Diplomado

Análisis Forense en Ciberseguridad

tech universidad tecnológica

tech universidad tecnológica

Diplomado
Análisis Forense en Ciberseguridad

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

Acceso web: www.techtitute.com/informatica/curso-universitario/analisis-forense-ciberseguridad

Índice

01

Presentación

El Diplomado en Análisis Forense en Ciberseguridad es una herramienta de alta capacitación que forma al Ingeniero Informático para investigar un incidente de ciberseguridad una vez que se ha producido. Un proceso completo que dotará al alumno con los conocimientos necesarios para obtener, analizar y plasmar en un informe todos sus hallazgos. Con la calidad de un programa creado para capacitar a los mejores expertos del sector.

Consigue la capacidad de intervención de un especialista en el análisis forense de los ciberdelitos”

Los delitos informáticos, como cualquier delito, ponen en marcha una investigación que proporcione los datos necesarios para establecer las consecuencias legales que se derivan de su realización.

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.

Para poder realizar estas acciones 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.

Este curso pone a tu servicio los materiales de mejor calidad para el aprendizaje de todos los contenidos que el profesional debe incorporar a su praxis profesional en este sector.

Entre estos materiales didácticos, el egresado dispone de una exclusiva *Masterclass* que ha sido elaborada por un experto en Inteligencia, Ciberseguridad y Tecnologías Disruptivas. De este modo, el alumno tendrá a su alcance un aprendizaje más profundo en torno a las metodologías y procedimientos de análisis informático gracias a este profesional de prestigio internacional. Así, el egresado se actualizará en importantes conceptos tan relevantes desde la encriptación hasta la redacción y presentación de informes forenses.

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

- El desarrollo de casos prácticos presentados por expertos en ciberseguridad
- 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

Profundiza en el Análisis Forense de Ciberseguridad gracias a una Masterclass impartida por un reputado profesional internacional en Inteligencia, Ciberseguridad y Tecnologías Disruptivas”

Serás capaz de averiguar el origen de un problema, o de un delito, y recuperar los datos eliminados con propósitos legales o meramente prácticos”

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

Estudia a través de un Diplomado centrado en la práctica impulsando tu capacidad hasta el nivel de un especialista.

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 Diplomado en Análisis Forense en Ciberseguridad proporciona al alumnado competencias para el trabajo en este campo, de forma eficiente. Con objetivos realistas y de alto interés, este proceso de estudio se ha configurado, de forma progresiva a la adquisición de conocimientos teóricos y prácticos necesarios para una intervención de calidad, desarrollando, además, competencias transversales que permitirán afrontar situaciones complejas elaborando respuestas ajustadas y precisas.

Pon en marcha tu capacidad forense en informática, un campo de trabajo lleno de posibilidades laborales a través de un proceso de excepcional calidad de enseñanza"

Objetivos generales

- Recopilar todas las pruebas y datos existentes para llevar a cabo un informe forense
- Analizar los datos y relacionarlos debidamente
- Preservar las pruebas para llevar a cabo un informe forense
- Presentar debidamente el informe forense

Con los sistemas de apoyo al estudio más interesantes del momento, este programa es una oportunidad excepcional de crecimiento profesional"

Objetivos específicos

- Identificar los diferentes elementos que ponen en evidencia un delito
- Generar conocimiento especializado para la obtención de los datos de los diferentes medios antes de que se pierdan
- Recuperar los datos que hayan sido borrados intencionalmente
- 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

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 Análisis Forense 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

