# Experto Universitario
## Seguridad Informática para las Comunicaciones

tech universidad

tech universidad

# Experto Universitario
## Seguridad Informática para las Comunicaciones

- Modalidad: **online**
- Duración: **3 meses**
- Titulación: **TECH Universidad**
- Acreditación: **18 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: www.techtitute.com/informatica/experto-universitario/experto-seguridad-informatica-comunicaciones

# Índice

01

# Presentación

El uso no autorizado e indebido de redes es internet es uno de los principales problemas a los que pueden enfrentarse los usuarios. Llevar a cabo acciones de seguridad informática es imprescindible, puesto que a través de internet se mueve gran cantidad de información privada y confidencial. Este Experto Universitario acerca a los alumnos al ámbito de la seguridad informática para las comunicaciones, con un programa actualizado y de calidad. Se trata de una completa preparación que busca capacitar a los alumnos para el éxito en su profesión.


*Si buscas una capacitación de calidad que te ayude a especializarte en uno de los campos con más salidas profesionales, esta es tu mejor opción"*

Los avances en las telecomunicaciones suceden constantemente, ya que esta es una de las áreas de más rápida evolución Por ello, es necesario contar con expertos en Informática que se adapten a estos cambios y conozcan de primera mano las nuevas herramientas y técnicas que surgen en este ámbito.

Dentro de este ámbito, la seguridad informática tiene que ser uno de los aspectos que más cuiden las empresas, ya que toda su información se encuentra en red, por lo que el acceso incontrolado de un usuario para llevar a cabo tareas ilícitas puede suponer un grave problema para la organización, ya sea a nivel económico o de reputación.

El Experto Universitario en Seguridad Informática para las Comunicaciones aborda la completa totalidad de temáticas que intervienen en este campo. Su estudio presenta una clara ventaja frente a otras capacitaciones que se centran en bloques concretos, lo que impide al alumno conocer la interrelación con otras áreas incluidas en el ámbito multidisciplinar de las telecomunicaciones. Además, el equipo docente de este programa educativo ha realizado una cuidadosa selección de cada uno de los temas de esta capacitación para ofrecer al alumno una oportunidad de estudio lo más completa posible y ligada siempre con la actualidad.

Este programa está dirigido a aquellas personas interesadas en alcanzar un nivel de conocimiento superior sobre Seguridad Informática para las Comunicaciones. El principal objetivo es capacitar al alumno para que aplique en el mundo real los conocimientos adquiridos en este Experto Universitario, en un entorno de trabajo que reproduzca las condiciones que se puede encontrar en su futuro, de manera rigurosa y realista.

Además, al tratarse de un Experto Universitario 100% online, el alumno no está condicionado por horarios fijos ni necesidad de trasladarse a otro lugar físico, sino que puede acceder a los contenidos en cualquier momento del día, equilibrando su vida laboral o personal con la académica.

Este **Experto Universitario en Seguridad Informática para las Comunicaciones** contiene el programa universitario 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 están concebidos 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 en seguridad informática para las comunicaciones
- 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

*No dejes pasar la oportunidad de realizar con nosotros este Experto Universitario en Seguridad Informática para las Comunicaciones. Es la oportunidad perfecta para avanzar en tu carrera”*

*Este Experto Universitario es la mejor inversión que puedes hacer en la selección de un programa de actualización para poner al día tus conocimientos en seguridad informática para las comunicaciones"*

*Esta capacitación cuenta con el mejor material didáctico, lo que te permitirá un estudio contextual que te facilitará el aprendizaje.*

*Este Experto Universitario 100% online te permitirá compaginar tus estudios con tu labor profesional. Tú eliges dónde y cuándo capacitarte.*

Incluye en su cuadro docente a profesionales pertenecientes al ámbito de la Informática de las telecomunicaciones, 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, el profesional contará con la ayuda de un novedoso sistema de vídeo interactivo realizado por reconocidos expertos en seguridad informática para las comunicaciones y con gran experiencia.

