

Diplomado

Fundamentos Forenses y DFIR



Diplomado Fundamentos Forenses y DFIR

- » Modalidad: No escolarizada (100% en línea)
- » Duración: 6 semanas
- » Titulación: TECH Universidad
- » Horario: a tu ritmo
- » Exámenes: online

Acceso web: www.techtitute.com/informatica/curso-universitario/fundamentos-forenses-dfir



Índice

01

Presentación

pág. 4

02

Objetivos

pág. 8

03

Dirección del curso

pág. 12

04

Estructura y contenido

pág. 16

05

Metodología de estudio

pág. 20

06

Titulación

pág. 30

01

Presentación

Con el avance de nuevas tecnologías como los sistemas informáticos, las instituciones cada vez tienen una mayor presencia en Internet. No obstante, ante el aumento de los ciberataques, las empresas se ven expuestas a diferentes contratiempos. En este sentido, si los hackers logran acceder a sus redes podrían borrar datos sensibles y hasta pedir rescates económicos a cambio de liberar los sistemas bloqueados. Por eso, es importante que las compañías cuenten con expertos en Fundamentos Forenses para detectar fallos de seguridad y reducir su impacto lo máximo posible. Ante esta necesidad, TECH lanza un innovador programa para implementar técnicas avanzadas para el análisis de evidencia digital. Además, se imparte en una modalidad 100% online, garantizando la comodidad de los alumnos.



“

¿Quieres analizar registros de firewall y detectar así intrusiones en la red? Lógralo en 180 horas gracias a esta capacitación”

Las empresas se están percatando cada vez más de la importancia de tener en sus organigramas a informáticos especializados en ciberseguridad. Entre los beneficios de esto, sobresale la protección de sus activos digitales y la investigación forense para determinar tanto las causas como el alcance de los posibles incidentes. A su vez estos profesionales también recaban informaciones que pueden ser utilizadas como pruebas judiciales y para perseguir a ciberdelincuentes. En este sentido, incluso ayudan a que las organizaciones cumplan con las regulaciones de seguridad de datos y los requisitos de notificación de violación de seguridad.

Ante esta situación, TECH desarrolla una vanguardista capacitación para que el alumnado pueda prevenir el ataque de los hackers mediante la instauración de las estrategias más oportunas. El itinerario académico profundizará en los procesos de adquisición de evidencias, a partir de la cadena de custodia. De este modo, los estudiantes actuarán como laboratorios forenses informáticos y resolverán los incidentes que afecten a las organizaciones. Asimismo, el programa abordará el análisis de paquetes de red y así el alumnado llevará a cabo registros de *firewall*. También se aportarán malwares, con el fin de ejecutar técnicas de desensamblado. Así los egresados aplicarán metodologías de DFIR y darán rienda suelta a su creatividad para ofrecer las soluciones empresariales más innovadoras.

Además, para afianzar el dominio de los contenidos, este plan de estudios aplica el sistema *Relearning*. Cabe destacar que 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 resúmenes interactivos o vídeos explicativos. Todo ello en una cómoda modalidad 100% online, que permite a los alumnos ajustar los horarios en función de sus responsabilidades.

Este **Diplomado en en Fundamentos Forenses y DFIR** contiene el programa universitario más completo y actualizado del mercado. Sus características más destacadas son:

- ♦ El desarrollo de casos prácticos presentados por expertos en Fundamentos Forenses y DFIR
- ♦ 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



*Crearás planes de respuesta
ante posibles incidentes 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”

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.

¿Necesitas recuperar datos de medios dañados? TECH te brinda las mejores herramientas para lograrlo.

Elaborarás informes forenses con los que podrás comparecer como testigo experto en importantes juicios.



02 Objetivos

El diseño del presente programa explorará las técnicas avanzadas para la recopilación y análisis de evidencia digital, abordando casos de violaciones de seguridad. Así los alumnos profundizarán en el análisis de archivo, así como en la preservación de la cadena de custodia. Además, los estudiantes examinarán las tácticas más provechosas para minimizar el impacto ante los posibles incidentes cibernéticos que surjan.



