Diplomado

Análisis y Desarrollo de Malware

tech universidad tecnológica

tech universidad tecnológica

Diplomado
Análisis y Desarrollo de Malware

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

Acceso web: **www.techtitute.com/informatica/curso-universitario/analisis-desarrollo-malware**

Índice

01

Presentación

En un contexto digital donde los activos empresariales dependen críticamente de la seguridad cibernética, la amenaza constante del malware representa un desafío significativo. En este aspecto, la proliferación de ataques maliciosos destaca la urgencia de contar con profesionales altamente capacitados en este ámbito. En este sentido, el plan de estudios aborda la necesidad imperante de expertos que no solo comprendan la complejidad de las amenazas digitales, sino que también puedan diseñar estrategias proactivas para su detección y mitigación. Así, los egresados profundizarán en herramientas esenciales para salvaguardar la integridad de los sistemas en un entorno empresarial cada vez más digitalizado. Con la flexibilidad de la modalidad 100% online, este curso garantiza la accesibilidad y la actualización continua necesarias para enfrentar los retos cambiantes del ciberespacio.

Conviértete en un experto en Malware con novedosas técnicas de análisis dinámico gracias a este exclusivo programa 100% online”

En el panorama actual de la ciberseguridad, la sofisticación de las amenazas cibernéticas ha alcanzado niveles sin precedentes, generando una demanda creciente de profesionales especializados en Análisis y Desarrollo de Malware. La constante evolución de las tácticas maliciosas exige una respuesta igualmente dinámica por parte de los expertos en seguridad cibernética. En este contexto, el presente programa universitario de TECH emerge como una solución integral para abordar estas necesidades. Diseñado para proporcionar a los alumnos conocimientos avanzados, el temario abarca desde la comprensión profunda de la naturaleza del malware hasta la evaluación de herramientas anti-malware. Este enfoque integral prepara a los profesionales para enfrentar las amenazas actuales y futuras.

El temario del programa en Análisis y Desarrollo de Malware de TECH se erige como un robusto compendio de conocimientos que abarca diversas dimensiones del mundo del malware. Los egresados explorarán en profundidad las diversas formas y objetivos del malware, adquiriendo conocimientos avanzados sobre su naturaleza, funcionalidad y comportamiento. El programa se adentra en el análisis forense aplicado al malware, proporcionando a los estudiantes las habilidades necesarias para identificar indicadores de compromiso (IoC) y patrones de ataque, crucial para la detección temprana y la respuesta efectiva a incidentes de seguridad. Además, el itinerario se enfoca en el desarrollo de habilidades específicas para evaluar y seleccionar herramientas de seguridad anti-malware. Los alumnos aprenderán a discernir la eficacia de estas herramientas y su adaptabilidad a entornos particulares, lo que resulta esencial en la implementación de estrategias de defensa efectivas.

Con un enfoque innovador y adaptable, este programa universitario se presenta como una propuesta de formación única. La modalidad 100% online y la metodología *Relearning* garantizan una experiencia educativa flexible y eficiente, permitiendo a los profesionales avanzar en su carrera sin interrupciones y adaptarse continuamente a las demandas cambiantes del campo de la ciberseguridad.

Este **Diplomado en Análisis y Desarrollo de Malware** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en Análisis y Desarrollo de Malware
- 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

Dominarás el análisis de llamadas con API monitos en solo 6 semanas de la mejor formación online”

Abordarás la generación de Shellcode en la universidad mejor valorada del mundo por sus alumnos según la plataforma Trustpilot (4,9/5)"

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

Profundizarás en la ofuscación de Strings ¡Dale a tu carrera el impulso que necesita!

