# Experto Universitario
## Ciberseguridad Correctiva y Peritaje Forense

tech universidad ULAC

tech universidad ULAC

# Experto Universitario
## Ciberseguridad Correctiva y Peritaje Forense

- Modalidad: **online**
- Duración: **6 meses**
- Titulación: **TECH Universidad ULAC**
- Acreditación: **18 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: **www.techtitute.com/informatica/experto-universitario/experto-ciberseguridad-correctiva-peritaje-forense**

# Índice


01
Presentación
*pág. 4*

02
Objetivos
*pág. 8*

03
Dirección de curso
*pág. 12*

04
Estructura y contenido
*pág. 18*

05
Metodología
*pág. 24*

06
Titulación
*pág. 32*

01

# Presentación

En un mundo que cambia y evoluciona cada día, con unas tecnologías que aparecen y se adoptan rápidamente sin estar maduras tenemos que estar preparados para afrontar gran cantidad de retos y predecir el impacto que van a tener en la sociedad. Este programa forma al Ingeniero Informático para investigar un incidente de ciberseguridad una vez que se ha producido, dotándole de conocimientos y mecanismos para obtener, analizar y plasmar en un informe todos sus hallazgos, desde que un forense encuentra un escenario, y decide, de forma no destructiva, adquirir las pruebas, necesita unas pautas para relacionar los datos obtenidos de diferentes fuentes y llegar a unas conclusiones irrefutables.

*Adquiere la capacidad de dar las claves de un incidente de ciberseguridad con los conocimientos más actualizados en peritaje forense en esta área"*

En el entorno informático existen diversas motivaciones que llevan a aplicar diferentes Técnicas de Ingeniería Inversa para entender y conocer lo suficiente un software, un protocolo de comunicación o un algoritmo.

Una de las aplicaciones más conocidas de la ingeniería inversa es el análisis de *malware* que, mediante diferentes técnicas como el *Sandboxing*, permitirá entender y conocer el software dañino que se estudia y, con ello, el desarrollo de un software que sea capaz de detectarlo y contrarrestarlo, como el caso de los antivirus que trabajan por firmas.

En ocasiones, la vulnerabilidad no se encuentra en el código fuente, sino que es introducida por el compilador que genera el código máquina. Los conocimientos en ingeniería inversa y, por tanto, en cómo obtenemos el código máquina nos permitirán detectar dichas vulnerabilidades.

Es necesario conocer los diferentes escenarios, entender las diferentes tecnologías y poder explicarlos en diferentes lenguajes en función del público al que va dirigido el informe en concreto. La cantidad de diferentes delitos a los que se va a enfrentar un perito forense hace que necesite de pericia, perspicacia y serenidad para acometer esta tarea sumamente importante ya que de su correcto desempeño puede depender el veredicto de un juicio.

Para ello, esta titulación universitaria cuenta con *Masterclasses* exclusivas que le servirán al alumno para ahondar un poco más en la Ciberseguridad Correctiva y el Peritaje Forense. Estas lecciones extra han sido elaboradas por un docente de relevancia internacional, dada su amplia experiencia y trayectoria profesional en el campo de la Inteligencia, la Ciberseguridad y las Tecnologías Disruptivas.

El profesional de este sector necesita tener una visión amplia y periférica para detectar no sólo los beneficios de estas tecnologías, sino también los posibles perjuicios de las mismas. Este programa prepara para entender lo que vendrá, cómo puede afectar a profesiones presentes, a la forma de ejercerlas y qué puede ocurrir en un futuro, a veces incierto.

Este **Experto Universitario en Ciberseguridad Correctiva y Peritaje Forense** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

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

*"Las Masterclasses impartidas por un especialista en Ciberseguridad serán clave para tu aprendizaje a través de este Experto Universitario"*

*Con un planteamiento totalmente centrado en la práctica, este Experto Universitario impulsará tu capacidad hasta el nivel de un especialista"*

*Un aprendizaje que te permitirá intervenir como perito forense en ciberseguridad, en el área jurídica.*