“

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



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



Tendrás el apoyo de un cuadro docente formado por distinguidos profesionales en Ciberseguridad Industrial"



Objetivos específicos

Módulo 1. Fundamentos Forenses y DFIR

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

03

Dirección del curso

En su compromiso de ofrecer una educación basada en la excelencia, TECH cuenta con profesionales de prestigio internacional. Estos profesionales de la ciberseguridad tienen un amplio bagaje laboral, por lo que mediante la presente capacitación ofrecen las herramientas más eficaces para que los alumnos adquieran habilidades esenciales para la investigación forense digital y den respuesta a los incidentes. De esta manera, los estudiantes poseen las garantías que requieren para especializarse en un sector digital que ofrece numerosas oportunidades laborales.



“

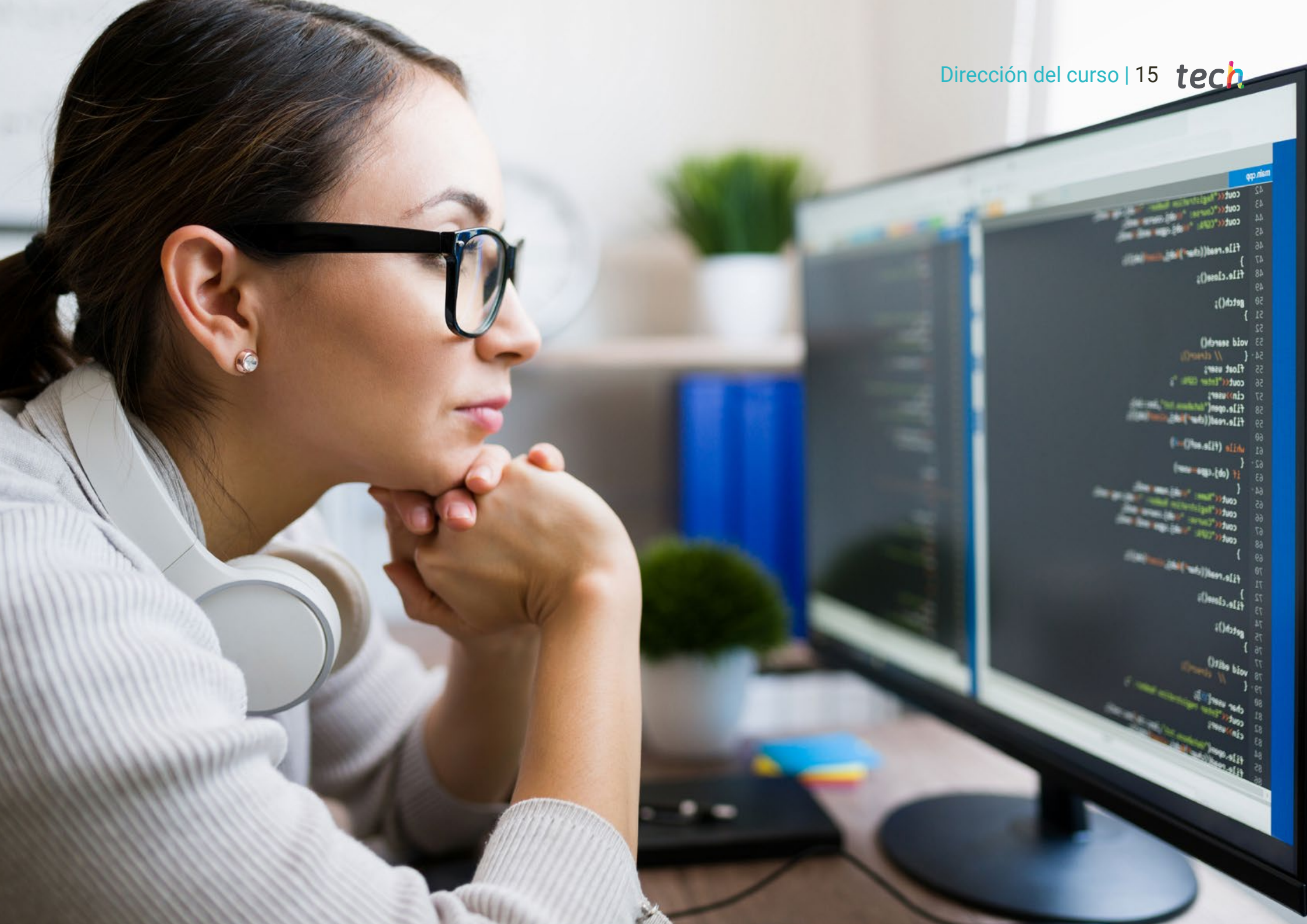
*Biblioteca atestada de recursos multimedia
en diferentes formatos audiovisuales”*

