Experto Universitario
Medidas de Defensa de Seguridad Informáticas



tech universidad tecnológica



tech universidad tecnológica

Experto Universitario

Medidas de Defensa de Seguridad Informáticas

Modalidad: **Online**
Duración: **6 meses**
Titulación: **TECH Universidad Tecnológica**
Horas lectivas: **450 h.**
Acceso web: **www.techtitute.com/informatica/experto-universitario/experto-medidas-defensa-seguridad-informaticas**

Índice

01 Presentación — pág. 4

02 Objetivos — pág. 8

03 Dirección de curso — pág. 12

04 Estructura y contenido — pág. 16

05 Metodología — pág. 22

06 Titulación — pág. 30

01

Presentación

Los sectores financiero, empresarial y turístico han sufrido un incremento de ataques de ingeniería social que ponen en peligro información sensible y valiosa de las propias entidades y de sus clientes. Los ataques cibernéticos siguen siendo un quebradero de cabeza para las compañías, por lo que el índice de empleos generados para garantizar la seguridad informática ha ido en aumento en los últimos años. Para dar respuesta a esta necesidad, este programa aporta una especialización a los profesionales de la informática en el campo de la adopción de medidas de defensa informática ante cualquier ataque. Un equipo docente experto en el área imparte esta titulación en modalidad 100% online permitiendo adquirir un aprendizaje actual y exhaustivo gracias a su amplio contenido multimedia.





Da la mejor respuesta en seguridad informática y evita que las empresas caigan en la ingeniería social con este Experto Universitario”

Implementar políticas de seguridad informática supone un costo para las empresas, no obstante, están dispuestas a sufragarlo debido a las elevadas pérdidas que supone para ellas el hackeo de sus sistemas, comprometiendo su correcto funcionamiento y la prestación de servicio a sus clientes. Un papel clave en este escenario es el que desempeña los profesionales de la informática.

Este Experto Universitario proporciona al alumnado un aprendizaje profundo en medidas de defensa de seguridad informáticas, que parten de un análisis de las amenazas para posteriormente clasificarlas correctamente en pro de averiguar en qué puntos es más o menos vulnerable una empresa. Asimismo, el equipo docente especializado en esta materia facilitará las herramientas esenciales para realizar un análisis forense informático. De esta manera, se mostrará la detección de incidentes a través de los sistemas IDS/IPS y su tratamiento en SIEM hasta el proceso de notificación y escalado.

Para estar a la vanguardia en materia de defensa de seguridad, los profesionales de la informática desarrollarán, en esta titulación, técnicas para mitigar la denegación de servicio, el *Session Hacking* y los ataques a aplicativos web. Todo ello, en una modalidad de enseñanza 100% online, que permite al alumnado compaginar su labor profesional con un programa, que ofrece contenido multimedia y novedoso. Únicamente necesitan un dispositivo con conexión a internet para poder acceder a un plan de estudio que pueden cursar a su ritmo.

Este **Experto Universitario en Medidas de Defensa de Seguridad Informáticas** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en Seguridad Informática
- Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que está concebido recogen una información técnica 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 o portátil con conexión a internet

Implementa de manera efectiva políticas de seguridad ante Session Hijacking, Hacking Web Servers o Mobile Platforms gracias a este Experto Universitario”

Controla la norma ISO 27035 y cumple los requisitos para una correcta gestión de incidentes. Matricúlate en este Experto Universitario"

Crece en tu carrera profesional con un programa que te permitirá profundizar en el análisis y control de amenazas informáticas.

Estás a un clic de inscribirte en un Experto Universitario que te abrirá más salidas profesionales.

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 vídeo interactivo realizado por reconocidos expertos.