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

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

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

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

02

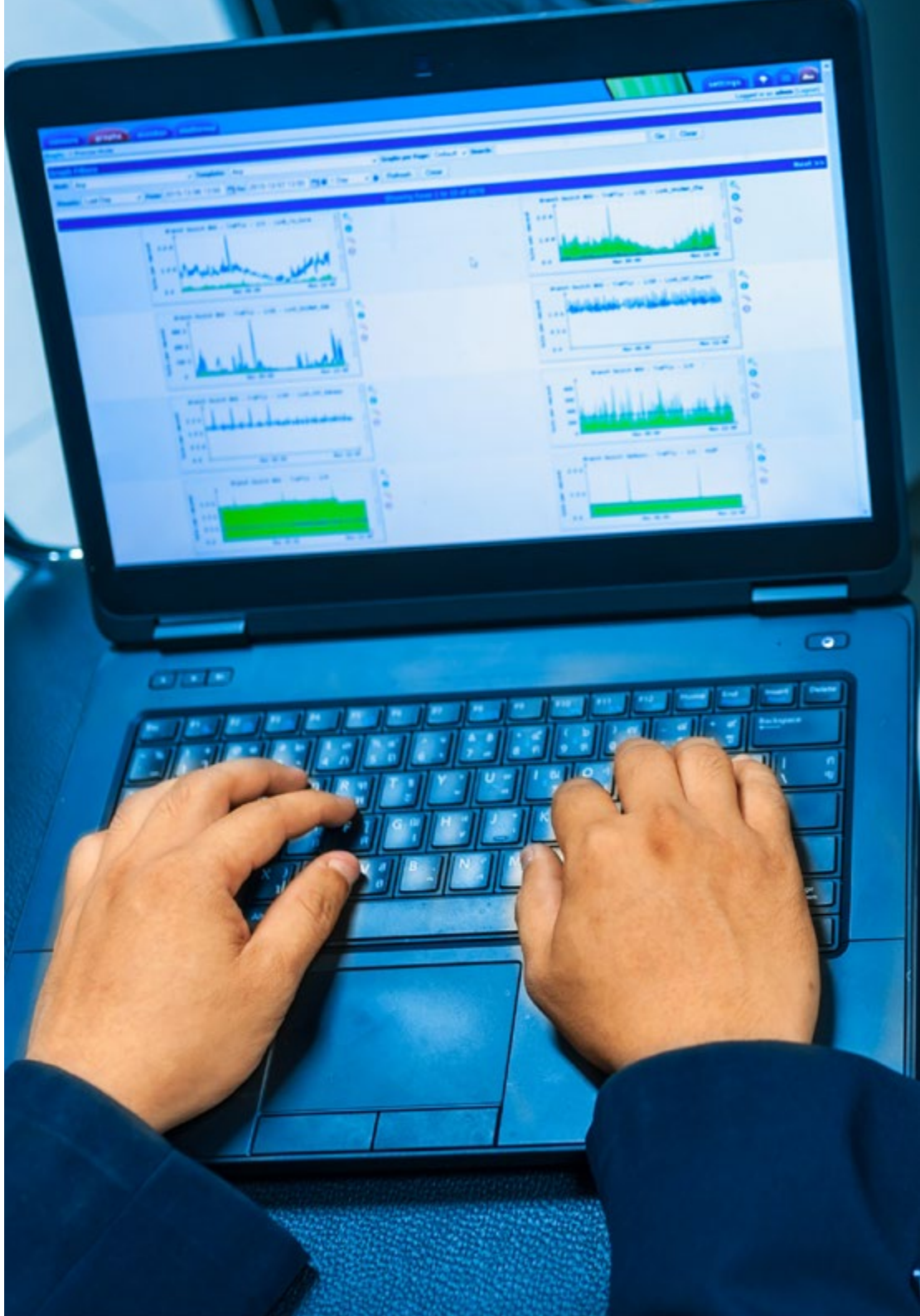
# Objetivos

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

*Un aprendizaje intensivo en Ciberseguridad Correctiva y Peritaje Forense que te permitirá ampliar tu campo de trabajo en un área llena de posibilidades laborales"*

## Objetivos generales

- Analizar la Ingeniería Inversa y las diferentes técnicas
- Examinar las diferentes arquitecturas y cómo afectan en la Ingeniería Inversa
- Determinar en qué condiciones usar las diferentes técnicas de Ingeniería Inversa
- Aplicar la Ingeniería Inversa al entorno de la Ciberseguridad
- Recopilar todas las pruebas y datos existentes para llevar a cabo un informe forense
- Analizar los datos y correlacionarlos debidamente
- Preservar las pruebas para llevar a cabo un Informe Forense
- Presentar debidamente el Informe Forense
- Analizar el estado actual y futuro de la seguridad informática
- Examinar los riesgos de las nuevas tecnologías emergentes
- Compilar las distintas tecnologías en relación a la Seguridad Informática



## Objetivos específicos

### Módulo 1. Ingeniería Inversa

- Analizar las fases de un compilador
- Examinar la arquitectura de procesadores x86 y la arquitectura de procesadores ARM
- Determinar los diferentes tipos de análisis
- Aplicar *Sandboxing* en diferentes entornos
- Desarrollar las diferentes técnicas de análisis de *malware*
- Establecer las herramientas orientadas al análisis de *malware*