02

# Objetivos

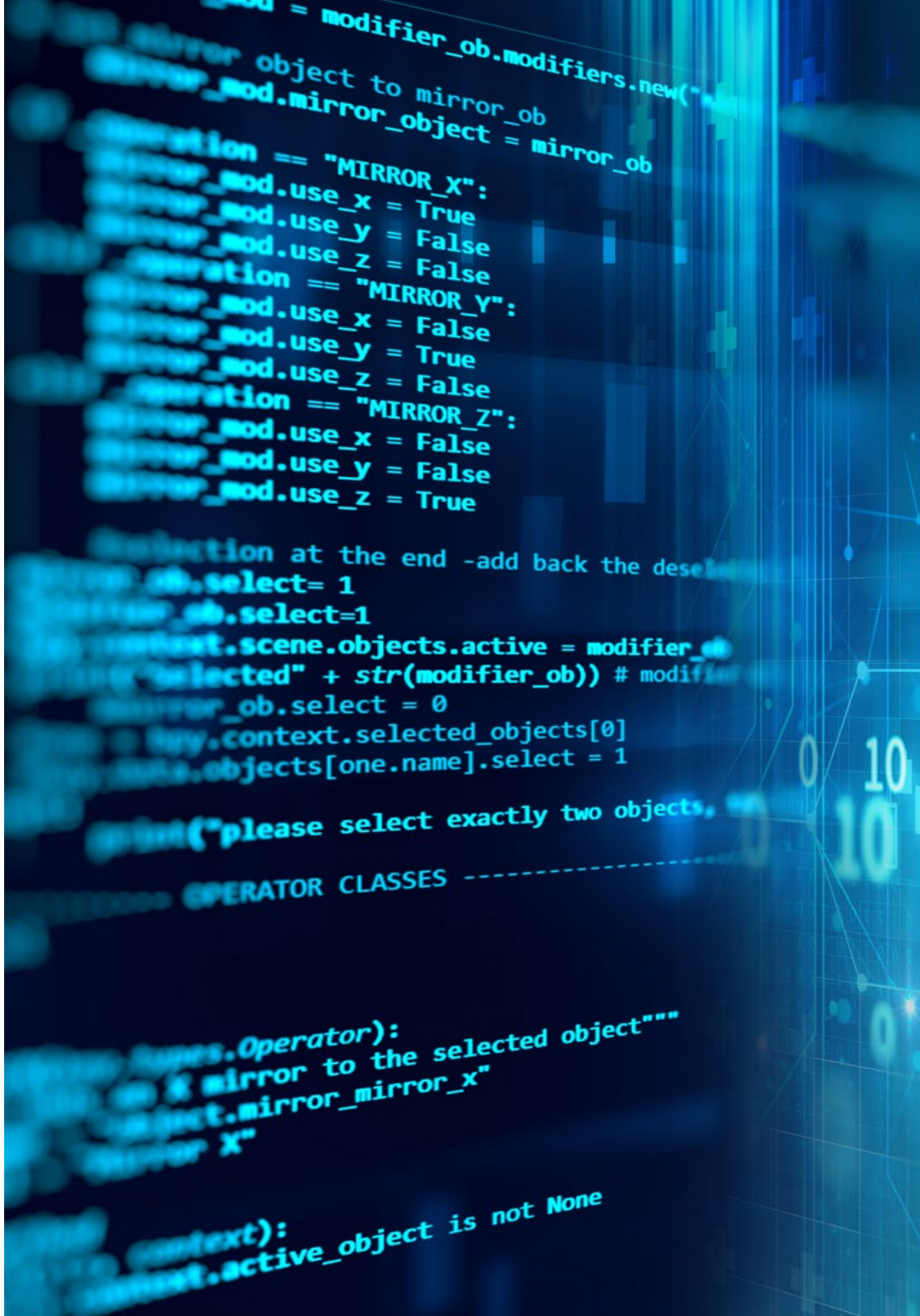
El Experto Universitario en Seguridad Informática para las Comunicaciones está orientado a facilitar la actuación del profesional de este campo para que adquiera y conozca las principales novedades en este ámbito.