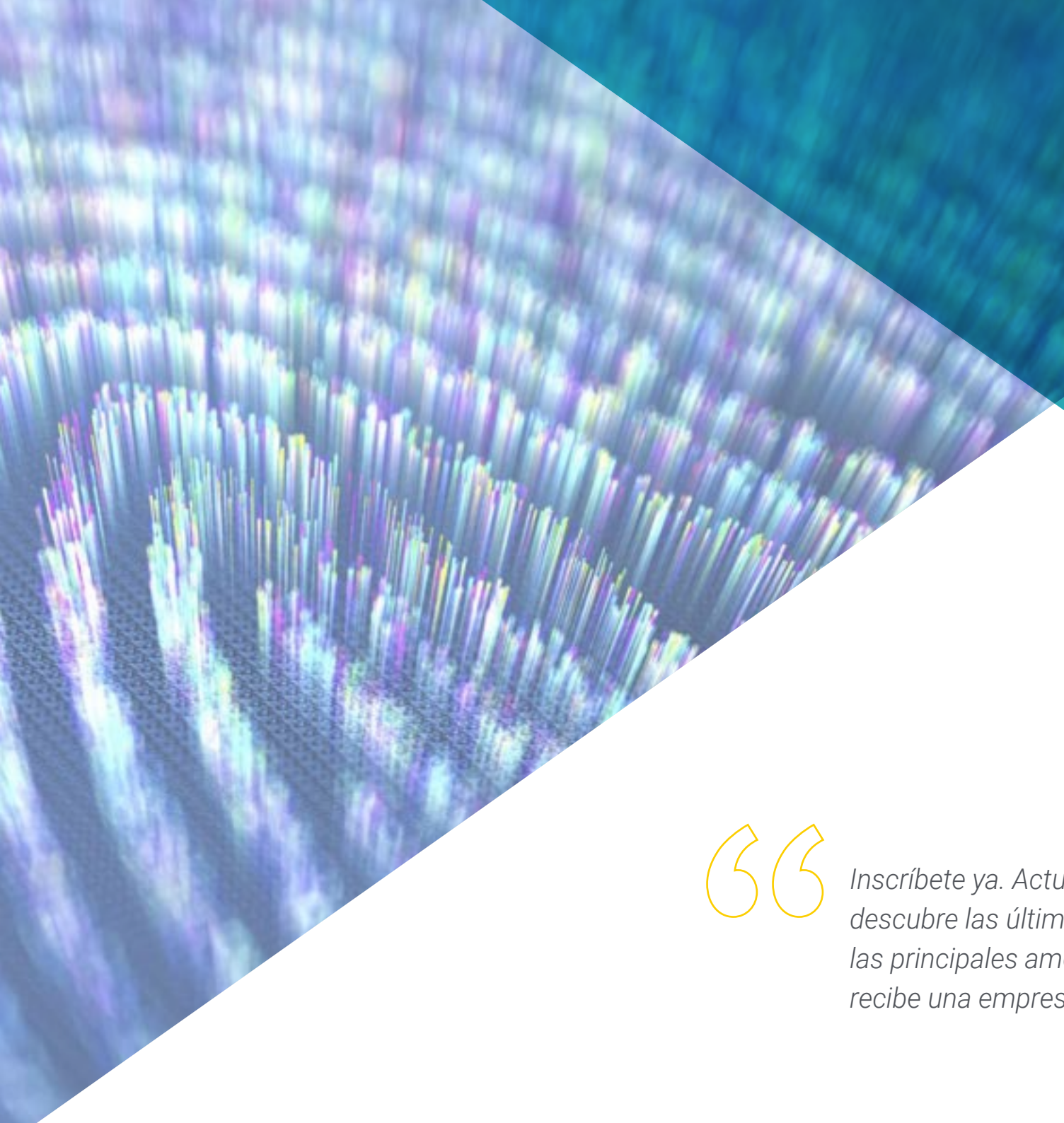


02

Objetivos

Este Experto Universitario propone una enseñanza cuya meta es lograr que los profesionales de la informática obtengan una titulación especializada en el campo de la seguridad. Así, a lo largo de este programa mejorarán sus competencias en el análisis de amenazas, comparando las distintas metodologías de gestión que les permitirá seleccionar aquella que mejor se ajuste al incidente. Así mismo, estarán capacitados para implementar técnicamente las medidas para mitigar las principales amenazas que reciba la empresa. De esta forma, los profesionales de la informática conseguirán una titulación que les permitirá progresar en el ámbito laboral.