### Módulo 2. Análisis Forense

- Identificar los diferentes elementos que ponen en evidencia un delito
- Generar conocimiento especializado para obtener los datos de los diferentes medios antes de que se pierdan
- Recuperar los datos que hayan sido borrados intencionadamente
- Analizar los registros y los logs de los sistemas
- Determinar cómo se duplican los datos para no alterar los originales
- Fundamentar las pruebas para que sean consistentes
- Generar un informe sólido y sin fisuras
- Presentar las conclusiones de forma coherente
- Establecer cómo defender el informe ante la autoridad competente
- Concretar estrategias para que el teletrabajo sea seguro

### Módulo 3. Retos actuales y futuros en Seguridad Informática

- Examinar el uso de las Criptomonedas, el impacto en la economía y la seguridad
- Analizar la situación de los usuarios y el grado de analfabetismo digital
- Determinar el ámbito de uso de *Blockchain*
- Presentar alternativas a IPv4 en el Direccionamiento de Redes
- Desarrollar estrategias para formar a la población en el uso correcto de las tecnologías
- Generar conocimiento especializado para hacer frente a los nuevos retos de seguridad y evitar la suplantación de identidad
- Concretar estrategias para que el teletrabajo sea seguro

*"Adquiere la competencia necesaria para preparar y presentar un informe completo y de calidad ante la autoridad competente"*

03

# Dirección del curso

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

*Docentes expertos en ciberseguridad te acompañarán en cada fase del estudio y te darán la visión más realista de este trabajo"*

## Director Invitado Internacional

El Doctor Frederic Lemieux es reconocido a nivel internacional como experto innovador y líder inspirador en los campos de la **Inteligencia**, **Seguridad Nacional**, **Seguridad Interna**, **Ciberseguridad** y **Tecnologías Disruptivas**. Y es que su constante dedicación y relevantes aportaciones en Investigación y Educación, le posicionan como una figura clave en la **promoción de la seguridad** y el **entendimiento de las tecnologías emergentes** en la actualidad. Durante su trayectoria profesional, ha conceptualizado y dirigido programas académicos de vanguardia en diversas instituciones de renombre, como la **Universidad de Montreal**, la **Universidad George Washington** y **la Universidad de Georgetown.**

A lo largo de su extenso bagaje, ha publicado múltiples libros de gran relevancia, todos ellos relacionados con la **inteligencia criminal**, la **labor policial**, las **amenazas cibernéticas** y la **seguridad internacional**. Asimismo, ha contribuido de manera significativa al campo de la **Ciberseguridad** con la publicación de numerosos artículos en revistas académicas, las cuales examinan el control del crimen durante desastres importantes, la lucha contra el terrorismo, las agencias de inteligencia y la cooperación policial. Además, ha sido panelista y ponente principal en diversas conferencias nacionales e internacionales, consolidándose como un referente en el ámbito académico y profesional.

El Doctor Lemieux ha desempeñado roles editoriales y evaluativos en diferentes organizaciones académicas, privadas y gubernamentales, reflejando su influencia y compromiso con la excelencia en su campo de especialización. De esta forma, su prestigiosa carrera académica lo ha llevado a desempeñarse como Profesor de Prácticas y Director de Facultad de los programas MPS en **Inteligencia Aplicada**, **Gestión de Riesgos en Ciberseguridad**, **Gestión Tecnológica** y **Gestión de Tecnologías de la Información** en la **Universidad de Georgetown.**

## Dr. Lemieux, Frederic

- Director del Máster en Cybersecurity Risk Management en Georgetown, Washington, Estados Unidos
- Director del Máster en Technology Management en la Universidad de Georgetown
- Director del Máster en Applied Intelligence en la Universidad de Georgetown
- Profesor de Prácticas en la Universidad de Georgetown
- Doctor en Criminología por la School of Criminology en la Universidad de Montreal
- Licenciado en Sociología y Minor Degree en Psicología por la Universidad de Laval
- Miembro de: New Program Roundtable Committee, Universidad de Georgetown