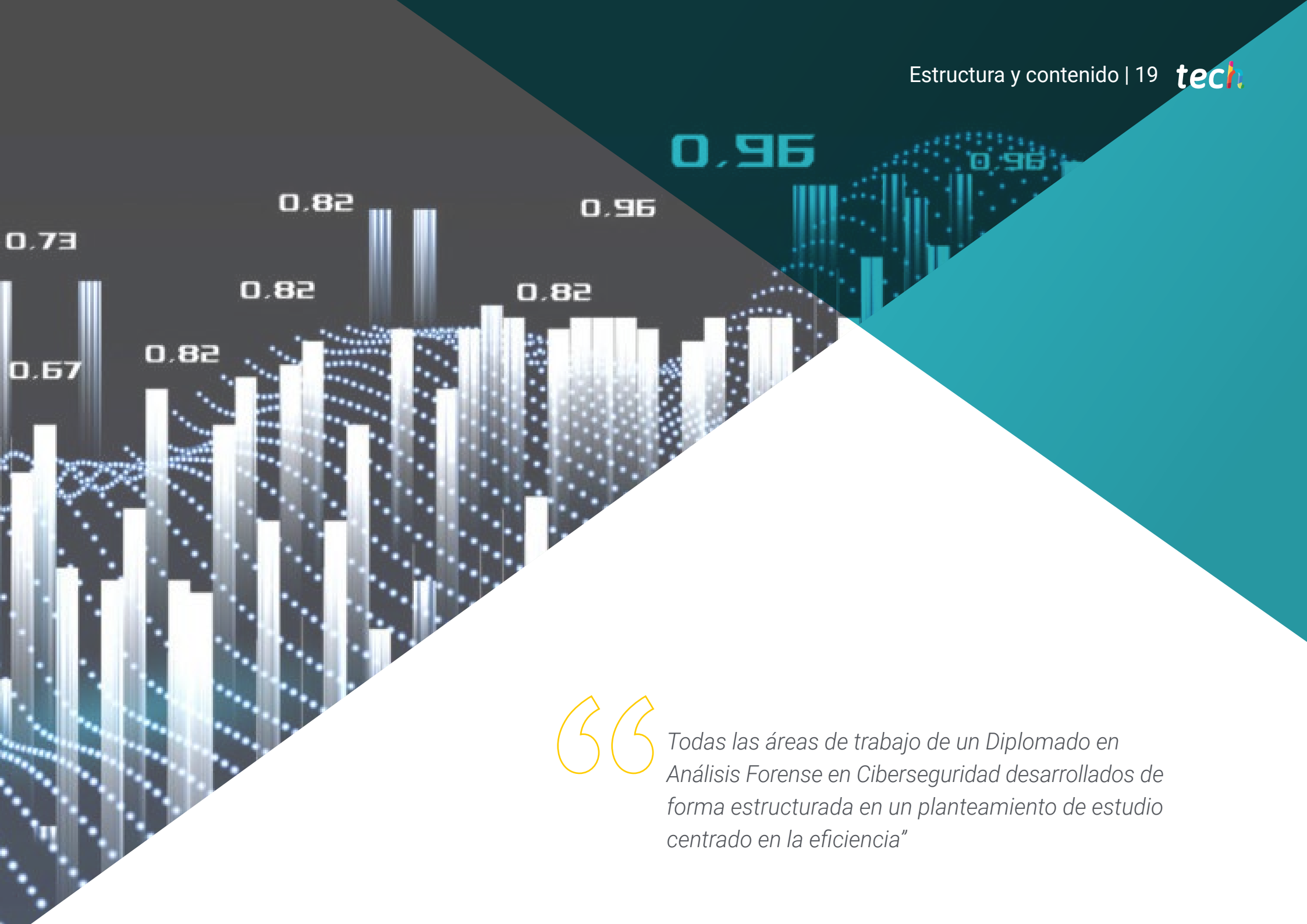
- Formadora de Seguridad Informática y Hacking Ético en el Centro de Referencia Nacional de Getafe en Informática y Telecomunicaciones de Madrid
- Instructora certificada E-Council
- Formadora en las siguientes certificaciones: EXIN Ethical Hacking Foundation y EXIN Cyber & IT Security Foundation. Madrid
- 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


CARBO
OFFSE
Ctrl

04

Estructura y contenido

A lo largo del desarrollo de los diferentes temas de este Diplomado el alumno podrá adquirir todos los conocimientos sobre la intervención en el ámbito legal en ciberseguridad y delitos informáticos que necesitan. Para ello el temario se ha estructurado con vistas a la adquisición eficiente de aprendizajes complementarios, que propicien la internalización de los aprendizajes y consoliden lo estudiado dotando al alumnado de capacidad de intervención de manera eficiente. Un recorrido de alta intensidad y enorme calidad creado para los mejores del sector.