Inscríbete ya. Actualiza tus conocimientos y descubre las últimas técnicas para impedir las principales amenazas informáticas que recibe una empresa”

Objetivos generales

- Profundizar en los conceptos clave de la seguridad de la información
- Desarrollar las medidas necesarias para garantizar buenas prácticas en materia de seguridad de la información
- Desarrollar las diferentes metodologías para la realización de un análisis exhaustivo de amenazas
- Instalar y conocer las distintas herramientas utilizadas en el tratamiento y prevención de incidencias

Accede a una titulación universitaria que te proporcionará las estrategias más novedosas y efectivas para gestionar cualquier ataque informático"





Objetivos específicos

Módulo 1. Políticas de seguridad para el análisis de amenazas en sistemas informáticos

- Analizar el significado de amenazas
- Determinar las fases de una gestión preventiva de amenazas
- Comparar las distintas metodologías de gestión de amenazas

Módulo 2. Políticas de gestión de incidencias de seguridad

- Desarrollar conocimiento especializado sobre cómo gestionar incidencias causadas por eventos de seguridad informática
- Determinar el funcionamiento de un equipo de tratamiento de incidencias en materia de seguridad
- Analizar las distintas fases de una gestión de eventos de seguridad informática
- Examinar los protocolos estandarizados para el tratamiento de incidencias de seguridad

Módulo 3. Implementación práctica de políticas de seguridad ante ataques

- Determinar los distintos ataques reales al sistema de información
- Evaluar las distintas políticas de seguridad para paliar los ataques
- Implementar técnicamente las medidas para mitigar las principales amenazas

03

Dirección del curso

TECH selecciona cuidadosamente a todo el personal docente que imparte las titulaciones. Este Experto Universitario cuenta con una profesional altamente cualificada en el campo de la seguridad informática. La experiencia como responsable de seguridad en esta área en entidades públicas y privadas, le garantizan alumnado un conocimiento cercano y que aporta gran valor al profesional que desee conocer de primera mano las principales medidas adoptadas en este campo ante las principales amenazas sufridas. De esta forma, los casos prácticos planteados se asemejan a situaciones reales ante la que debe hacer frente el alumnado en su ámbito laboral, y por ende le harán crecer profesionalmente.





Un cuadro docente especializado en materia de seguridad informática pondrá todo su saber a tu alcance para que avances en tu carrera profesional”

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

Dña. López García, Rosa María

- Especialista en Información de Gestión
- Profesora de Linux Professional Institute
- Colaboradora en Academia Hacker Incibe
- Capitana de Talento en Ciberseguridad en Teamciberhack
- Administrativa y gestora contable y financiera en Integra2Transportes
- Auxiliar administrativo en recursos de compras en el Centro de Educación Cardenal Marcelo Espínola
- Técnico Superior en Ciberseguridad y hacking Ético
- Miembro de Ciberpatrulla

D. Oropesiano Carrizosa, Francisco

- Ingeniero informático
- Técnico en Microinformática, Redes y Seguridad en Cas-Training
- Desarrollador de servicios web, CMS, e-Commerce, UI y UX en Fersa Reparaciones
- Gestor de servicios web, contenidos, correo y DNS en Oropesia Web & Network
- Diseñador gráfico y de aplicaciones web en Xarxa Sakai Projectes
- Diplomado en Informática de Sistemas por la Universidad de Alcalá de Henares
- Master en DevOps: Docker and Kubernetes por Cyber Business Center
- Técnico de Redes y Seguridad Informática por la Universidad de las Islas Baleares
- Experto en Diseño Gráfico por la Universidad Politécnica de Madrid

04

Estructura y contenido

El profesorado de este Experto Universitario ha elaborado un plan de estudio en el que profundiza en cada una de las fases de la elaboración de un plan de seguridad que afronta las amenazas en sistemas informáticos. De esta forma entra en detalle sobre la auditoría de la amenaza, su categorización, la gestión de la incidencia y las últimas herramientas para su detección. Así mismo, atiende a la problemática que suscita la ingeniería social en las empresas que se ven afectadas. Todo ello, con un material multimedia actualizado que facilita la comprensión del contenido, y con un sistema *Relearning*, que posibilita adquirir un conocimiento sólido.



