales, los ataques a los sistemas Windows constituyen para ellas una preocupación. En este sentido, dicho software es relevante al garantizar la continuidad de las operaciones comerciales y proteger los datos confidenciales. Por este motivo, cada vez más empresas invierten en la incorporación de expertos informáticos capaces de adoptar medidas de seguridad óptimas. En este contexto, estos especialistas tienen que actualizar sus contenidos habitualmente y estar al corriente de las técnicas más modernas de ciberataques. Para dar respuesta a esta necesidad, TECH ofrece un innovador programa con las estrategias de defensa más efectiva en Windows. Además, se basa en una modalidad 100% online, garantizando la comodidad del alumnado.



“

*Explorarás las defensas en el Active Directory Certificate Services y realizarás las auditorías más completas”*

Los especialistas en ciberseguridad generan numerosos activos intangibles a las organizaciones. Entre ellos, sobresale la implantación de procedimientos de seguridad como *firewalls* o prácticas de gestión de contraseñas sólidas para minimizar los riesgos. De esta manera, las compañías mejoran su productividad en su cadena productiva mientras se adaptan a las tecnologías emergentes. Cabe destacar que los ataques exitosos de los hackers dañan la reputación las empresas y afecta a la confianza de los *stakeholders*. De ahí la necesidad de que cuenten con auténticos expertos de la cibernética, que evalúen los riesgos y desarrollen estándares de seguridad.

Ante esta realidad, TECH implementa un completo programa que explotará las debilidades internas de los sistemas operativos Windows y explorará diversos procesos de mitigación. La capacitación profundizará en la ejecución de redes en Directorio Activo, tras conocer el funcionamiento de los servidores DNS y sus componentes. Además, en el plan de estudio se analizarán los fundamentos de Kerberos para demostrar la identidad de manera segura. También se profundizará en las herramientas que ofrece el Directorio Activo, detectando así comportamientos sospechosos. En este sentido, se brindarán claves para dar respuesta a los incidentes. Por último, se indagará en el Azure AD para operar en la nube y también autorizar a varios servicios de Microsoft.

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

Este **Diplomado en Ataques a Redes y Sistemas Windows** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

- ♦ El desarrollo de casos prácticos presentados por expertos en Ataques a redes y sistemas Windows
- ♦ Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que está concebido recogen una información actualizada y práctica sobre aquellas disciplinas indispensables para el ejercicio profesional
- ♦ Los ejercicios prácticos donde realizar el proceso de autoevaluación para mejorar el aprendizaje
- ♦ Su especial hincapié en metodologías innovadoras
- ♦ Las lecciones teóricas, preguntas al experto, foros de discusión de temas controvertidos y trabajos de reflexión individual
- ♦ La disponibilidad de acceso a los contenidos desde cualquier dispositivo fijo o portátil con conexión a internet



*¿Quieres una mayor protección contra las amenazas en la red? Conviértete en un experto del Azure AD en tan solo 6 semanas”*



*Garantiza la integridad de las comunicaciones mediante el tráfico Kerberos gracia a este avanzado programa”*

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.

*Detecta las vulnerabilidades más comunes de los ADCS en la mejor universidad digital del mundo según Forbes.*

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



# 02

## Objetivos

El diseño del presente programa explora detalladamente las amenazas y debilidades internas, así como las técnicas avanzadas de intrusión empleadas por los profesionales de seguridad ofensiva. Asimismo, el módulo incluye estrategias de mitigación para que los estudiantes desarrollen capacidades tanto en el ataque como en la protección de entornos Windows. Bajo el apoyo del mejor cuadro docente, el alumnado adquirirá una experiencia para fortalecer la seguridad en estos sistemas y luego podrá aplicarla a escenarios del mundo real.







