Curso Universitario
Fundamentos Forenses y DFIR

tech global university

tech global university

Curso Universitario
Fundamentos Forenses y DFIR

- Modalidad: **online**
- Duración: **6 semanas**
- Titulación: **TECH Global University**
- Acreditación: **6 ECTS**
- 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 — pág. 20

06 Titulación — pág. 28

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 **Curso Universitario en en Fundamentos Forenses y DFIR** contiene el programa educativo 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”

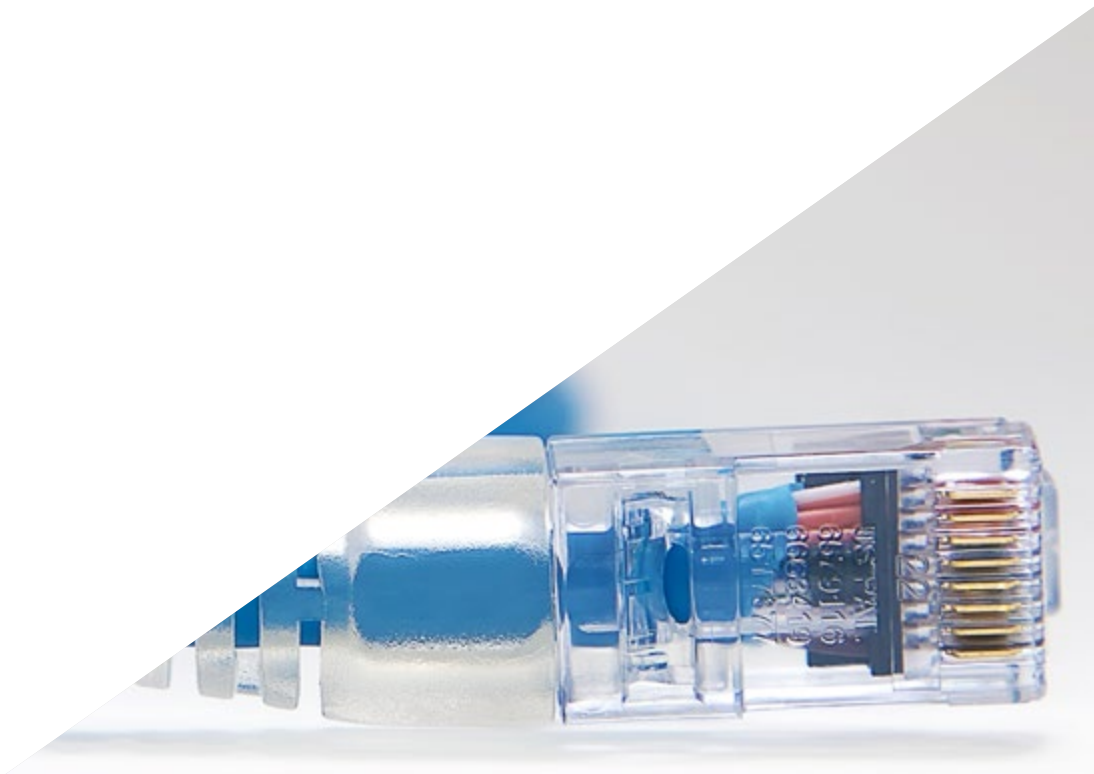
¿Necesitas recuperar datos de medios dañados? TECH te brinda las mejores herramientas para lograrlo.

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

El programa incluye en su cuadro docente a profesionales del sector que vierten en esta capacitación la experiencia de su trabajo, además de reconocidos especialistas de sociedades de referencia y universidades de prestigio.

Su contenido multimedia, elaborado con la última tecnología educativa, permitirá al profesional un aprendizaje situado y contextual, es decir, un entorno simulado que proporcionará una capacitación inmersiva programada para entrenarse ante situaciones reales.