Accede a una enseñanza 100% online, flexible, que te permite ir a tu ritmo. Compatibiliza tu vida personal con una enseñanza de calidad. Inscríbete"

Módulo 1. Políticas de seguridad para el análisis de amenazas en sistemas informáticos

1.1. La gestión de amenazas en las políticas de seguridad
- 1.1.1. La gestión del riesgo
- 1.1.2. El riesgo en seguridad
- 1.1.3. Metodologías en la gestión de amenazas
- 1.1.4. Puesta en marcha de metodologías

1.2. Fases de la gestión de amenazas
- 1.2.1. Identificación
- 1.2.2. Análisis
- 1.2.3. Localización
- 1.2.4. Medidas de salvaguarda

1.3. Sistemas de auditoría para localización de amenazas
- 1.3.1. Sistemas de auditoría para la localización de amenazas
- 1.3.2. Clasificación y flujo de información
- 1.3.3. Análisis de los procesos vulnerables

1.4. Clasificación del riesgo
- 1.4.1. Tipos de riesgo
- 1.4.2. Calculo de la probabilidad de amenaza
- 1.4.3. Riesgo residual

1.5. Tratamiento del riesgo
- 1.5.1. Tratamiento del riesgo
- 1.5.2. Implementación de medidas de salvaguarda
- 1.5.3. Transferir o asumir

1.6. Control de riesgo
- 1.6.1. Proceso continuo de gestión de riesgo
- 1.6.2. Implementación de métricas de seguridad
- 1.6.3. Modelo estratégico de métricas en seguridad de la información





1.7. Metodologías prácticas para el análisis y control de amenazas
- 1.7.1. Catálogo de amenazas
- 1.7.2. Catálogo de medidas de control
- 1.7.3. Catálogo de salvaguardas

1.8. Norma ISO 27005
- 1.8.1. Identificación del riesgo
- 1.8.2. Análisis del riesgo
- 1.8.3. Evaluación del riesgo

1.9. Matriz de riesgo, impacto y amenazas
- 1.9.1. Datos, sistemas y personal
- 1.9.2. Probabilidad de amenaza
- 1.9.3. Magnitud del daño

1.10. Diseño de fases y procesos en el análisis de amenazas
- 1.10.1. Identificación elementos críticos de la organización
- 1.10.2. Determinación de amenazas e impactos
- 1.10.3. Análisis del impacto y riesgo
- 1.10.4. Metodologías

Módulo 2. Políticas de gestión de incidencias de seguridad

2.1. Políticas de gestión de incidencias de seguridad de la información y mejoras
- 2.1.1. Gestión de incidencias
- 2.1.2. Responsabilidades y procedimientos
- 2.1.3. Notificación de eventos

2.2. Sistemas de detección y prevención de intrusiones (IDS/IPS)
- 2.2.1. Datos de funcionamiento del sistema
- 2.2.2. Tipos de sistemas de detección de intrusos
- 2.2.3. Criterios para la ubicación de los IDS/IPS

2.3. Respuesta ante incidentes de seguridad
- 2.3.1. Procedimiento de recolección de información
- 2.3.2. Proceso de verificación de intrusión
- 2.3.3. Organismos CERT

2.4. Proceso de notificación y gestión de intentos de intrusión
- 2.4.1. Responsabilidades en el proceso de notificación
- 2.4.2. Clasificación de los incidentes
- 2.4.3. Proceso de resolución y recuperación

2.5. Análisis forense como política de seguridad
- 2.5.1. Evidencias volátiles y no volátiles
- 2.5.2. Análisis y recogida de evidencias electrónicas
  - 2.5.2.1. Análisis de evidencias electrónicas
  - 2.5.2.2. Recogida de evidencias electrónicas

2.6. Herramientas de sistemas de detección y prevención de intrusiones (IDS/IPS)
- 2.6.1. Snort
- 2.6.2. Suricata
- 2.6.3. SolarWinds

2.7. Herramientas centralizadoras de eventos
- 2.7.1. SIM
- 2.7.2. SEM
- 2.7.3. SIEM

2.8. Guía de seguridad CCN-STIC 817
- 2.8.1. Guía de seguridad CCN-STIC 817
- 2.8.2. Gestión de ciberincidentes
- 2.8.3. Métricas e Indicadores

2.9. NIST SP800-61
- 2.9.1. Capacidad de respuesta antes incidentes de seguridad informática
- 2.9.2. Manejo de un incidente
- 2.9.3. Coordinación e información compartida