*"Gracias a TECH podrás aprender con los mejores profesionales del mundo"*

## Dirección

### Dña. Fernández Sapena, Sonia

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

## Profesores

**D. Redondo, Jesús Serrano**

- Desarrollador Web y Técnico en Ciberseguridad
- Desarrollador Web en Roams, Palencia
- Desarrollador *FrontEnd* en Telefónica, Madrid
- Desarrollador *FrontEnd* en Best Pro Consulting SL, Madrid
- Instalador de Equipos y Servicio de Telecomunicaciones en Grupo Zener, Castilla y León
- Instalador de Equipos y Servicios de Telecomunicaciones en Lican Comunicaciones SL, Castilla y León
- Certificado en Seguridad Informática por CFTIC Getafe, Madrid
- Técnico Superior en Sistemas Telecomunicaciones e Informáticos por IES Trinidad Arroyo, Palencia
- Técnico Superior en Instalaciones Electrotécnicas MT y BT por IES Trinidad Arroyo, Palencia
- Formación en Ingeniería Inversa, Estenografía y Cifrado por la Academia Hacker Incibe

*"Un estimulante viaje de crecimiento profesional concebido para mantener tu interés y su motivación durante toda la capacitación"*

04

# Estructura y contenido

Este Experto Universitario es un análisis completo de todos y cada uno de los campos de conocimiento que el profesional que interviene en ciberseguridad debe conocer en el ámbito de la ciberseguridad correctiva y el peritaje forense. Para ello se ha estructurado con vistas a la adquisición eficiente de conocimientos sumatorios, que propicien la penetración de los aprendizajes y consoliden lo estudiado dotando al alumnado de capacidad de intervención de la manera más rápida posible. Un recorrido de alta intensidad y enorme calidad creado para capacitar a los mejores del sector.

*Todos los conceptos de la Ciberseguridad Correctiva y Peritaje Forense desarrollados de forma estructurada en un planteamiento de estudio centrado en la eficiencia"*

## **Módulo 1.** Ingeniería Inversa

1.1. Compiladores
- 1.1.1. Tipos de códigos
- 1.1.2. Fases de un compilador
- 1.1.3. Tabla de símbolos
- 1.1.4. Gestor de errores
- 1.1.5. Compilador GCC

1.2. Tipos de análisis en compiladores
- 1.2.1. Análisis léxico
  - 1.2.1.1. Terminología
  - 1.2.1.2. Componentes léxicos
  - 1.2.1.3. Analizador léxico LEX
- 1.2.2. Análisis sintáctico
  - 1.2.2.1. Gramáticas libres de contexto
  - 1.2.2.2. Tipos de análisis sintácticos
    - 1.2.2.2.1. Análisis descendente
    - 1.2.2.2.2. Análisis ascendente
  - 1.2.2.3. Árboles sintácticos y derivaciones
  - 1.2.2.4. Tipos de analizadores sintácticos
    - 1.2.2.4.1. Analizadores LR (*Left to Right*)
    - 1.2.2.4.2. Analizadores LALR
- 1.2.3. Análisis semántico
  - 1.2.3.1. Gramáticas de atributos
  - 1.2.3.2. S-Atribuidas
  - 1.2.3.3. L-Atribuidas

1.3. Estructuras de datos en ensamblador
- 1.3.1. Variables
- 1.3.2. Arrays
- 1.3.3. Punteros
- 1.3.4. Estructuras
- 1.3.5. Objetos

1.4. Estructuras de código en ensamblador
- 1.4.1. Estructuras de selección
  - 1.4.1.1. *If, else if, Else*
  - 1.4.1.2. *Switch*
- 1.4.2. Estructuras de iteración
  - 1.4.2.1. *For*
  - 1.4.2.2. *While*
  - 1.4.2.3. Uso del *break*
- 1.4.3. Funciones

1.5. Arquitectura Hardware x86
- 1.5.1. Arquitectura de procesadores x86
- 1.5.2. Estructuras de datos en x86
- 1.5.3. Estructuras de código en x86

1.6. Arquitectura Hardware ARM
- 1.6.1. Arquitectura de procesadores ARM
- 1.6.2. Estructuras de datos en ARM
- 1.6.3. Estructuras de código en ARM

1.7. Análisis de código estático
- 1.7.1. Desensambladores
- 1.7.2. IDA
- 1.7.3. Reconstructores de código

1.8. Análisis de código dinámico
- 1.8.1. Análisis del comportamiento
  - 1.8.1.1. Comunicaciones
  - 1.8.1.2. Monitorización
- 1.8.2. Depuradores de código en Linux
- 1.8.3. Depuradores de código en Windows

1.9. *Sandbox*
- 1.9.1. Arquitectura de un *Sandbox*
- 1.9.2. Evasión de un *Sandbox*
- 1.9.3. Técnicas de detección
- 1.9.4. Técnicas de evasión
- 1.9.5. Contramedidas
- 1.9.6. *Sandbox* en Linux
- 1.9.7. *Sandbox* en Windows
- 1.9.8. *Sandbox* en MacOS
- 1.9.9. *Sandbox* en Android