El diseño de este programa se centra en el Aprendizaje Basado en Problemas, mediante el cual el profesional deberá tratar de resolver las distintas situaciones de práctica profesional que se le planteen a lo largo del curso académico. Para ello, contará con la ayuda de un novedoso sistema de vídeo interactivo realizado por reconocidos expertos.



02

Objetivos

El 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

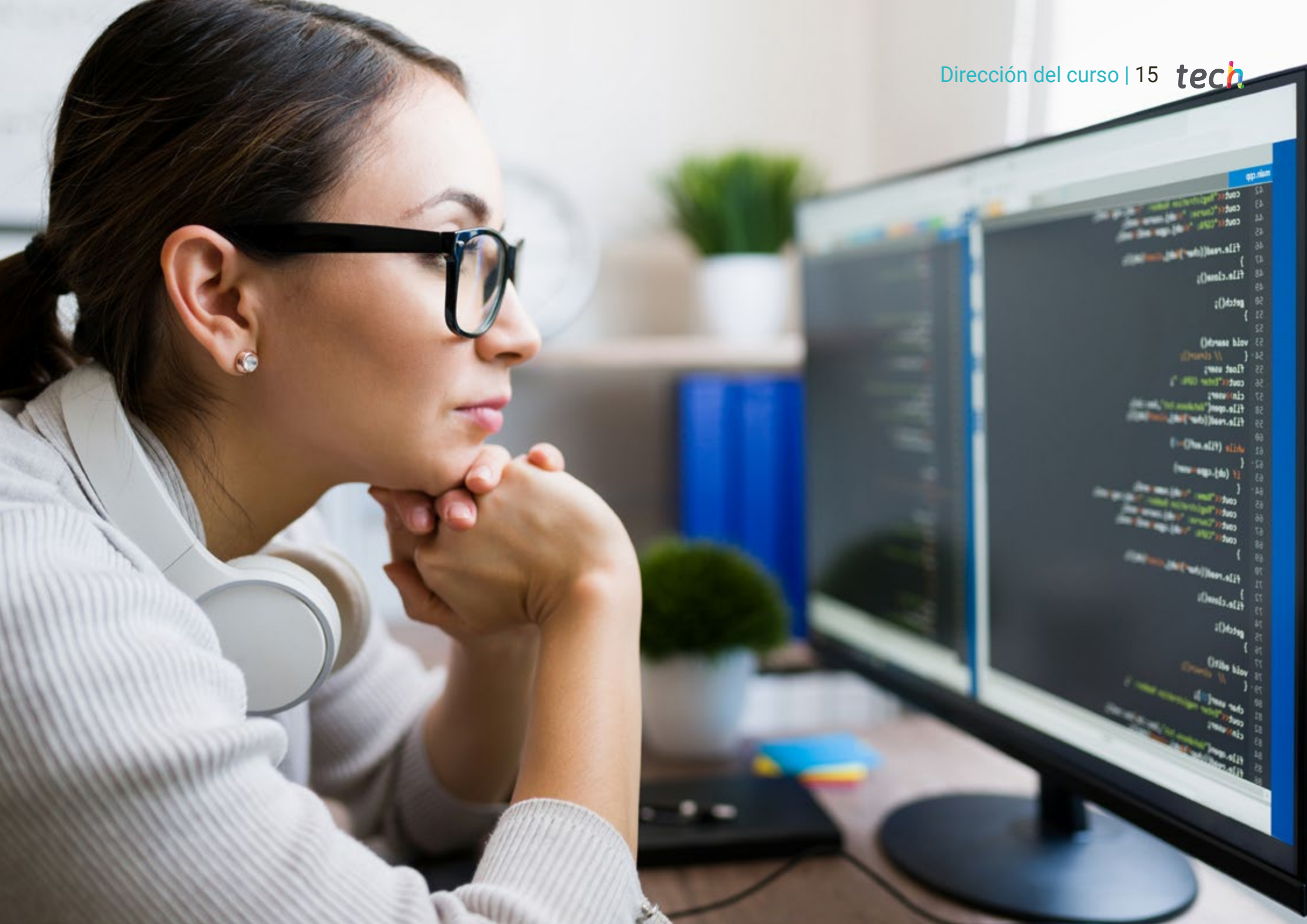
En su compromiso de ofrecer una educación basada en la excelencia, TECH cuenta con profesionales de prestigio internacional. Estos profesionales de la ciberseguridad tienen un amplio bagaje laboral, por lo que mediante la presente capacitación ofrecen las herramientas más eficaces para que los alumnos 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