Todas las áreas de trabajo de un Diplomado en Análisis Forense en Ciberseguridad desarrollados de forma estructurada en un planteamiento de estudio centrado en la eficiencia"

Módulo 1. Análisis Forense

1.1. Adquisición de datos y duplicación
- 1.1.1. Adquisición de datos volátiles
  - 1.1.1.1. Información del sistema
  - 1.1.1.2. Información de la red
  - 1.1.1.3. Orden de volatilidad
- 1.1.2. Adquisición de datos estáticos
  - 1.1.2.1. Creación de una imagen duplicada
  - 1.1.2.2. Preparación de un documento para la cadena de custodia
- 1.1.3. Métodos de validación de los datos adquiridos
  - 1.1.3.1. Métodos para Linux
  - 1.1.3.2. Métodos para Windows

1.2. Evaluación y derrota de técnicas antiforenses
- 1.2.1. Objetivos de las técnicas antiforenses
- 1.2.2. Borrado de datos
  - 1.2.2.1. Borrado de datos y ficheros
  - 1.2.2.2. Recuperación de archivos
  - 1.2.2.3. Recuperación de particiones borradas
- 1.2.3. Protección por contraseña
- 1.2.4. Esteganografía
- 1.2.5. Borrado seguro de dispositivos
- 1.2.6. Encriptación

1.3. Análisis forense del sistema operativo
- 1.3.1. Análisis forense de Windows
- 1.3.2. Análisis forense de Linux
- 1.3.3. Análisis forense de Mac

1.4. Análisis forense de la red
- 1.4.1. Análisis de los *logs*
- 1.4.2. Correlación de datos
- 1.4.3. Investigación de la red
- 1.4.4. Pasos a seguir en el análisis forense de la red

1.5. Análisis forense Web
- 1.5.1. Investigación de los ataques webs
- 1.5.2. Detección de ataques
- 1.5.3. Localización de direcciones IPs

1.6. Análisis forense de Bases de Datos
- 1.6.1. Análisis forense en MSSQL
- 1.6.2. Análisis forense en MySQL
- 1.6.3. Análisis forense en PostgreSQL
- 1.6.4. Análisis forense en MongoDB

1.7. Análisis forense en *Cloud*
- 1.7.1. Tipos de crímenes en *Cloud*
  - 1.7.1.1. Cloud como sujeto
  - 1.7.1.2. Cloud como objeto
  - 1.7.1.3. Cloud como herramienta
- 1.7.2. Retos del análisis forense en *Cloud*
- 1.7.3. Investigación de los servicios de almacenamiento en *Cloud*
- 1.7.4. Herramientas de análisis forense para *Cloud*

1.8. Investigación de crímenes de correo electrónico
- 1.8.1. Sistemas de correo
  - 1.8.1.1. Clientes de correo
  - 1.8.1.2. Servidor de correo
  - 1.8.1.3. Servidor SMTP
  - 1.8.1.4. Servidor POP3
  - 1.8.1.5. Servidor IMAP4
- 1.8.2. Crímenes de correo
- 1.8.3. Mensaje de correo
  - 1.8.3.1. Cabeceras estándar
  - 1.8.3.2. Cabeceras extendidas
- 1.8.4. Pasos para la investigación de estos crímenes
- 1.8.5. Herramientas forenses para correo electrónico

1.9. Análisis forense de móviles
- 1.9.1. Redes celulares
  - 1.9.1.1. Tipos de redes
  - 1.9.1.2. Contenidos del CDR
- 1.9.2. *Subscriber Identity Module* (SIM)
- 1.9.3. Adquisición lógica
- 1.9.4. Adquisición física
- 1.9.5. Adquisición del sistema de ficheros

1.10. Redacción y presentación de informes forenses
- 1.10.1. Aspectos importantes de un informe forense
- 1.10.2. Clasificación y tipos de informes
- 1.10.3. Guía para escribir un informe
- 1.10.4. Presentación del informe
  - 1.10.4.1. Preparación previa para testificar
  - 1.10.4.2. Deposición
  - 1.10.4.3. Trato con los medios

Un temario de alto interés y total actualidad que te llevará a la mayor capacitación en este campo, habilitándote para competir entre los mejores del sector”