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

Este plan de estudios tiene como objetivo principal capacitar a los egresados para dominar conocimientos avanzados sobre la naturaleza, funcionalidad y comportamiento del malware. A lo largo del programa, los estudiantes profundizarán en las diversas formas y objetivos del malware, permitiéndoles analizar y desarrollar estrategias defensivas efectivas en el ámbito de la ciberseguridad. Asimismo, este enfoque integral busca formar profesionales capaces de enfrentar los desafíos emergentes en la detección, análisis y mitigación de amenazas de malware en entornos digitales complejos. Además, el uso de una metodología 100% online flexibiliza el aprendizaje dando la posibilidad de acceder en cualquier momento y lugar.

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

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

¿Quieres experimentar un salto de calidad en tu carrera? Con TECH adquirirás habilidades en el análisis forense aplicado al malware"

Objetivos específicos

- 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

03

Dirección del curso

El programa en Análisis y Desarrollo de Malware cuenta con un cuerpo docente excepcionalmente calificado. Para ello, TECH ha seleccionado a expertos con una amplia experiencia y reconocido prestigio en empresas líderes del sector de ciberseguridad. Este claustro, compuesto por profesionales destacados, aporta no solo su experiencia práctica en el análisis y desarrollo de malware, sino también su compromiso en la formación de futuros especialistas, garantizando una enseñanza actualizada y alineada con las demandas y desafíos actuales del campo de la ciberseguridad.

Actualízate en la configuración de máquinas virtuales y snapshots de la mano de los mejores expertos en la materia. ¡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, Marco

- Consultor de Ciberseguridad en Cipherbit
- eLearnSecurity Certified eXploit Developer
- Offensive Security Certified Professional
- Offensive Security Wireless Professional
- Virtual Hacking Labs Plus
- Graduado en Ingeniería del Software por la Universidad Politécnica de Madrid

04

Estructura y contenido

El presente programa universitario proporcionará a los alumnos una inmersión profunda en el mundo del malware, centrándose en su desarrollo con propósitos educativos y defensivos. A lo largo del temario, los egresados abordarán las complejidades del malware, permitiendo una comprensión detallada de las tácticas empleadas por los atacantes. En este aspecto, el enfoque equilibrado del temario no solo fomenta la adquisición de conocimientos avanzados en el análisis de malware, sino que también capacita a los estudiantes para desarrollar estrategias defensivas esenciales en el ámbito de la ciberseguridad.

Accederás a un plan de estudios diseñado por un reputado cuadro docente, que te garantizará un aprendizaje exitoso"