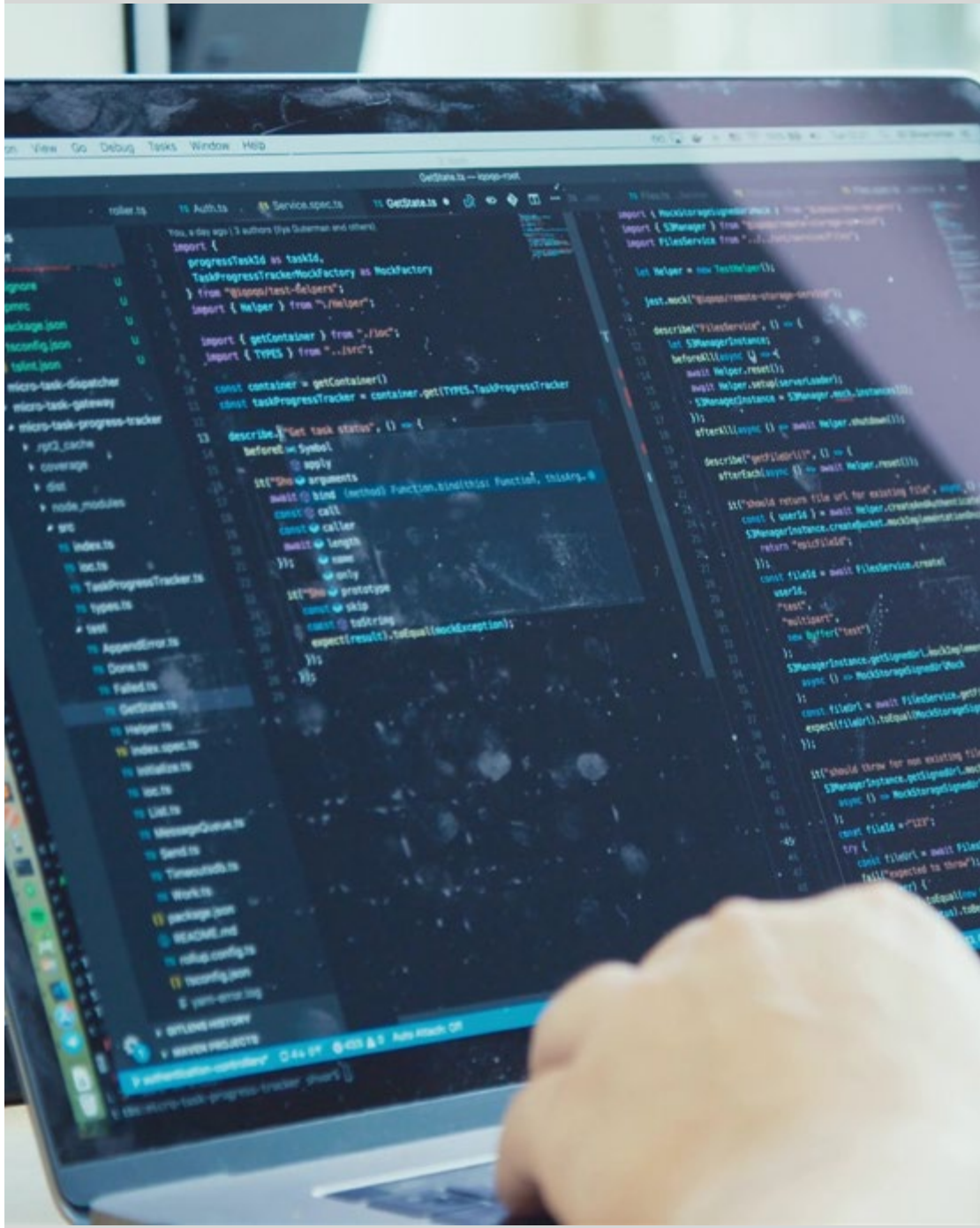
1.3. Sistemas de Archivos y Estructura de Datos
- 1.3.1. Principales sistemas de archivos
- 1.3.2. Métodos de ocultamiento de datos
- 1.3.3. Análisis de metadatos y atributos de archivos