2.10. Norma ISO 27035
- 2.10.1. Norma ISO 27035. Principios de la gestión de incidentes
- 2.10.2. Guías para la elaboración de un plan para la gestión de incidentes
- 2.10.3. Guías de operaciones en la respuesta a incidentes

Módulo 3. Implementación práctica de políticas de seguridad ante ataques

3.1. *System Hacking*
- 3.1.1. *System Hacking*
- 3.1.2. Riesgos y vulnerabilidades
- 3.1.3. Contramedidas

3.2. DoS en servicios
- 3.2.1. DoS en Servicios
- 3.2.2. Riesgos y vulnerabilidades
- 3.2.3. Contramedidas

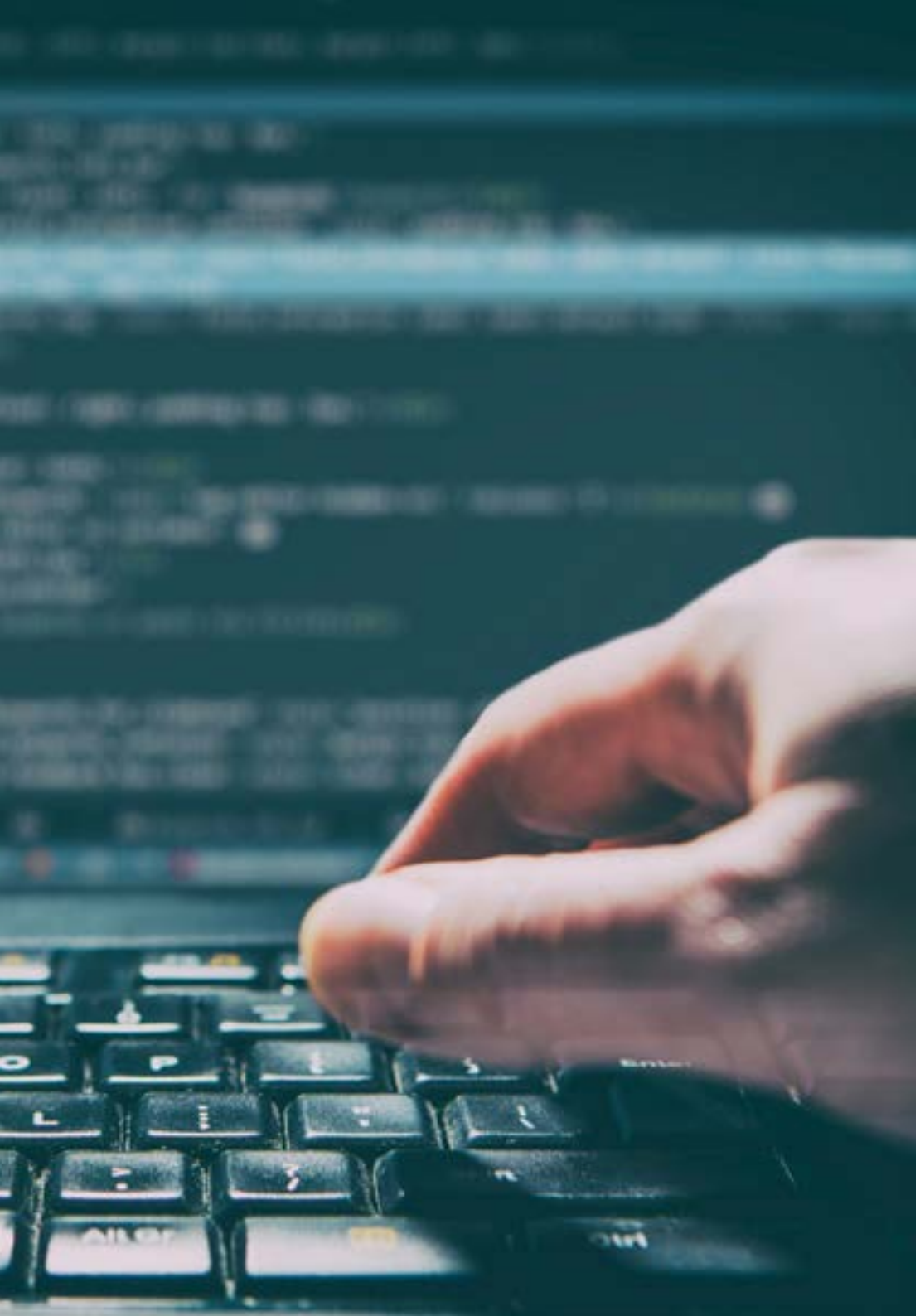
3.3. *Session Hijacking*
- 3.3.1. Session Hijacking
- 3.3.2. El proceso de Hijacking
- 3.3.3. Contramedidas a *Hijacking*