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

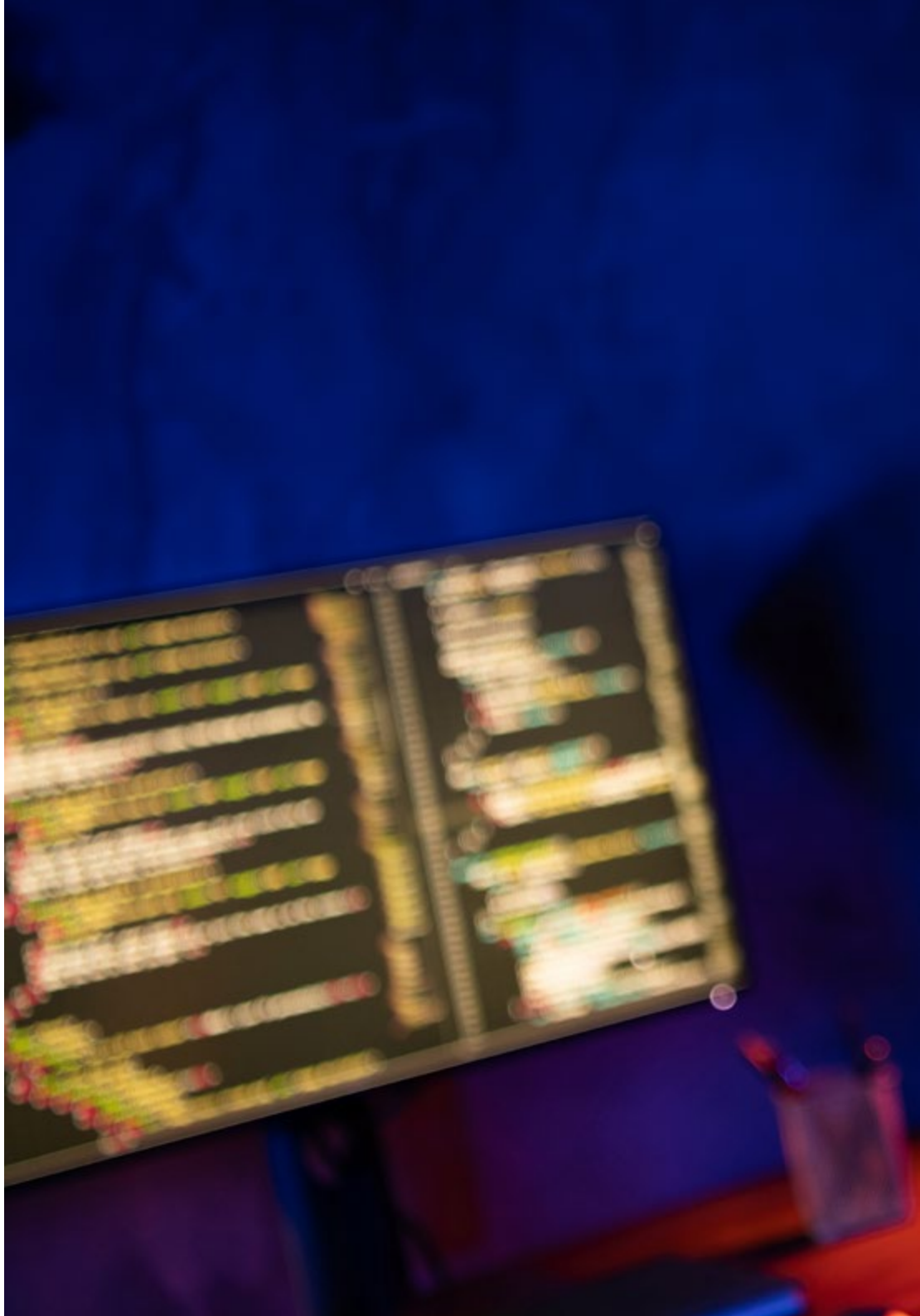
1.2. Preparando el Entorno
- 1.2.1. Configuración de Máquinas Virtuales y Snapshots
- 1.2.2. Herramientas para Análisis de Malware
- 1.2.3. Herramientas para Desarrollo de Malware

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

No dejes pasar la oportunidad de impulsar tu carrera mediante este programa innovador”