*Nuestro objetivo es te conviertas en el mejor profesional en tu sector. Para, ello contamos con la mejor metodología y contenido"*

## Objetivo general

- Capacita al alumno para que sea capaz de desarrollar su labor con total seguridad y calidad en el ámbito de la seguridad informática para las comunicaciones

*Fórmate en la principal universidad online privada de habla hispana del mundo”*



## Objetivos especificos

### Módulo 1: Seguridad en sistemas y redes de comunicación

- Conocer y saber aplicar los fundamentos de programación en redes, sistemas y servicios de telecomunicación
- Dominar la normativa y regulación de protocolos y redes de los organismos internacionales de normalización
- Comprender los conceptos de criptografía simétrica y asimétrica, firma digital, funciones hash y securización de cada nivel de una arquitectura de comunicaciones
- Comprender los distintos mecanismos y protocoles de seguridad basados en control de acceso: autenticación y defensa perimetral
- Conocer el funcionamiento de las amenazas técnicas y humanas a la seguridad de las redes y sistemas de telecomunicación
- Categorizar adecuadamente los distintos servicios de seguridad para redes y sistemas, en función de los activos que protegen
- Aplicar a las redes y servicios de telecomunicación los sistemas de gestión de red y de servicios para la configuración, operación, supervisión y tarificación de los mismos
- Saber gestionar la seguridad de las redes y servicios de telecomunicación mediante la aplicación de tunelado, cortafuegos, protocolos de cifrado y autenticación, y mecanismos de protección de contenidos
- Ser capaz de entender y aplicar las principales técnicas de programación segura

### Módulo 2: Arquitecturas de seguridad

- Comprender los principios básicos de la seguridad informática
- Dominar los estándares de seguridad informática y procesos de certificación
- Analizar los fundamentos organizativos y criptográficos en los que se basan las tecnologías de seguridad
- Identificar las principales amenazas y vulnerabilidades de los distintos elementos involucrados en las TIC, así como sus causas
- Conocer en profundidad las herramientas para la seguridad en redes y sus funciones específicas
- Saber aplicar las tecnologías que conforman una arquitectura de seguridad de las TIC, en sus distintas perspectivas

### Módulo 3: Auditoría de sistemas de información

- Dominar los principales conceptos, normas y metodologías de la auditoría de sistemas
- Estar al tanto de los elementos organizativos y el marco legal de las auditorías
- Obtener una guía de referencia para el diseño nuevos sistemas de controles internos informáticos
- Comprender y determinar los riesgos que trae consigo el desarrollo tecnológico
- Detectar cómo los diferentes sistemas de información cumplen o no con los requisitos de seguridad deseados
- Ser capaces de llevar a cabo un proceso de mejora continua de la ciberseguridad

03

# Estructura y contenido

La estructura de los contenidos ha sido diseñada por los mejores profesionales del sector de la ingeniería de telecomunicaciones, con una amplia trayectoria y reconocido prestigio en la profesión.

*Contamos con el programa científico más completo y actualizado del mercado. Buscamos la excelencia y que tú también la logres"*

## **Módulos 1.** Seguridad en Sistemas y Redes de Comunicación

1.1. Una perspectiva global de la seguridad, la criptografía y los criptoanálisis clásicos
- 1.1.1. La seguridad informática: perspectiva histórica
- 1.1.2. Pero, ¿qué se entiende exactamente por seguridad?
- 1.1.3. Historia de la criptografía
- 1.1.4. Cifradores de sustitución
- 1.1.5. Caso de estudio: la máquina Enigma

1.2. Criptografía simétrica
- 1.2.1. Introducción y terminología básica
- 1.2.2. Cifrado simétrico
- 1.2.3. Modos de operación
- 1.2.4. DES
- 1.2.5. El nuevo estándar AES
- 1.2.6. Cifrado en flujo
- 1.2.7. Criptoanálisis