3.4. Evasión de IDS, *Firewalls and Honeypots*
- 3.4.1. Evasión de IDS, *Firewalls and Honeypots*
- 3.4.2. Técnicas de evasión
- 3.4.3. Implementación de contramedidas

3.5. *Hacking Web Servers*
- 3.5.1. *Hacking Web Servers*
- 3.5.2. Ataques a servidores web
- 3.5.3. Implementación de medidas de defensa

3.6. *Hacking Web Applications*
- 3.6.1. *Hacking* Web *Applications*
- 3.6.2. Ataques a aplicaciones web
- 3.6.3. Implementación de medidas de defensa

3.7. *Hacking Wireless Networks*
- 3.7.1. *Hacking Wireless Networks*
- 3.7.2. Vulnerabilidades redes wifi
- 3.7.3. Implementación de medidas de defensa



3.8. *Hacking Mobile Platforms*
- 3.8.1. Hacking Mobile *Platforms*
- 3.8.2. Vulnerabilidades de plataformas móviles
- 3.8.3. Implementación de contramedidas

3.9. *Ramsonware*
- 3.9.1. *Ramsonware*
- 3.9.2. Vulnerabilidades causantes del *Ramsonware*
- 3.9.3. Implementación de contramedidas

3.10. Ingeniera social
- 3.10.1. Ingeniería social
- 3.10.2. Tipos de ingeniería social
- 3.10.3. Contramedidas para la ingeniería social

Los casos prácticos y el contenido multimedia son las herramientas más potentes de este Experto Universitario. Descárgatelas desde el primer día y avanza en tu carrera profesional"

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.

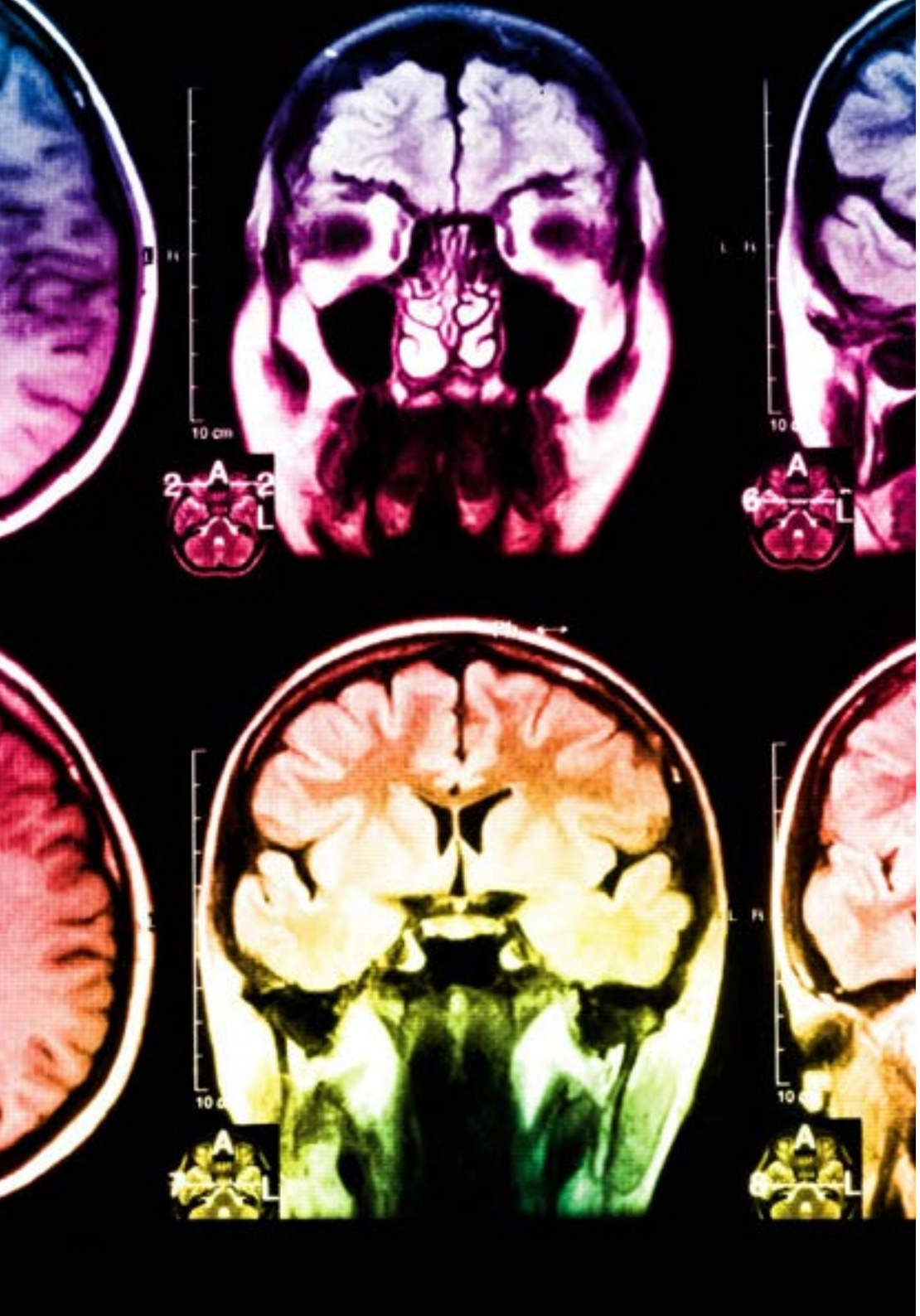
Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el *Relearning*.