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

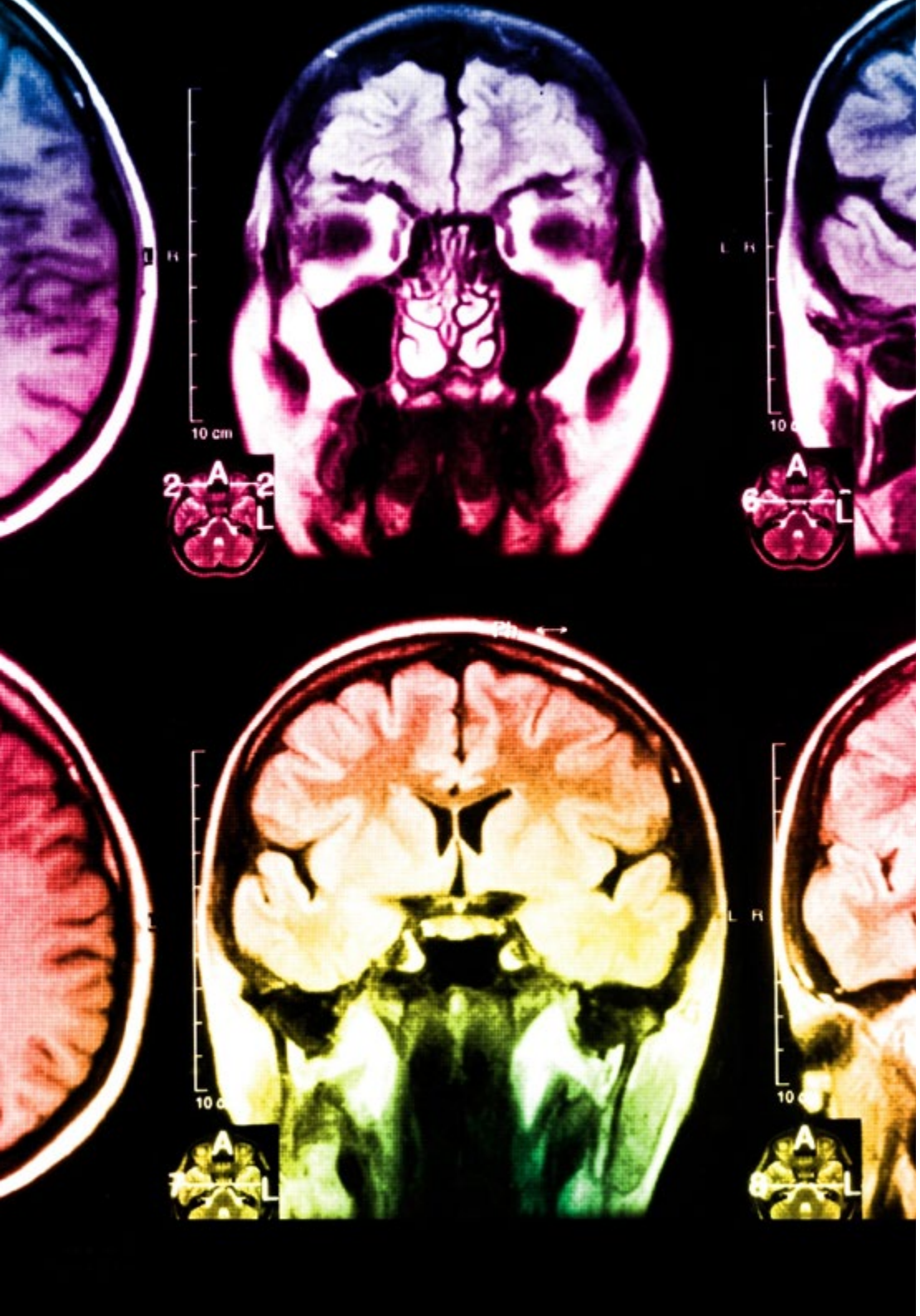
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

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.

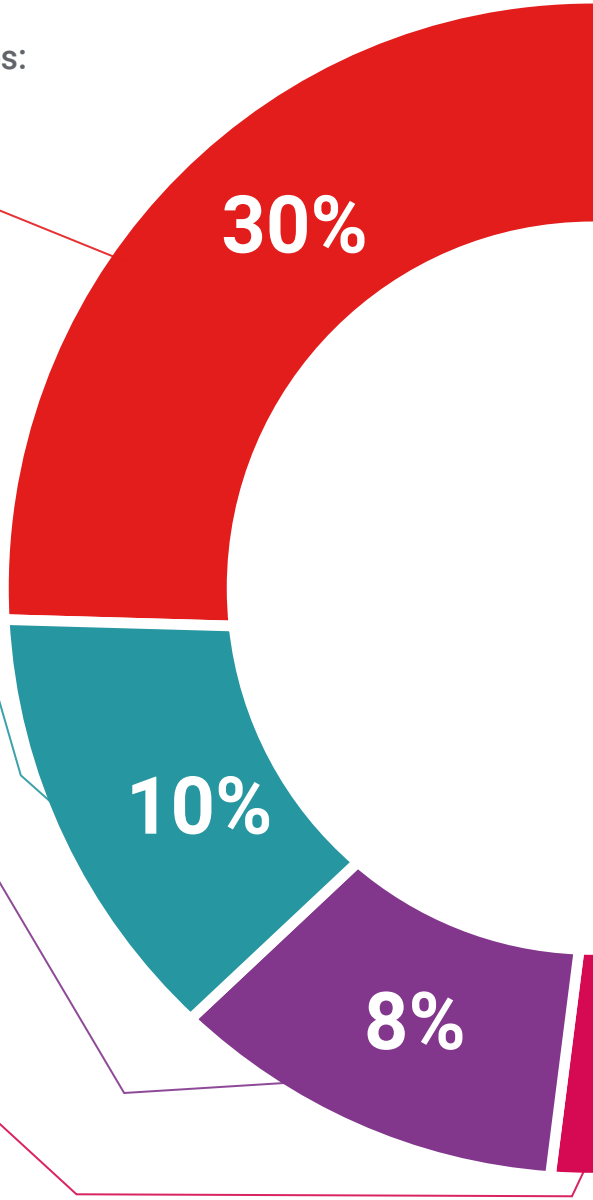
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