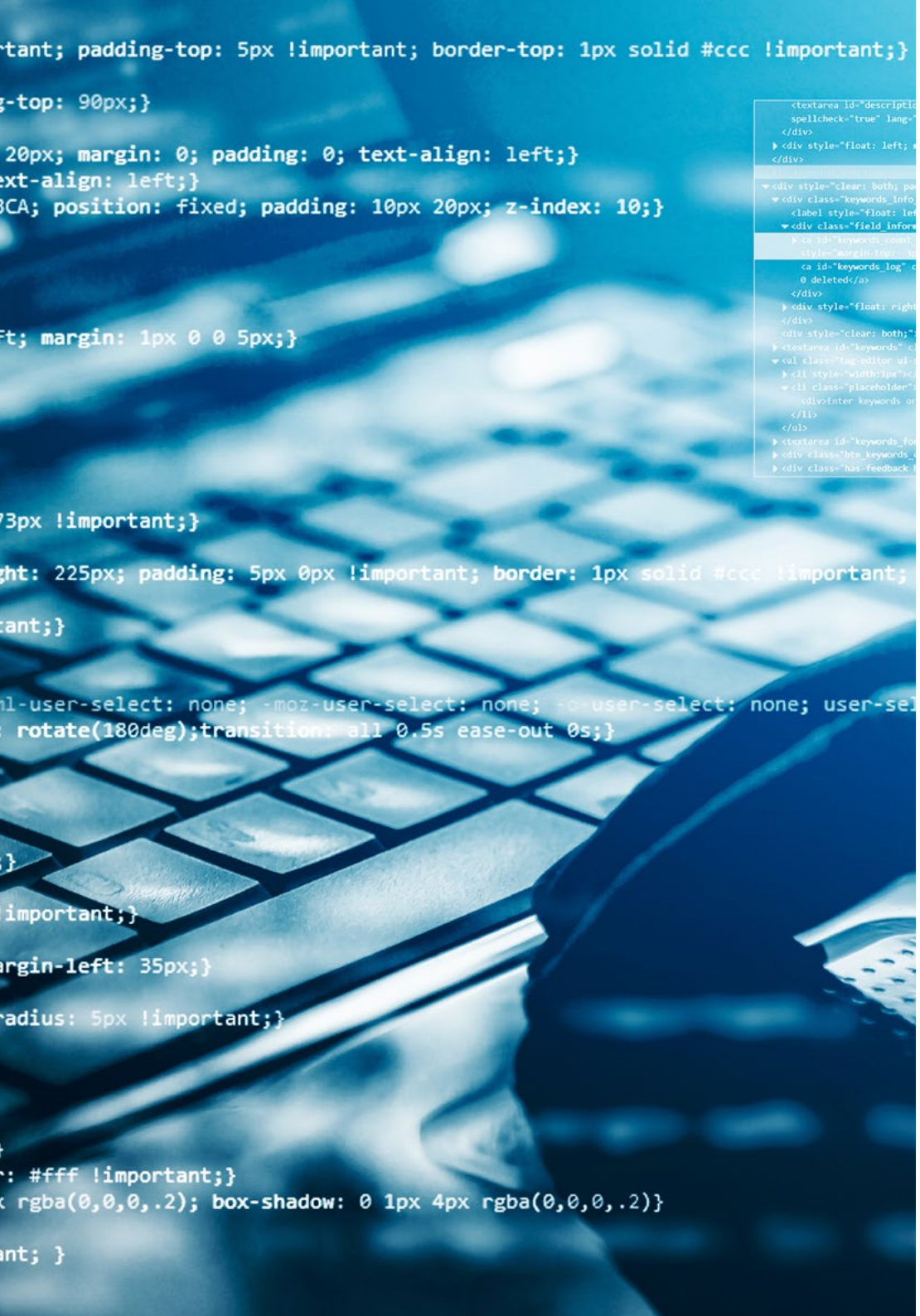
1.3. Criptografía asimétrica
- 1.3.1. Orígenes de la criptografía de clave pública
- 1.3.2. Conceptos básicos y funcionamiento
- 1.3.3. El algoritmo RSA
- 1.3.4. Certificados digitales
- 1.3.5. Almacenamiento y gestión de claves