“

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



## 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



*Adquieres conocimientos  
sin limitaciones geográficas  
o timing preestablecido"*





## Objetivos específicos

---

- ♦ 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

# 03

## Dirección del curso

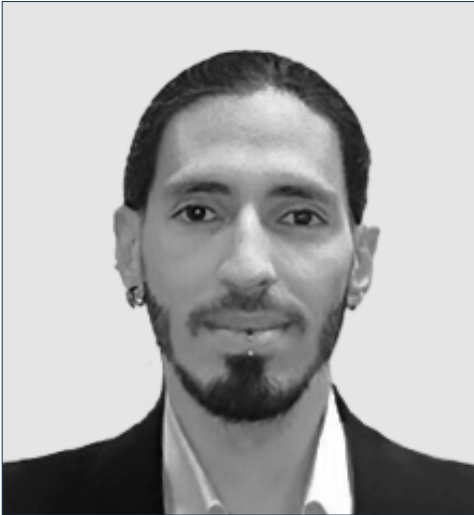
En su compromiso por ofrecer la máxima calidad educativa, TECH cuenta con un equipo docente con una amplia experiencia en el sector de la ciberseguridad. Gracias a esto, poseen un conocimiento profundo sobre las tácticas específicas dirigidas a sistemas operativos Windows. Además, ofrecen las tecnologías más avanzadas para que los alumnos desarrollen sus habilidades mientras exploran su creatividad para ofrecer propuestas innovadoras. De esta forma, estarán altamente cualificados y destacarán en un campo digital que ofrece múltiples oportunidades laborales.



“

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

## Dirección



### D. Gómez Pintado, Carlos

- ♦ Gerente de Ciberseguridad y Red Team CIPHERBIT en Grupo Oesía
- ♦ Gerente *Advisor & Investor* en Wesson App
- ♦ Graduado en Ingeniería del Software y Tecnologías de la Sociedad de la Información, por la Universidad Politécnica de Madrid
- ♦ Colabora con instituciones educativas para la confección de Ciclos Formativos de Grado Superior en ciberseguridad