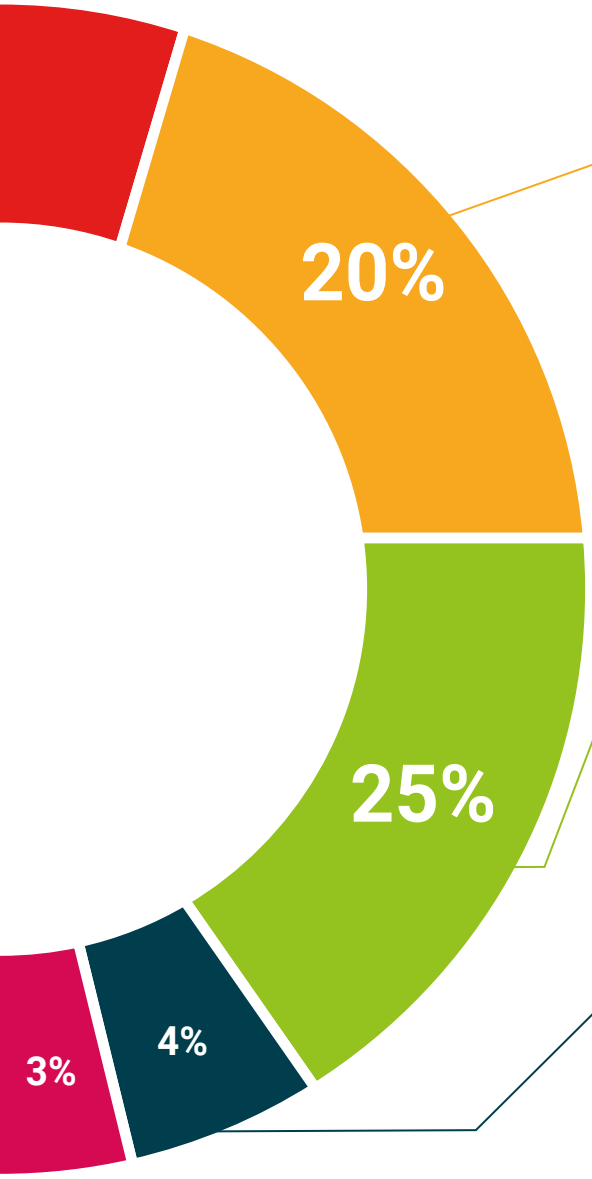
Prácticas de habilidades y competencias

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 Análisis y Desarrollo de Malware 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 Análisis y Desarrollo de Malware** 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 Análisis y Desarrollo de Malware**

Modalidad: **online**

Duración: **6 semanas**


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

Análisis y Desarrollo de Malware

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

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.

tech universidad tecnológica

Diplomado
Análisis y Desarrollo de Malware

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

Diplomado

Análisis y Desarrollo de Malware

tech universidad tecnológica