1.4. Ataques en redes
- 1.4.1. Amenazas y ataques de una red
- 1.4.2. Enumeración
- 1.4.3. Interceptación de tráfico: *sniffers*
- 1.4.4. Ataques de denegación de servicio
- 1.4.5. Ataques de envenenamiento ARP

1.5. Arquitecturas de seguridad
- 1.5.1. Arquitecturas de seguridad tradicionales
- 1.5.2. *Secure Socket Layer*: SSL
- 1.5.3. Protocolo SSH
- 1.5.4. Redes Privadas Virtuales (VPNs)
- 1.5.5. Mecanismos de protección de unidades de almacenamiento externo
- 1.5.6. Mecanismos de protección hardware

1.6. Técnicas de protección de sistemas y desarrollo de código seguro
- 1.6.1. Seguridad en operaciones
- 1.6.2. Recursos y controles
- 1.6.3. Monitorización
- 1.6.4. Sistemas de detección de intrusión
- 1.6.5. IDS de host
- 1.6.6. IDS de red
- 1.6.7. IDS basados en firmas
- 1.6.8. Sistemas señuelos
- 1.6.9. Principios de seguridad básicos en el desarrollo de código
- 1.6.10. Gestión del fallo
- 1.6.11. Enemigo público número 1: el desbordamiento de búfer
- 1.6.12. Chapuzas criptográficas

1.7. Botnets y spam
- 1.7.1. Origen del problema
- 1.7.2. Proceso del spam
- 1.7.3. Envío del spam
- 1.7.4. Refinamiento de las listas de direcciones de correo
- 1.7.5. Técnicas de protección
- 1.7.6. Servicio antispam ofrecidos por terceros
- 1.7.7. Casos de estudio
- 1.7.8. Spam exótico



1.8. Auditoría y ataques Web
- 1.8.1. Recopilación de información
- 1.8.2. Técnicas de ataque
- 1.8.3. Herramientas

1.9. Malware y código malicioso
- 1.9.1. ¿Qué es el *Malware*?
- 1.9.2. Tipos de *Malware*
- 1.9.3. Virus
- 1.9.4. Criptovirus
- 1.9.5. Gusanos
- 1.9.6. *Adware*
- 1.9.7. *Spyware*
- 1.9.8. *Hoaxes*
- 1.9.9. *Pishing*
- 1.9.10. Troyanos
- 1.9.11. La economía del *Malware*
- 1.9.12. Posibles soluciones

1.10. Análisis forense
- 1.10.1. Recolección de evidencias
- 1.10.2. Análisis de las evidencias
- 1.10.3. Técnicas antiforenses
- 1.10.4. Caso de estudio práctico

## **Módulo 2.** Arquitecturas de Seguridad

2.1. Principios básicos de seguridad informática
- 2.1.1. Qué se entiende por seguridad informática
- 2.1.2. Objetivos de la seguridad informática
- 2.1.3. Servicios de seguridad informática
- 2.1.4. Consecuencias de la falta de seguridad
- 2.1.5. Principio de "defensa en seguridad"
- 2.1.6. Políticas, planes y procedimientos de seguridad
  - 2.1.6.1. Gestión de cuentas de usuarios
  - 2.1.6.2. Identificación y autenticación de usuarios
  - 2.1.6.3. Autorización y control de acceso lógico
  - 2.1.6.4. Monitorización de servidores
  - 2.1.6.5. Protección de datos
  - 2.1.6.6. Seguridad en conexiones remotas
- 2.1.7. La importancia del factor humano

2.2. Estandarización y certificación en seguridad informática
- 2.2.1. Estándares de seguridad
  - 2.2.1.1. Propósito de los estándares
  - 2.2.1.2. Organismos responsables
- 2.2.2. Estándares en EEUU
  - 2.2.2.1. TCSEC
  - 2.2.2.2. Federal Criteria
  - 2.2.2.3. FISCAM
  - 2.2.2.4. NIST SP 800
- 2.2.3. Estándares europeos
  - 2.2.3.1. ITSEC
  - 2.2.3.2. ITSEM
  - 2.2.3.3. Agencia Europea de Seguridad de la Información y las Redes
- 2.2.4. Estándares internacionales
- 2.2.5. Proceso de certificación