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

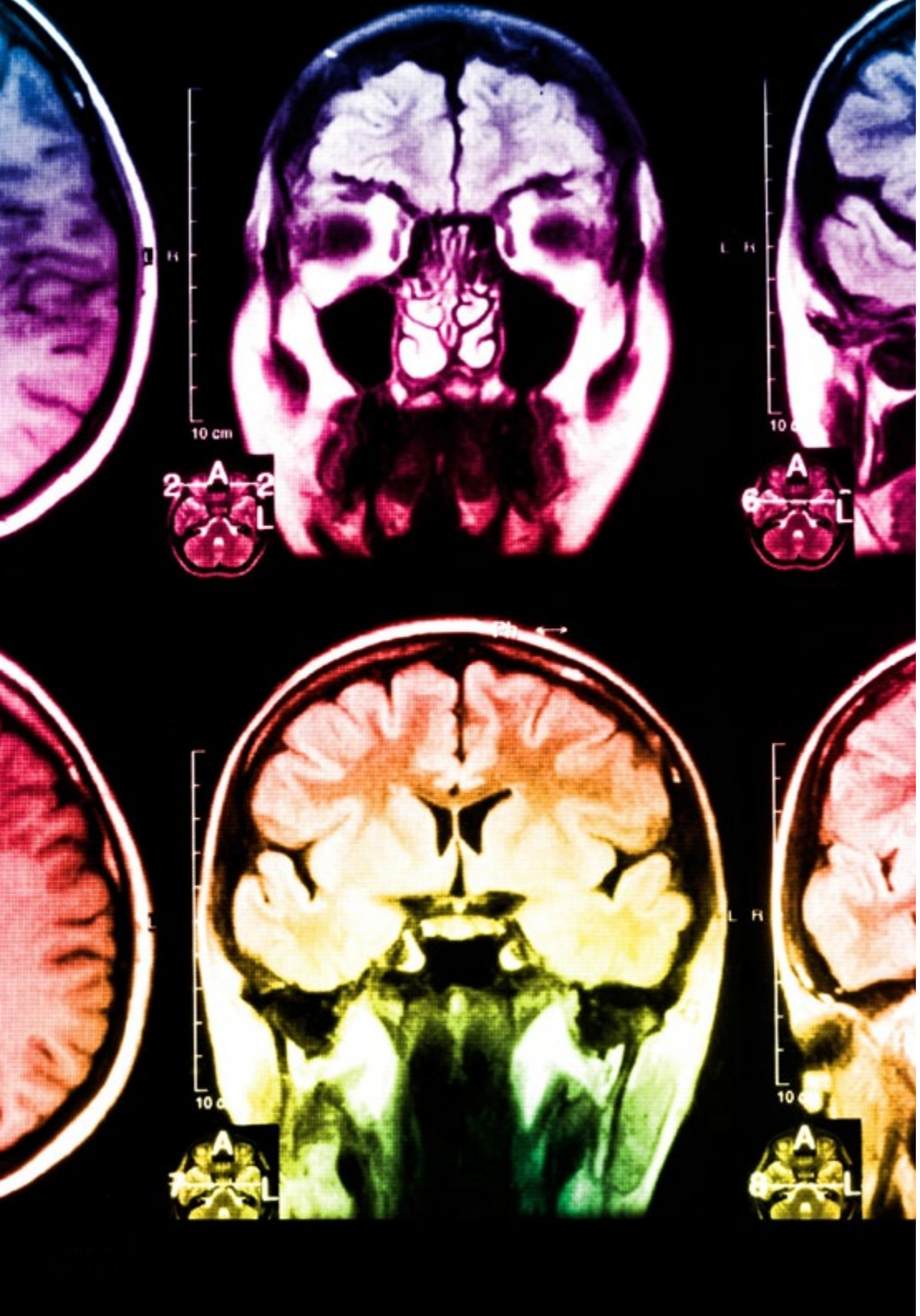
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

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.