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.

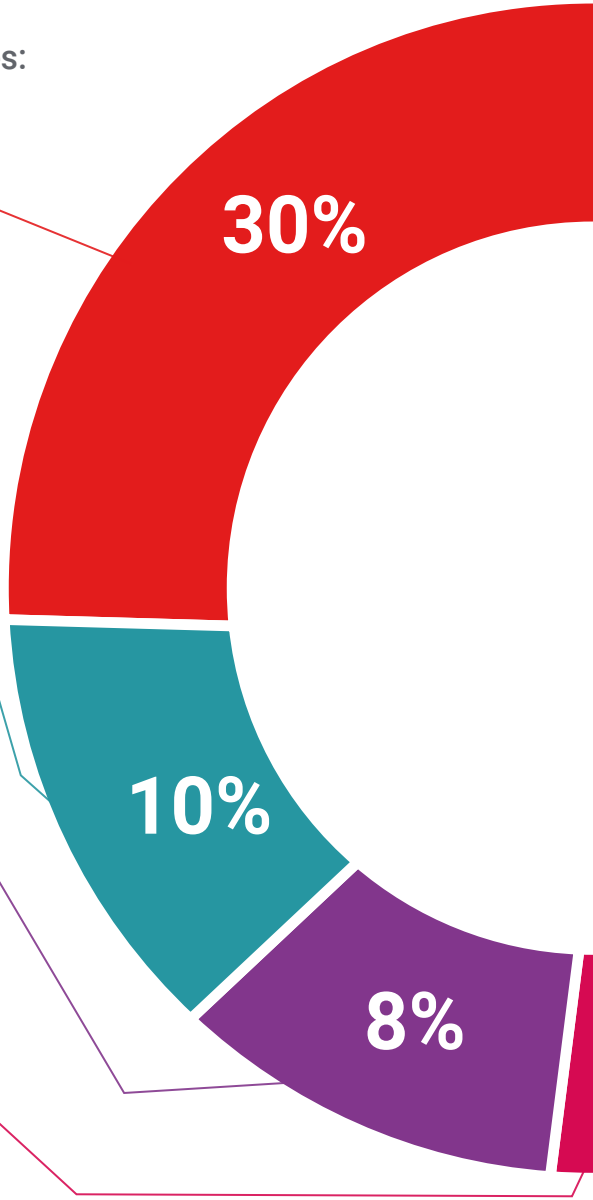
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