2.3. Amenazas a la seguridad informática: vulnerabilidades y *Malware*
- 2.3.1. Introducción
- 2.3.2. Vulnerabilidades de los sistemas
  - 2.3.2.1. Incidentes de seguridad en las redes
  - 2.3.2.2. Causas de las vulnerabilidades de los sistemas informáticos
  - 2.3.2.3. Tipos de vulnerabilidades
  - 2.3.2.4. Responsabilidades de los fabricantes de software
  - 2.3.2.5. Herramientas para la evaluación de vulnerabilidades
- 2.3.3. Amenazas de la seguridad informática
  - 2.3.3.1. Clasificación de los intrusos en redes
  - 2.3.3.2. Motivaciones de los atacantes
  - 2.3.3.3. Fases de un ataque
  - 2.3.3.4. Tipos de ataques
- 2.3.4. Virus informáticos
  - 2.3.4.1. Características generales
  - 2.3.4.2. Tipos de virus
  - 2.3.4.3. Daños ocasionados por virus
  - 2.3.4.4. Cómo combatir los virus

2.4. Ciberterrorismo y Respuesta a Incidentes
- 2.4.1. Introducción
- 2.4.2. La amenaza del ciberterrorismo y de las guerras informáticas
- 2.4.3. Consecuencias de los fallos y ataques en las empresas
- 2.4.4. El espionaje en las redes de ordenadores

2.5. Identificación de usuarios y sistemas biométricos
- 2.5.1. Introducción a la autenticación, autorización y registro de usuarios
- 2.5.2. Modelo de seguridad AAA
- 2.5.3. Control de acceso
- 2.5.4. Identificación de usuarios
- 2.5.5. Verificación de contraseñas

2.5.6. Autenticación con certificados digitales
2.5.7. Identificación remota de usuarios
2.5.8. Inicio de sesión único
2.5.9. Gestores de contraseñas
2.5.10. Sistemas biométricos
2.5.10.1. Características generales
2.5.10.2. Tipos de sistemas biométricos
2.5.10.3. Implantación de los sistemas
2.6. Fundamentos de criptografía y protocolos criptográficos
2.6.1. Introducción a la criptografía
2.6.1.1. Criptografía, criptoanálisis y criptología
2.6.1.2. Funcionamiento de un sistema criptográfico
2.6.1.3. Historia de los sistemas criptográficos
2.6.2. Criptoanálisis
2.6.3. Clasificación de los sistemas criptográficos
2.6.4. Sistemas criptográficos simétricos y asimétricos
2.6.5. Autenticación con sistemas criptográficos
2.6.6. Firma electrónica
2.6.6.1. Qué es la firma electrónica
2.6.6.2. Características de la firma electrónica
2.6.6.3. Autoridades de certificación
2.6.6.4. Certificados digitales
2.6.6.5. Sistemas basados en el tercero de confianza
2.6.6.6. Utilización de la firma electrónica
2.6.6.7. DNI electrónico
2.6.6.8. Factura electrónica
2.7. Herramientas para la seguridad en redes
2.7.1. El problema de la seguridad en la conexión a internet
2.7.2. La seguridad en la red externa
2.7.3. El papel de los servidores Proxy
2.7.4. El papel de los cortafuegos
2.7.5. Servidores de autenticación para conexiones remotas
2.7.6. El análisis de los registros de actividad
2.7.7. Sistemas de detección de intrusiones
2.7.8. Los señuelos
2.8. Seguridad en redes privadas virtuales e inalámbricas
2.8.1. Seguridad en redes privadas virtuales
2.8.1.1 El papel de las VPN
2.8.1.2 Protocolos para VPNs
2.8.2. Seguridad tradicional en redes inalámbricas
2.8.3. Posibles ataques en redes inalámbricas
2.8.4. El protocolo WEP
2.8.5. Estándares para seguridad en redes inalámbricas
2.8.6. Recomendaciones para reforzar la seguridad
2.9. Seguridad en el uso de servicios de internet
2.9.1. Navegación segura en la web
2.9.1.1. El servicio www
2.9.1.2. Problemas de seguridad en www
2.9.1.3. Recomendaciones de seguridad
2.9.1.4. Protección de la privacidad en internet
2.9.2. Seguridad en correo electrónico
2.9.2.1. Características del correo electrónico
2.9.2.2. Problemas de seguridad en el correo electrónico
2.9.2.3. Recomendaciones de seguridad en el correo electrónico
2.9.2.4. Servicios de correo electrónico avanzados
2.9.2.5. Uso de correo electrónico por empleados
2.9.3. El SPAM
2.9.4. El *phising*
2.10. Control de contenidos
2.10.1. La distribución de contenidos a través de internet
2.10.2. Medidas legales para combatir los contenidos ilícitos
2.10.3. Filtrado, catalogación y bloqueo de contenidos
2.10.4. Daños a la imagen y reputación