## Profesores

### D. 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



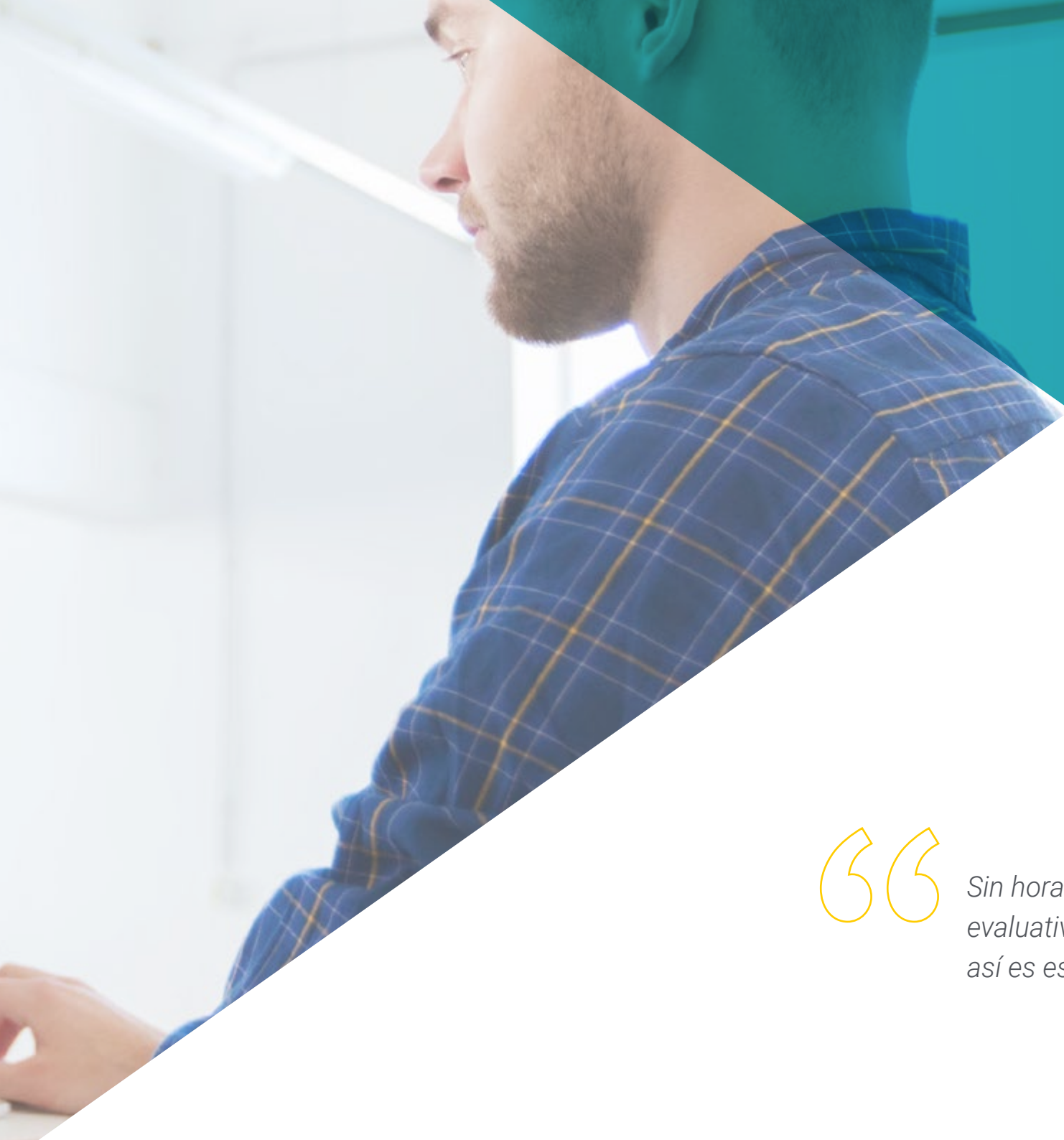
# 04

## Estructura y contenido

La capacitación se sumerge en las estrategias específicas destinadas a sistemas operativos Windows. En este sentido, se profundiza en las técnicas avanzadas de intrusión para apreciar las vulnerabilidades internas de las compañías. También durante la programación se abordarán ataques desde la perspectiva de la red y del sistema operativo. Tras una contextualización histórica, se analizarán la arquitectura general del Directorio Activo y sus protocolos más seguros. Además, se ahondará en el proceso de autenticación y gestión de credenciales. A su vez, se hará énfasis en la importancia en el funcionamiento del protocolo de Kerberos para distinguir identidades de los usuarios.







“

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

## Módulo 1. Ataques a redes y sistemas Windows

- 1.1. Windows y Directorio Activo
  - 1.1.1. Historia y evolución de Windows
  - 1.1.2. Conceptos básicos de Directorio Activo
  - 1.1.3. Funciones y servicios del Directorio Activo
  - 1.1.4. Arquitectura general del Directorio Activo
- 1.2. Redes en entornos de Directorio Activo
  - 1.2.1. Protocolos de red en Windows
  - 1.2.2. DNS y su funcionamiento en el Directorio Activo
  - 1.2.3. Herramientas de diagnóstico de red
  - 1.2.4. Implementación de redes en Directorio Activo
- 1.3. Autenticación y autorización en Directorio Activo
  - 1.3.1. Proceso y flujo de autenticación
  - 1.3.2. Tipos de credenciales
  - 1.3.3. Almacenamiento y gestión de credenciales
  - 1.3.4. Seguridad en la autenticación
- 1.4. Permisos y políticas en Directorio Activo
  - 1.4.1. GPOs
  - 1.4.2. Aplicación y gestión de GPOs
  - 1.4.3. Administración de permisos en Directorio Activo
  - 1.4.4. Vulnerabilidades y mitigaciones en permisos
- 1.5. Fundamentos de Kerberos
  - 1.5.1. ¿Qué es Kerberos?
  - 1.5.2. Componentes y funcionamiento
  - 1.5.3. Tickets en Kerberos
  - 1.5.4. Kerberos en el contexto de Directorio Activo
- 1.6. Técnicas avanzadas en Kerberos
  - 1.6.1. Ataques comunes en Kerberos
  - 1.6.2. Mitigaciones y protecciones
  - 1.6.3. Monitorización del tráfico Kerberos
  - 1.6.4. Ataques avanzados en Kerberos