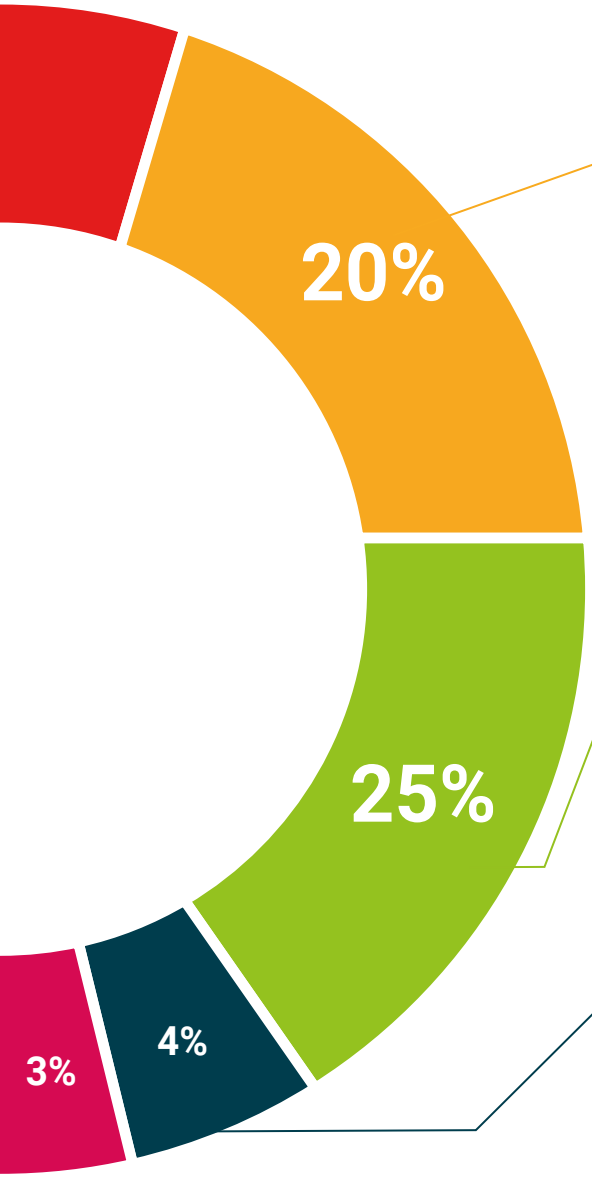
Prácticas de habilidades y competencias

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 Medidas de Defensa de Seguridad Informáticas garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Experto Universitario expedido por TECH Universidad Tecnológica.





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

Este **Experto Universitario en Medidas de Defensa de Seguridad Informáticas** contiene el programa más completo y actualizado del mercado.

Tras la superación de la evaluacion, el alumno recibirá por correo postal* con acuse de recibo su correspondiente título de **Experto Universitario** emitido por **TECH Universidad Tecnológica.**

El título expedido por **TECH Universidad Tecnológica** expresará la calificación que haya obtenido en el Experto Universitario, y reunirá los requisitos comúnmente exigidos por las bolsas de trabajo, oposiciones y comités evaluadores de carreras profesionales.

Título: **Experto Universitario en Medidas de Defensa de Seguridad Informáticas**

N.º Horas Oficiales: **450 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

EXPERTO UNIVERSITARIO

en

Medidas de Defensa de Seguridad Informáticas

Se trata de un título propio de esta Universidad con una duración de 450 horas, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH es una Institución Particular de Educación Superior reconocida por la Secretaría de Educación Pública a partir del 28 de junio de 2018.

A 17 de junio de 2020

Mtra.Tere Guevara Navarro
Rectora

código único TECH: AFWOR23S techtitute.com/titulos

*Apostilla de La Haya. En caso de que el alumno solicite que su título en papel recabe la Apostilla de La Haya, TECH EDUCATION realizará las gestiones oportunas para su obtención, con un coste adicional.

tech universidad tecnológica

Experto Universitario
Medidas de Defensa de Seguridad Informáticas

Modalidad: **Online**
Duración: **6 meses**
Titulación: **TECH Universidad Tecnológica**
Horas lectivas: **450 h.**

Experto Universitario

Medidas de Defensa de Seguridad Informáticas



tech universidad tecnológica