## **Módulo 3.** Auditoría de Sistemas de Información

3.1. Auditoría de sistemas de información. Normas de buenas prácticas
- 3.1.1. Introducción
- 3.1.2. Auditoría y COBIT
- 3.1.3. Auditoría de los sistemas de gestión en las TIC
- 3.1.4. Certificaciones

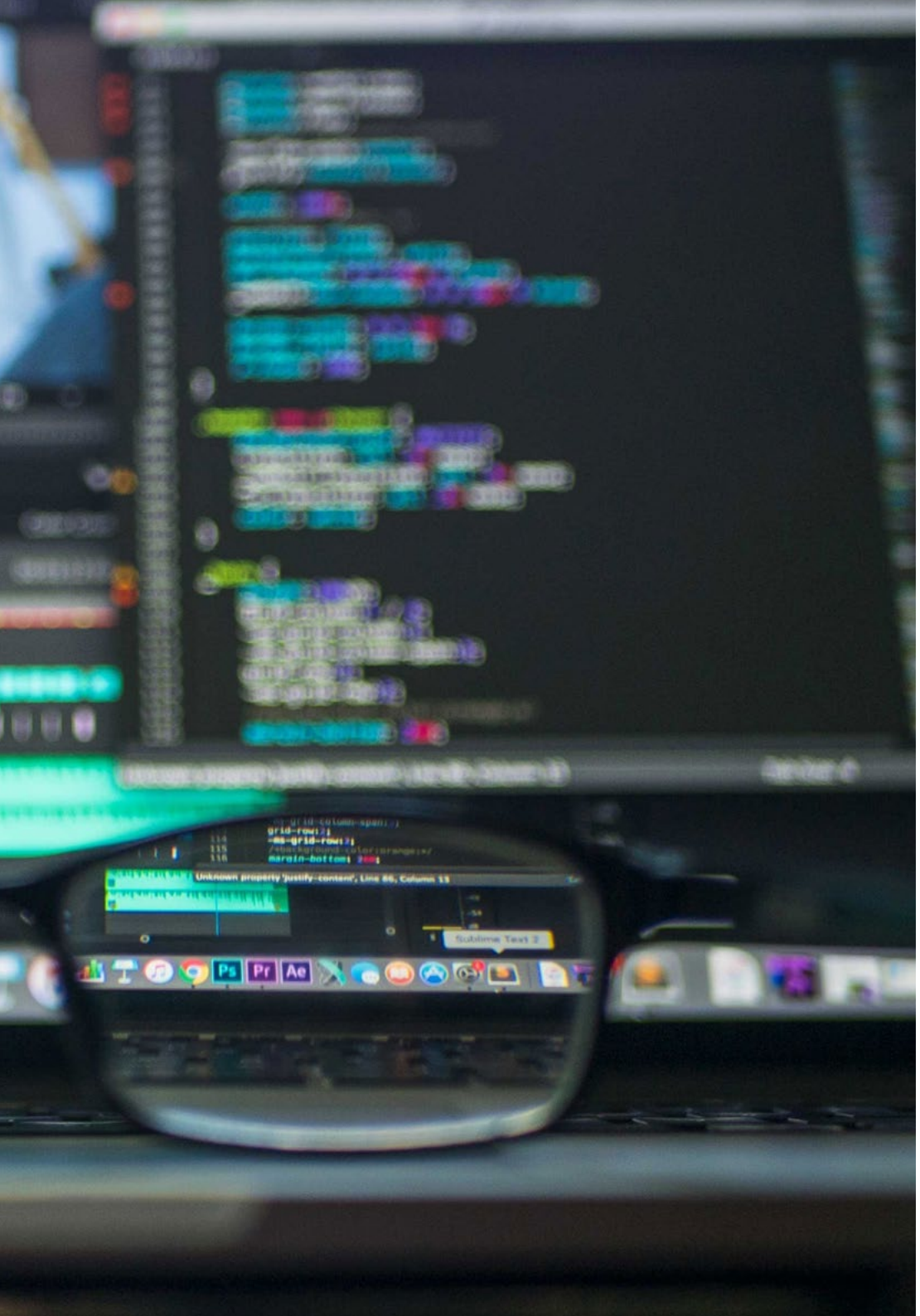
3.2. Conceptos y metodologías de la auditoría de sistemas
- 3.2.1. Introducción
- 3.2.2. Metodologías de evaluación de sistemas: cuantitativas y cualitativas
- 3.2.3. Metodologías de auditoría informática
- 3.2.4. El plan auditor