1.10. Análisis de *malware*
- 1.10.1. Métodos de análisis de *malware*
- 1.10.2. Técnicas de ofuscación de *malware*
  - 1.10.2.1. Ofuscación de ejecutables
  - 1.10.2.2. Restricción de entornos de ejecución
- 1.10.3. Herramientas de análisis de *malware*

## **Módulo 2.** Análisis Forense

2.1. Adquisición de datos y duplicación
- 2.1.1. Adquisición de datos volátiles
  - 2.1.1.1. Información del sistema
  - 2.1.1.2. Información de la red
  - 2.1.1.3. Orden de volatilidad
- 2.1.2. Adquisición de datos estáticos
  - 2.1.2.1. Creación de una imagen duplicada
  - 2.1.2.2. Preparación de un documento para la cadena de custodia
- 2.1.3. Métodos de validación de los datos adquiridos
  - 2.1.3.1. Métodos para Linux
  - 2.1.3.2. Métodos para Windows

2.2. Evaluación y derrota de técnicas anti-forenses
- 2.2.1. Objetivos de las técnicas anti-forenses
- 2.2.2. Borrado de datos
  - 2.2.2.1. Borrado de datos y ficheros
  - 2.2.2.2. Recuperación de archivos
  - 2.2.2.3. Recuperación de particiones borradas
- 2.2.3. Protección por contraseña
- 2.2.4. Esteganografía
- 2.2.5. Borrado seguro de dispositivos
- 2.2.6. Encriptación

2.3. Análisis Forense del sistema operativo
- 2.3.1. Análisis Forense de Windows
- 2.3.2. Análisis Forense de Linux
- 2.3.3. Análisis Forense de Mac

2.4. Análisis Forense de la red
- 2.4.1. Análisis de los *logs*
- 2.4.2. Correlación de datos
- 2.4.3. Investigación de la red
- 2.4.4. Pasos a seguir en el análisis forense de la red

2.5. Análisis Forense Web
- 2.5.1. Investigación de los ataques webs
- 2.5.2. Detección de ataques
- 2.5.3. Localización de direcciones IPs

2.6. Análisis Forense de Dases de Fatos
- 2.6.1. Análisis Forense en MSSQL
- 2.6.2. Análisis Forense en MySQL
- 2.6.3. Análisis Forense en PostgreSQL
- 2.6.4. Análisis Forense en MongoDB

2.7. Análisis Forense en Cloud
- 2.7.1. Tipos de Crímenes en Cloud
  - 2.7.1.1. Cloud como Sujeto
  - 2.7.1.2. Cloud como Objeto
  - 2.7.1.3. Cloud como Herramienta
- 2.7.2. Retos del Análisis Forense en Cloud
- 2.7.3. Investigación de los servicios de Almacenamiento el Cloud
- 2.7.4. Herramientas de Análisis forense para Cloud

2.8. Investigación de crímenes de Correo Electrónico
- 2.8.1. Sistemas de correo
  - 2.8.1.1. Clientes de Correo
  - 2.8.1.2. Servidor de Correo
  - 2.8.1.3. Servidor SMTP
  - 2.8.1.4. Servidor POP3
  - 2.8.1.5. Servidor IMAP4
- 2.8.2. Crímenes de correo
- 2.8.3. Mensaje de Correo
  - 2.8.3.1. Cabeceras Estándar
  - 2.8.3.2. Cabeceras Extendidas
- 2.8.4. Pasos para la investigación de estos crímenes
- 2.8.5. Herramientas Forenses para correo electrónico

2.9. Análisis Forense de Móviles
- 2.9.1. Redes Celulares
  - 2.9.1.1. Tipos de redes
  - 2.9.1.2. Contenidos del CDR
- 2.9.2. *Subscriber Identity Module* (SIM)
- 2.9.3. Adquisición lógica
- 2.9.4. Adquisición física
- 2.9.5. Adquisición del sistema de ficheros

2.10. Redacción y presentación de Informes Forenses
- 2.10.1. Aspectos importantes de un Informe Forense
- 2.10.2. Clasificación y tipos de informes
- 2.10.3. Guía para escribir un informe
- 2.10.4. Presentación del informe
  - 2.10.4.1. Preparación previa para testificar
  - 2.10.4.2. Deposición
  - 2.10.4.3. Trato con los medios