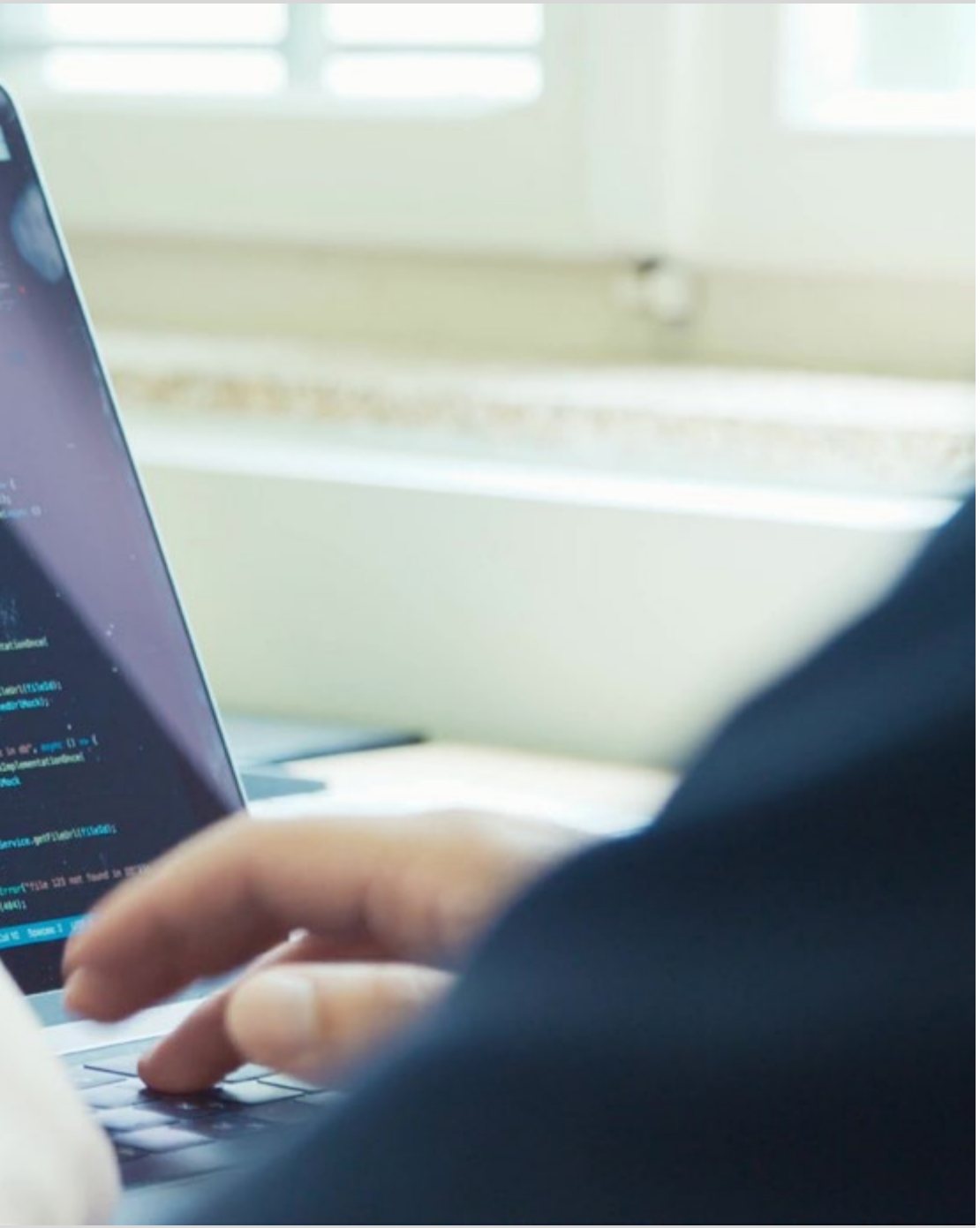
1.4. Análisis de Sistemas Operativos
- 1.4.1. Análisis forense de sistemas Windows
- 1.4.2. Análisis forense de sistemas Linux
- 1.4.3. Análisis forense de sistemas macOS