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



04

Estructura y contenido

El temario abarcará simulaciones destinadas a responder con inmediatez ante incidentes cibernéticos, reduciendo sus efectos y restaurando la normalidad operativa. Además, el itinerario académico profundiza en el análisis de los sistemas operativos más importantes (Windows, Linux y macOS) con el fin de que los estudiantes recuperen datos de medios dañados. También se ahondará en el análisis de malware para identificar los códigos maliciosos e impedir así que las organizaciones sufran virus como gusanos o troyanos. De este modo, el alumnado adquirirá conocimientos sólidos acerca de la investigación forense digital.

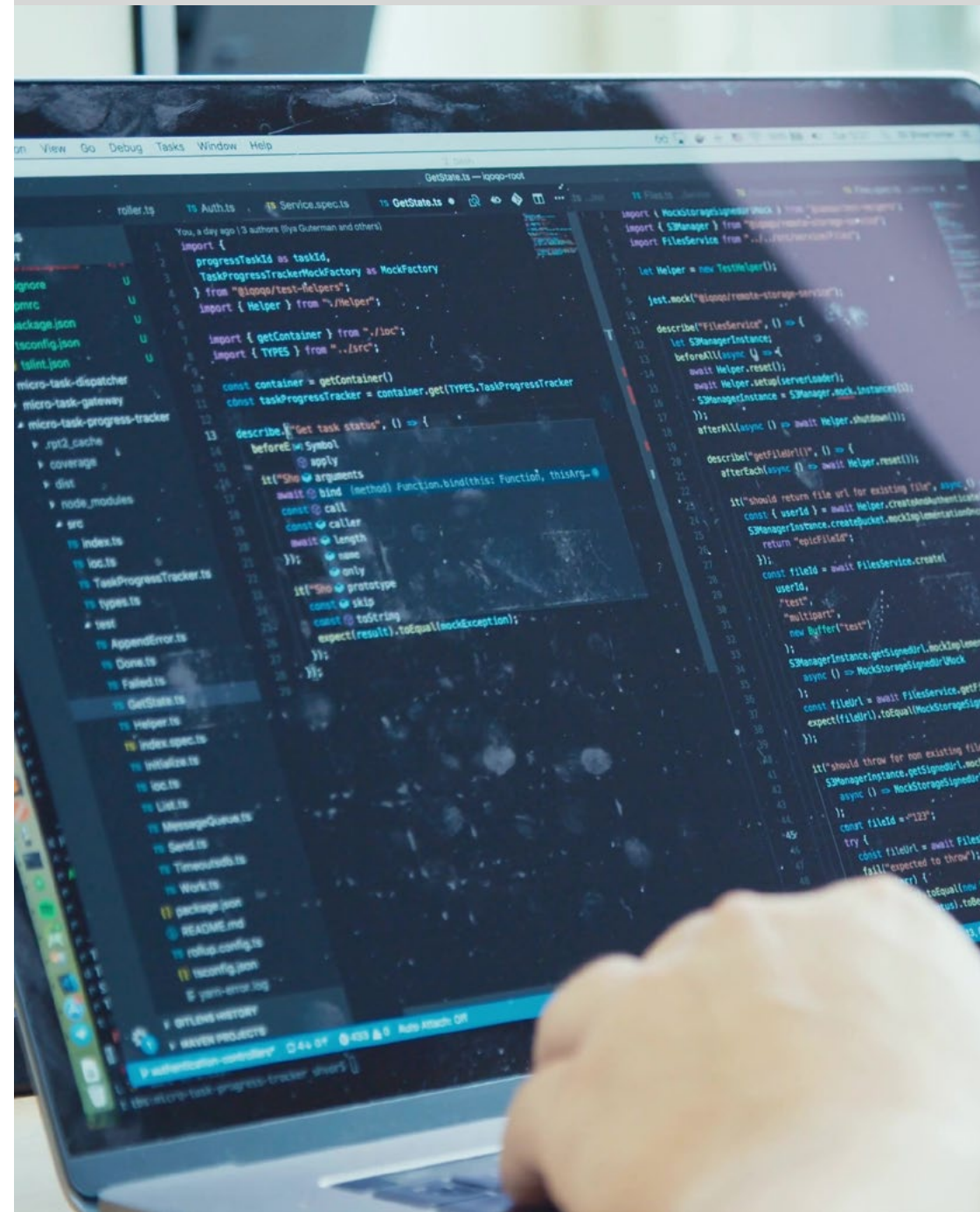


“

*Biblioteca atestada de recursos multimedia
en diferentes formatos audiovisuales”*

Módulo 1. Fundamentos Forenses y DFIR

- 1.1. Forense Digital
 - 1.1.1. Historia y evolución de la informática forense
 - 1.1.2. Importancia de la informática forense en la ciberseguridad
 - 1.1.3. Historia y evolución de la informática forense
- 1.2. Fundamentos de la Informática Forense
 - 1.2.1. Cadena de custodia y su aplicación
 - 1.2.2. Tipos de evidencia digital
 - 1.2.3. Procesos de adquisición de evidencia
- 1.3. Sistemas de Archivos y Estructura de Datos
 - 1.3.1. Principales sistemas de archivos
 - 1.3.2. Métodos de ocultamiento de datos
 - 1.3.3. Análisis de metadatos y atributos de archivos