- 1.7. Active Directory Certificate Services (ADCS)
  - 1.7.1. Conceptos básicos de PKI
  - 1.7.2. Roles y componentes de ADCS
  - 1.7.3. Configuración y despliegue de ADCS
  - 1.7.4. Seguridad en ADCS
- 1.8. Ataques y defensas en Active Directory Certificate Services (ADCS)
  - 1.8.1. Vulnerabilidades comunes en ADCS
  - 1.8.2. Ataques y técnicas de explotación
  - 1.8.3. Defensas y mitigaciones
  - 1.8.4. Monitorización y auditoría de ADCS
- 1.9. Auditoría del Directorio Activo
  - 1.9.1. Importancia de la auditoría en el Directorio Activo
  - 1.9.2. Herramientas de auditoría
  - 1.9.3. Detección de anomalías y comportamientos sospechosos
  - 1.9.4. Respuesta a incidentes y recuperación
- 1.10. Azure AD
  - 1.10.1. Conceptos básicos de Azure AD
  - 1.10.2. Sincronización con el Directorio Activo local
  - 1.10.3. Gestión de identidades en Azure AD
  - 1.10.4. Integración con aplicaciones y servicios

“Biblioteca atestada de recursos multimedia en diferentes formatos audiovisuales”



# 05 Metodología

Este programa de capacitación ofrece una forma diferente de aprender. Nuestra metodología se desarrolla a través de un modo de aprendizaje de forma cíclica: ***el Relearning***.

Este sistema de enseñanza es utilizado, por ejemplo, en las facultades de medicina más prestigiosas del mundo y se ha considerado uno de los más eficaces por publicaciones de gran relevancia como el ***New England Journal of Medicine***.



“

*Descubre el Relearning, un sistema que abandona el aprendizaje lineal convencional para llevarte a través de sistemas cíclicos de enseñanza: una forma de aprender que ha demostrado su enorme eficacia, especialmente en las materias que requieren memorización”*

## Estudio de Caso para contextualizar todo el contenido

Nuestro programa ofrece un método revolucionario de desarrollo de habilidades y conocimientos. Nuestro objetivo es afianzar competencias en un contexto cambiante, competitivo y de alta exigencia.

“

*Con TECH podrás experimentar una forma de aprender que está moviendo los cimientos de las universidades tradicionales de todo el mundo”*



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



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

## Un método de aprendizaje innovador y diferente

El presente programa de TECH es una enseñanza intensiva, creada desde 0, que propone los retos y decisiones más exigentes en este campo, ya sea en el ámbito nacional o internacional. Gracias a esta metodología se impulsa el crecimiento personal y profesional, dando un paso decisivo para conseguir el éxito. El método del caso, técnica que sienta las bases de este contenido, garantiza que se sigue la realidad económica, social y profesional más vigente.

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

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de Informática del mundo desde que éstas existen. Desarrollado en 1912 para que los estudiantes de Derecho no solo aprendiesen las leyes a base de contenidos teóricos, el método del caso consistió en presentarles situaciones complejas reales para que tomaran decisiones y emitieran juicios de valor fundamentados sobre cómo resolverlas. En 1924 se estableció como método estándar de enseñanza en Harvard.

Ante una determinada situación, ¿qué debería hacer un profesional? Esta es la pregunta a la que te enfrentamos en el método del caso, un método de aprendizaje orientado a la acción. A lo largo del curso, los estudiantes se enfrentarán a múltiples casos reales. Deberán integrar todos sus conocimientos, investigar, argumentar y defender sus ideas y decisiones.