## **Módulo 3.** Retos Actuales y Futuros en Seguridad Informática

3.1. Tecnología *Blockchain*
- 3.1.1. Ámbitos de aplicación
- 3.1.2. Garantía de confidencialidad
- 3.1.3. Garantía de no-repudio

3.2. Dinero digital
- 3.2.1. Bitcoins
- 3.2.2. Critpomonedas
- 3.2.3. Minería de Criptomonedas
- 3.2.4. Estafas piramidales
- 3.2.5. Otros potenciales delitos y problemas

3.3. *Deepfake*
- 3.3.1. Impacto en los medios
- 3.3.2. Peligros para la sociedad
- 3.3.3. Mecanismos de detección

3.4. El futuro de la inteligencia artificial
- 3.4.1. Inteligencia artificial y computación cognitiva
- 3.4.2. Usos para simplificar el servicio a clientes

3.5. Privacidad digital
- 3.5.1. Valor de los datos en la red
- 3.5.2. Uso de los datos en la red
- 3.5.3. Gestión de la privacidad e identidad digital

3.6. Ciberconflictos, cibercriminales y ciberataques
- 3.6.1. Impacto de la ciberseguridad en conflictos internacionales
- 3.6.2. Consecuencias de ciberataques en la población general
- 3.6.3. Tipos de cibercriminales. Medidas de protección

3.7. Teletrabajo
- 3.7.1. Revolución del teletrabajo durante y post COVID-19
- 3.7.2. Cuellos de botella en el acceso
- 3.7.3. Variación de la superficie de ataque
- 3.7.4. Necesidades de los trabajadores

3.8. Tecnologías *Wireless* emergentes
- 3.8.1. WPA3
- 3.8.2. 5G
- 3.8.3. Ondas milimétricas
- 3.8.4. Tendencia en "*Get smart*" en vez de "*Get more*"

3.9. Direccionamiento futuro en redes
- 3.9.1. Problemas actuales con el direccionamiento IP
- 3.9.2. IPv6
- 3.9.3. IPv4+
- 3.9.4. Ventajas de IPv4+ sobre IPv4
- 3.9.5. Ventajas de IPv6 sobre IPv4

3.10. El reto de la concienciación de la formación temprana y continua de la población
- 3.10.1. Estrategias actuales de los gobiernos
- 3.10.2. Resistencia de la población al aprendizaje
- 3.10.3. Planes de formación que deben adoptar las empresas

*"Un temario de alto impacto para tus competencias que te permitirá intervenir con eficiencia en Ciberseguridad Correctiva y Peritaje Forense con los recursos de última generación"*

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

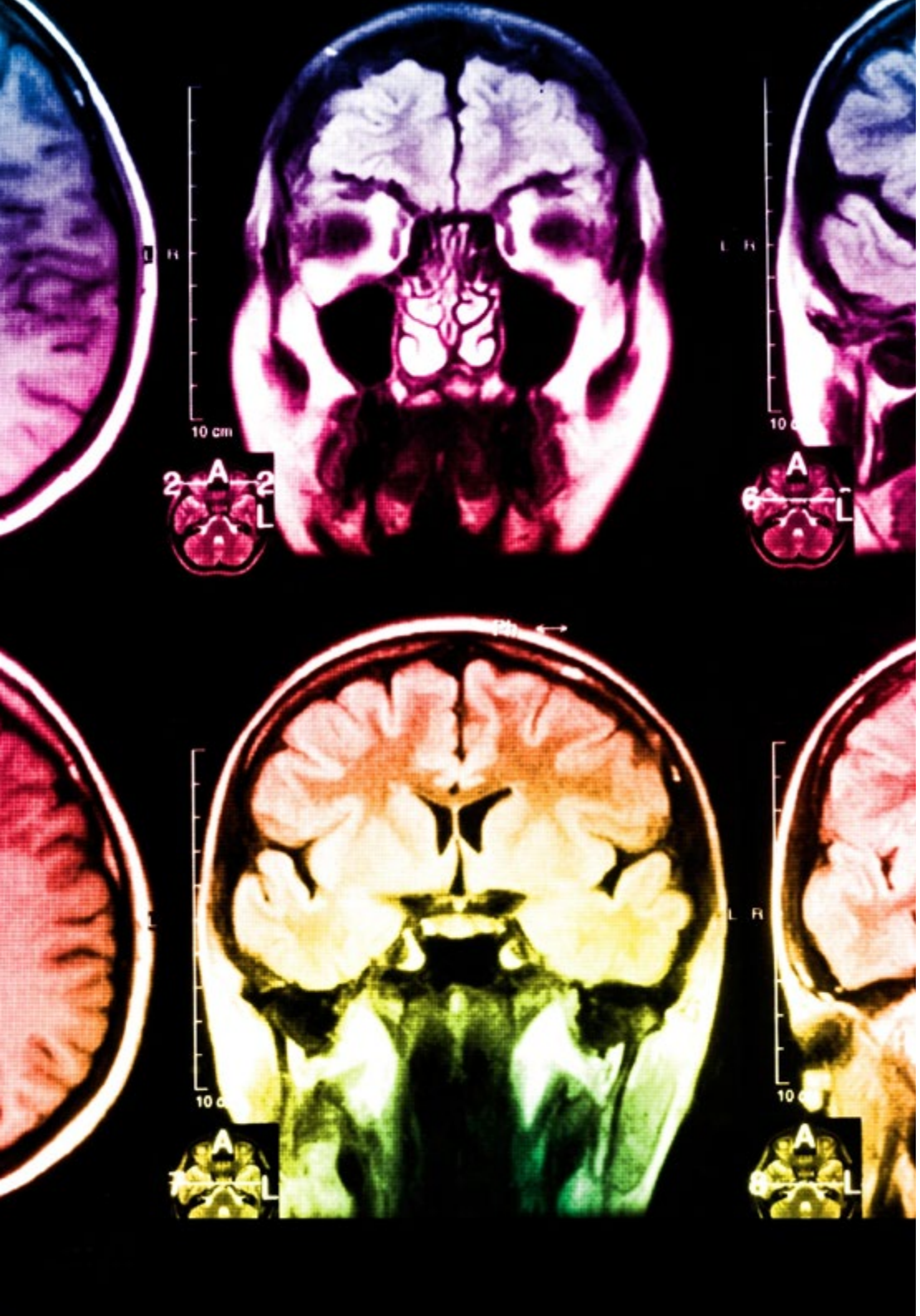
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