- 1.4. Análisis de Sistemas Operativos
 - 1.4.1. Análisis forense de sistemas Windows
 - 1.4.2. Análisis forense de sistemas Linux
 - 1.4.3. Análisis forense de sistemas macOS
- 1.5. Recuperación de Datos y Análisis de Disco
 - 1.5.1. Recuperación de datos de medios dañados
 - 1.5.2. Herramientas de análisis de disco
 - 1.5.3. Interpretación de tablas de asignación de archivos
- 1.6. Análisis de Redes y Tráfico
 - 1.6.1. Captura y análisis de paquetes de red
 - 1.6.2. Análisis de registros de firewall
 - 1.6.3. Detección de intrusiones en red
- 1.7. Malware y Análisis de Código Malicioso
 - 1.7.1. Clasificación de malware y sus características
 - 1.7.2. Análisis estático y dinámico de malware
 - 1.7.3. Técnicas de desensamblado y depuración





- 1.8. Análisis de Registros y Eventos
 - 1.8.1. Tipos de registros en sistemas y aplicaciones
 - 1.8.2. Interpretación de eventos relevantes
 - 1.8.3. Herramientas de análisis de registros
- 1.9. Responder a Incidentes de Seguridad
 - 1.9.1. Proceso de respuesta a incidentes
 - 1.9.2. Creación de un plan de respuesta a incidentes
 - 1.9.3. Coordinación con equipos de seguridad
- 1.10. Presentación de Evidencia y Jurídico
 - 1.10.1. Reglas de evidencia digital en el ámbito legal
 - 1.10.2. Preparación de informes forenses
 - 1.10.3. Comparecencia en juicio como testigo experto

“Biblioteca atestada de recursos multimedia en diferentes formatos audiovisuales”