## Relearning Methodology

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

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

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

En TECH aprenderás con una metodología vanguardista concebida para capacitar a los directivos del futuro. Este método, a la vanguardia pedagógica mundial, se denomina Relearning.

Nuestra universidad es la única en habla hispana licenciada para emplear este exitoso método. En 2019, conseguimos mejorar los niveles de satisfacción global de nuestros alumnos (calidad docente, calidad de los materiales, estructura del curso, objetivos...) con respecto a los indicadores de la mejor universidad online en español.





En nuestro programa, el aprendizaje no es un proceso lineal, sino que sucede en espiral (aprender, desaprender, olvidar y reaprender). Por eso, se combinan cada uno de estos elementos de forma concéntrica. Con esta metodología se han capacitado más de 650.000 graduados universitarios con un éxito sin precedentes en ámbitos tan distintos como la bioquímica, la genética, la cirugía, el derecho internacional, las habilidades directivas, las ciencias del deporte, la filosofía, el derecho, la ingeniería, el periodismo, la historia o los mercados e instrumentos financieros. Todo ello en un entorno de alta exigencia, con un alumnado universitario de un perfil socioeconómico alto y una media de edad de 43,5 años.

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

A partir de la última evidencia científica en el ámbito de la neurociencia, no solo sabemos organizar la información, las ideas, las imágenes y los recuerdos, sino que sabemos que el lugar y el contexto donde hemos aprendido algo es fundamental para que seamos capaces de recordarlo y almacenarlo en el hipocampo, para retenerlo en nuestra memoria a largo plazo.

De esta manera, y en lo que se denomina Neurocognitive context-dependent e-learning, los diferentes elementos de nuestro programa están conectados con el contexto donde el participante desarrolla su práctica profesional.



Este programa ofrece los mejores materiales educativos, preparados a conciencia para los profesionales:



#### Material de estudio

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

Estos contenidos son aplicados después al formato audiovisual, para crear el método de trabajo online de TECH. Todo ello, con las técnicas más novedosas que ofrecen piezas de gran calidad en todos y cada uno los materiales que se ponen a disposición del alumno.



#### Clases magistrales

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

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



#### Prácticas de habilidades y competencias

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



#### Lecturas complementarias

Artículos recientes, documentos de consenso y guías internacionales, entre otros. En la biblioteca virtual de TECH el estudiante tendrá acceso a todo lo que necesita para completar su capacitación.





**Case studies**

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



**Resúmenes interactivos**

El equipo de TECH presenta los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audios, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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



**Testing & Retesting**

Se evalúan y reevalúan periódicamente los conocimientos del alumno a lo largo del programa, mediante actividades y ejercicios evaluativos y autoevaluativos para que, de esta manera, el estudiante compruebe cómo va consiguiendo sus metas.



06

# Titulación

El Diplomado en Ataques a Redes y Sistemas Windows 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 tu titulación universitaria sin desplazamientos ni farragosos trámites”*

Este **Diplomado en Ataques a Redes y Sistemas Windows** 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 Ataques a Redes y Sistemas Windows**

N.º Horas Oficiales: **150 h.**



\*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 Ataques a Redes y Sistemas Windows

- » Modalidad: online
- » Duración: 6 semanas
- » Titulación: TECH Universidad Tecnológica
- » Dedicación: 16h/semana
- » Horario: a tu ritmo
- » Exámenes: online

# Diplomado

## Ataques a Redes y Sistemas Windows

```
27
28 /** replicating death on client */
29 UFUNCTION()
30 void OnRep_Dying();
31
32 /** Returns True if the pawn can die in the current state */
33 virtual bool CanDie() const;
34
35 /** Kills pawn. [Server/authority only]
36 virtual void Die();
37
38 /** Event on death [Server/Client]
39 virtual void OnDeath();
```