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

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

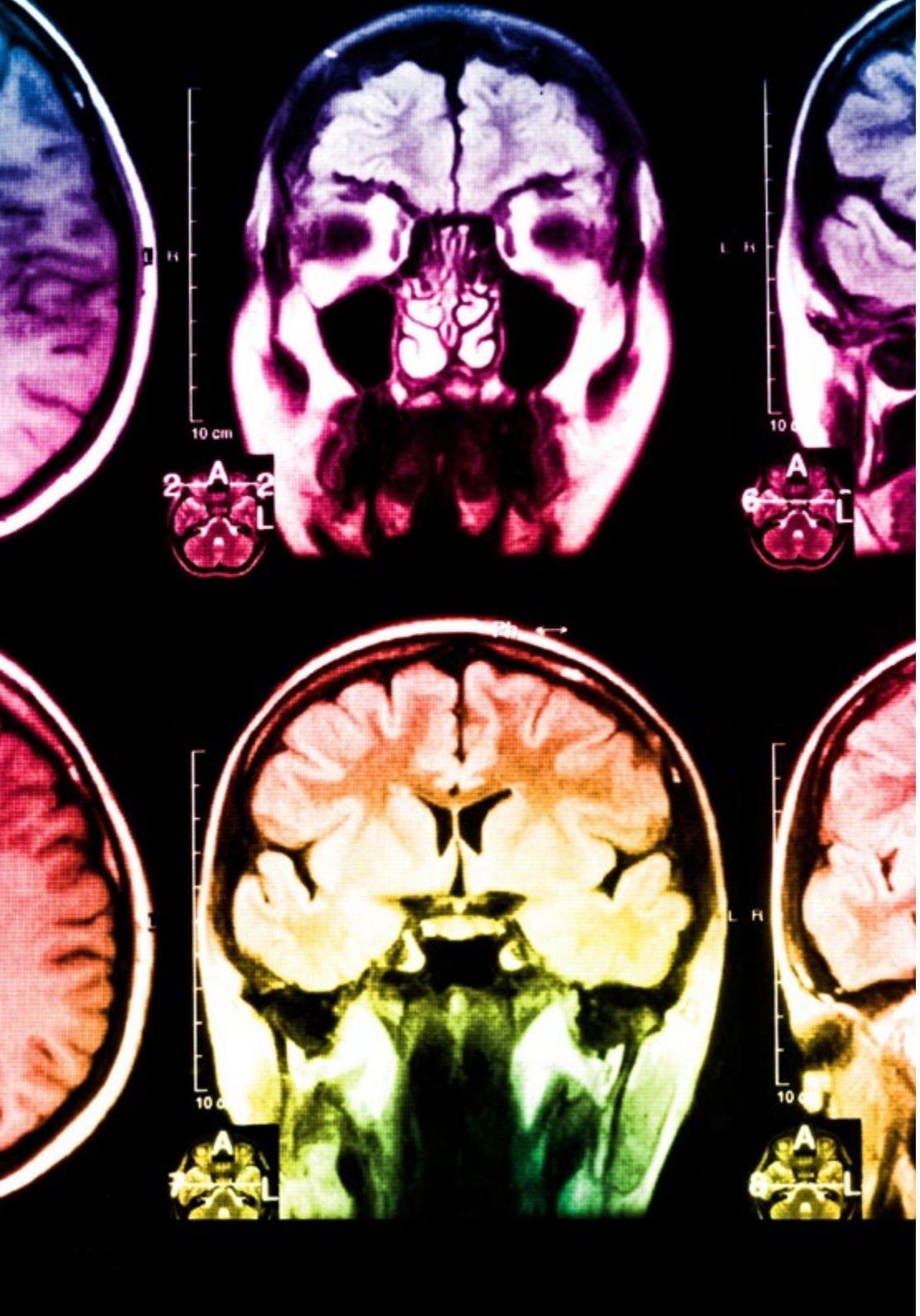
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