05

Metodología de estudio

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

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



“

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

El alumno: la prioridad de todos los programas de TECH

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

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

“

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



Los planes de estudios más exhaustivos a nivel internacional

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

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

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

“

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

Case studies o Método del caso

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

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

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



Método Relearning

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

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

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

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



Un Campus Virtual 100% online con los mejores recursos didácticos

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

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

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

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



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

La eficacia del método se justifica con cuatro logros fundamentales:

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

La metodología universitaria mejor valorada por sus alumnos

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

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

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

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

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



Material de estudio

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

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



Prácticas de habilidades y competencias

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



Resúmenes interactivos

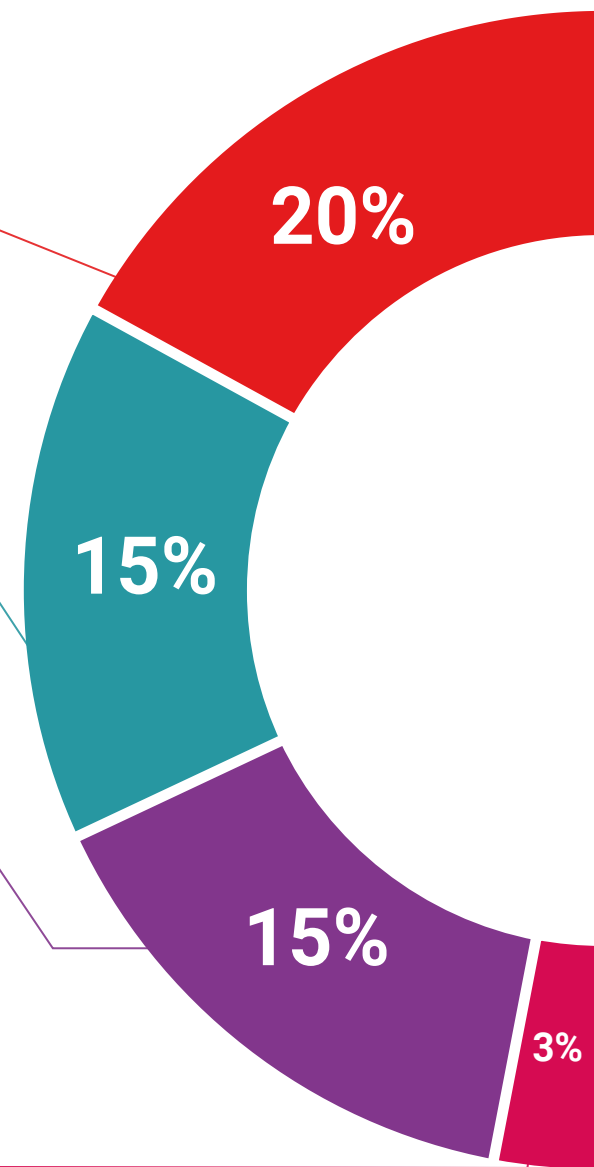
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