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.

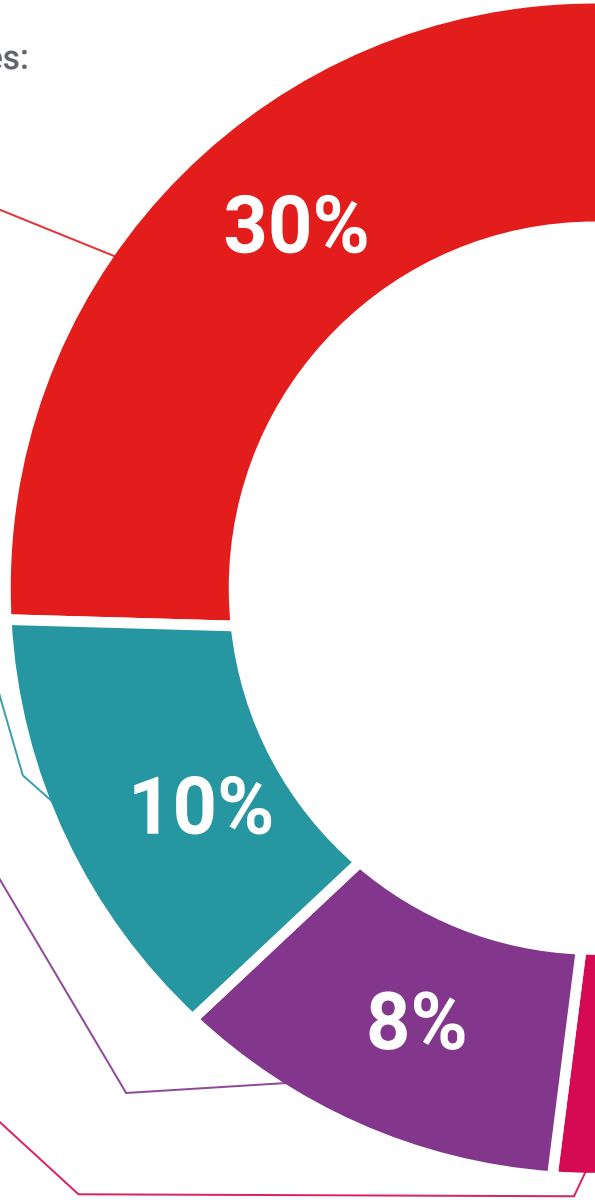
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