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.

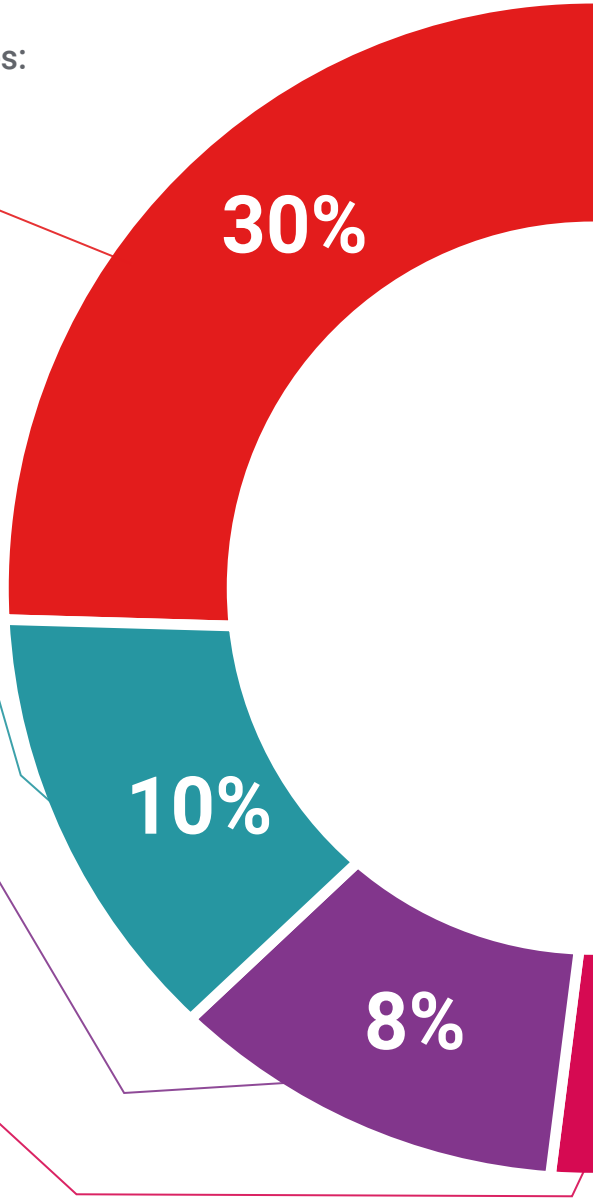
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