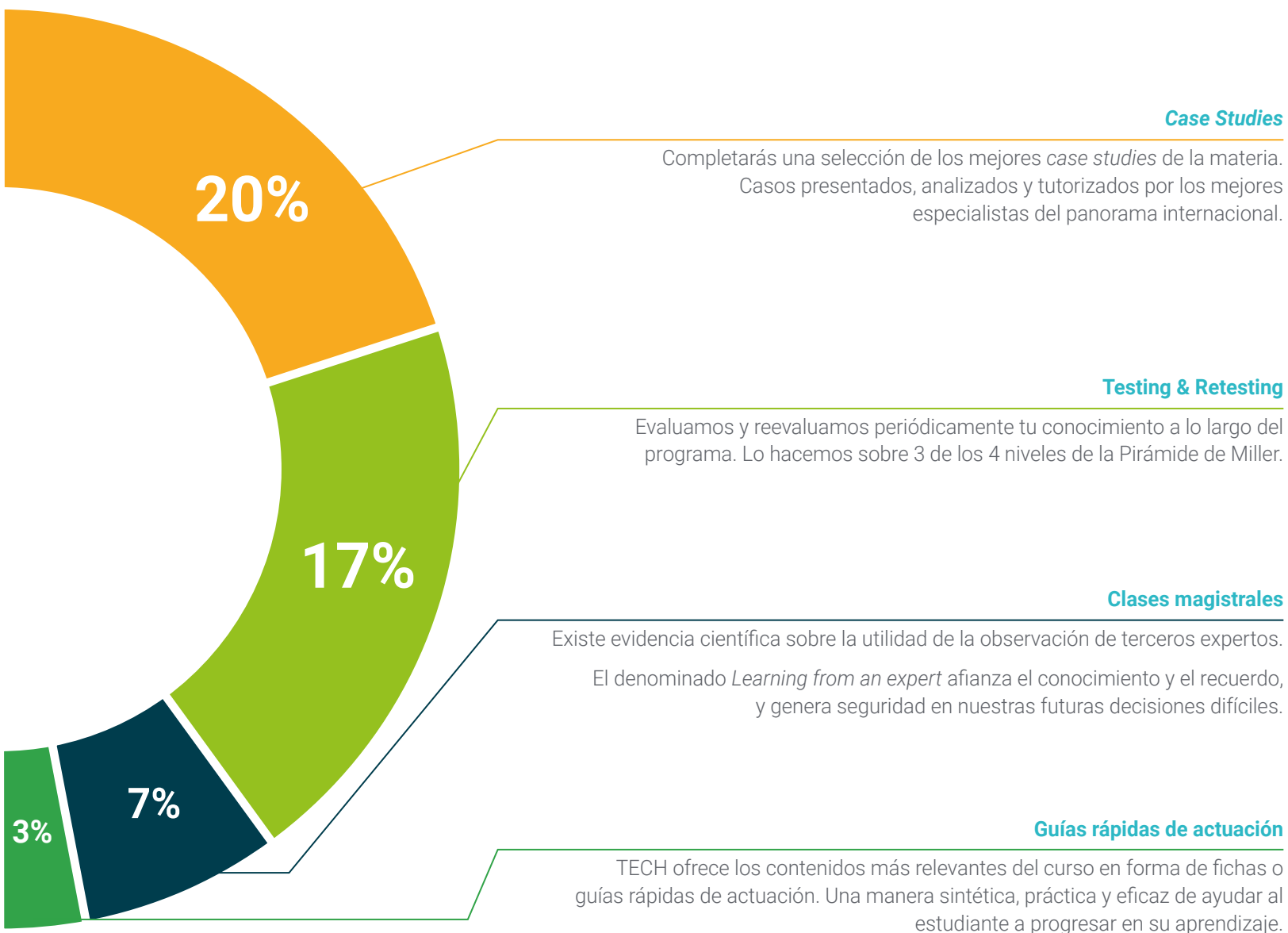
Este sistema exclusivo educativo para la presentación de contenidos multimedia fue premiado por Microsoft como "Caso de éxito en Europa".



Lecturas complementarias

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





Case Studies



Testing & Retesting



Clases magistrales



Guías rápidas de actuación



06 Titulación

El Diplomado en Fundamentos Forenses y DFIR garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un Diplomado expedido por TECH Universidad.



“

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

Este **Diplomado en Fundamentos Forenses y DFIR** contiene el programa universitario más completo y actualizado del mercado.

Tras la superación de la evaluación, el alumno recibirá por correo postal* con acuse de recibo su correspondiente título de **Diplomado** emitido por **TECH Universidad**.

Este título expedido por **TECH Universidad** 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 Fundamentos Forenses y DFIR**

Modalidad: **No escolarizada (100% en línea)**

Duración: **6 semanas**



*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.



Diplomado
Fundamentos Forenses
y DFIR

- » Modalidad: No escolarizada (100% en línea)
- » Duración: 6 semanas
- » Titulación: TECH Universidad
- » Horario: a tu ritmo
- » Exámenes: online

Diplomado

Fundamentos Forenses y DFIR