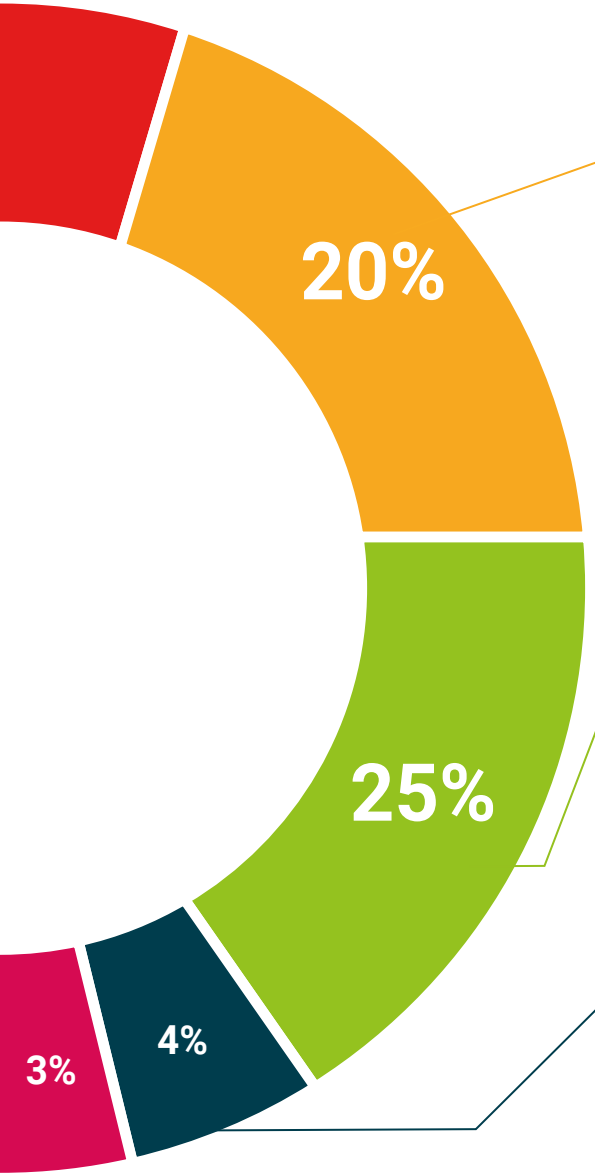
### Prácticas de habilidades y competencias

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 Experto Universitario en Ciberseguridad Correctiva y Peritaje Forense garantiza, además de la capacitación más rigurosa y actualizada, el acceso a dos diplomas de Experto Universitario, uno expedido por TECH Global University y otro expedido por la Universidad Latinoamericana y del Caribe.

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

El programa del **Experto Universitario en Ciberseguridad Correctiva y Peritaje Forense** es el más completo del panorama académico actual. A su egreso, el estudiante recibirá un diploma universitario emitido por TECH Global University, y otro por la Universidad Latinoamericana y del Caribe.

Estos títulos de formación permanente y actualización profesional de TECH Global University y Universidad Latinoamericana y del Caribe garantizan la adquisición de competencias en el área de conocimiento, otorgando un alto valor curricular al estudiante que supere las evaluaciones y acredite el programa tras cursarlo en su totalidad.

Este doble reconocimiento, de dos destacadas instituciones universitarias, suponen una doble recompensa a una formación integral y de calidad, asegurando que el estudiante obtenga una certificación reconocida tanto a nivel nacional como internacional. Este mérito académico le posicionará como un profesional altamente capacitado y preparado para enfrentar los retos y demandas en su área profesional.

Título: **Experto Universitario en Ciberseguridad Correctiva y Peritaje Forense**

Modalidad: **online**

Duración: **6 meses**

Acreditación: **18 ECTS**

UNIVERSIDAD
LATINOAMERICANA Y DEL CARIBE

CERTIFICA A:

_____

**Identificación:** _____

Por haber superado con éxito y obtenido el título de:

**EXPERTO UNIVERSITARIO EN CIBERSEGURIDAD CORRECTIVA Y PERITAJE FORENSE**

En la ciudad de Caracas a los 04 días del mes de diciembre de 2023

**Dr. Elmo Bell-Smythe**
Rector de la ULAC

**Raúl Aramayo**
CEO de La Vida Integral

Verifique la validez y autenticidad de este Certificado escaneando el código QR

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

**Experto Universitario en Ciberseguridad Correctiva y Peritaje Forense**

Se trata de un título propio de 450 horas de duración equivalente a 18 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: 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 Universidad ULAC realizará las gestiones oportunas para su obtención, con un coste adicional.

tech universidad ULAC

# Experto Universitario
## Ciberseguridad Correctiva y Peritaje Forense

- Modalidad: **online**
- Duración: **6 meses**
- Titulación: **TECH Universidad ULAC**
- Acreditación: **18 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

# Experto Universitario
## Ciberseguridad Correctiva y Peritaje Forense

tech universidad ULAC