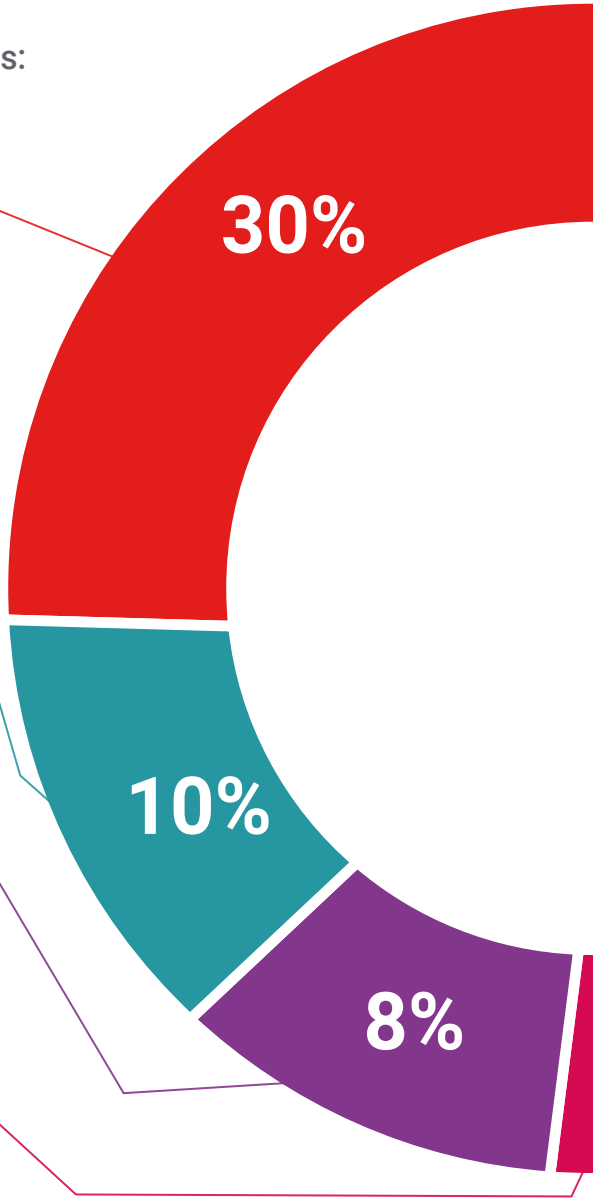
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

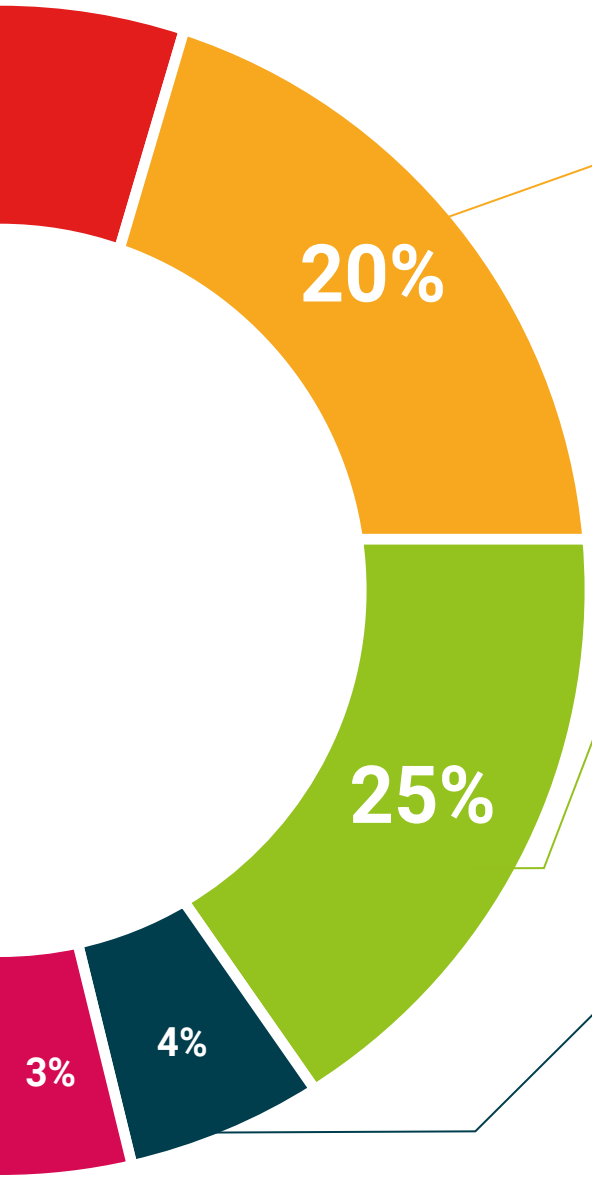
Prácticas de habilidades y competencias

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 Forense en Ciberseguridad 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 una titulación universitaria sin desplazamientos ni farragosos trámites”

Este **Diplomado en Análisis Forense en Ciberseguridad** 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 Forense en Ciberseguridad**

N.º Horas Oficiales: **150 h.**


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 Forense en Ciberseguridad

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

Este título propio se deberá acompañar siempre del título universitario habilitante expedido por la autoridad competente para ejercer profesionalmente en cada país. 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 Forense en Ciberseguridad

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

Diplomado

Análisis Forense en Ciberseguridad

tech universidad tecnológica