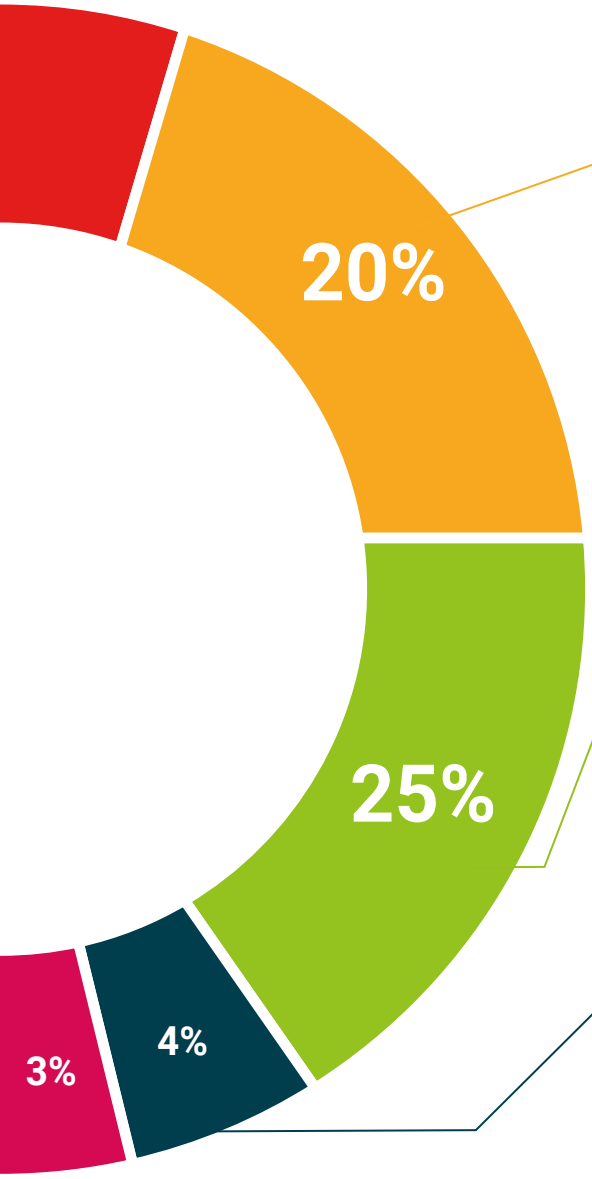
Prácticas de habilidades y competencias

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 Curso Universitario en Fundamentos Forenses y DFIR garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Curso Universitario expedido por TECH Global University.

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

Este programa te permitirá obtener el título propio de **Curso Universitario en Fundamentos Forenses y DFIR** avalado por **TECH Global University**, la mayor Universidad digital del mundo.

TECH Global University, es una Universidad Oficial Europea reconocida públicamente por el Gobierno de Andorra (***boletín oficial***). Andorra forma parte del Espacio Europeo de Educación Superior (EEES) desde 2003. El EEES es una iniciativa promovida por la Unión Europea que tiene como objetivo organizar el marco formativo internacional y armonizar los sistemas de educación superior de los países miembros de este espacio. El proyecto promueve unos valores comunes, la implementación de herramientas conjuntas y fortaleciendo sus mecanismos de garantía de calidad para potenciar la colaboración y movilidad entre estudiantes, investigadores y académicos.

Este título propio de **TECH Global University**, es un programa europeo de formación continua y actualización profesional que garantiza la adquisición de las competencias en su área de conocimiento, confiriendo un alto valor curricular al estudiante que supere el programa.

Título: **Curso Universitario en Fundamentos Forenses y DFIR**

Modalidad: **online**

Duración: **6 semanas**

Acreditación: **6 ECTS**


tech global university

D/Dña _____, con documento de identificación _____ ha superado con éxito y obtenido el título de:

Curso Universitario en Fundamentos Forenses y DFIR

Se trata de un título propio de 180 horas de duración equivalente a 6 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH Global University es una universidad reconocida oficialmente por el Gobierno de Andorra el 31 de enero de 2024, que pertenece al Espacio Europeo de Educación Superior (EEES).

En Andorra la Vella, a 28 de febrero de 2024

Dr. Pedro Navarro Illana
Rector

código único TECH: AFWDR2SS 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 Global University realizará las gestiones oportunas para su obtención, con un coste adicional.

tech global university

Curso Universitario
Fundamentos Forenses y DFIR

- Modalidad: **online**
- Duración: **6 semanas**
- Titulación: **TECH Global University**
- Acreditación: **6 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Curso Universitario
Fundamentos Forenses y DFIR

tech global university