3.3. Contrato de auditoría
- 3.3.1. Naturaleza jurídica del contrato
- 3.3.2. Partes de un contrato de auditoría
- 3.3.3. Objeto del contrato de auditoría
- 3.3.4. El informe de auditoría

3.4. Elementos organizativos de las auditorías
- 3.4.1. Introducción
- 3.4.2. Misión del departamento de auditoría
- 3.4.3. Planificación de las auditorías
- 3.4.4. Metodología de la auditoría de SI

3.5. Marco legal de las auditorías
- 3.5.1. Protección de datos de caracter personal
- 3.5.2. Protección jurídica del software
- 3.5.3. Delitos tecnológicos
- 3.5.4. Contratación, firma y DNI electrónico

3.6. Auditoría del *Outsourcing* y marcos de referencia
- 3.6.1. Introducción
- 3.6.2. Conceptos básicos del *Outsourcing*
- 3.6.3. Auditoría del *Outsourcing* de TI
- 3.6.4. Marcos de referencia: CMMI, ISO27001, ITIL





3.7. Auditoría de seguridad
- 3.7.1. Introducción
- 3.7.2. Seguridad física y lógica
- 3.7.3. Seguridad del entorno
- 3.7.4. Planificación y ejecución de la auditoría de la seguridad física

3.8. Auditoría de redes e internet
- 3.8.1. Introducción
- 3.8.2. Vulnerabilidades en redes
- 3.8.3. Principios y derechos en internet
- 3.8.4. Controles y tratamientos de los datos

3.9. Auditoría de aplicaciones y sistemas informáticos
- 3.9.1. Introducción
- 3.9.2. Modelos de referencia
- 3.9.3. Evaluación de la calidad de las aplicaciones
- 3.9.4. Auditoría de la organización y gestión del área de desarrollo y mantenimiento

3.10. Auditoría de los datos de carácter personal
- 3.10.1. Introducción
- 3.10.2. Leyes y reglamentos de protección de datos
- 3.10.3. Desarrollo de la auditoría
- 3.10.4. Infracciones y sanciones

*Esta capacitación te permitirá avanzar en tu carrera de una manera cómoda”*

04

# Metodología de estudio

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

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

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

## El alumno: la prioridad de todos los programas de TECH

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

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

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

## Los planes de estudios más exhaustivos a nivel internacional

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

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

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

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

## *Case studies* o Método del caso

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

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

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

## Método *Relearning*

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

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

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

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

## Un Campus Virtual 100% online con los mejores recursos didácticos

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

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

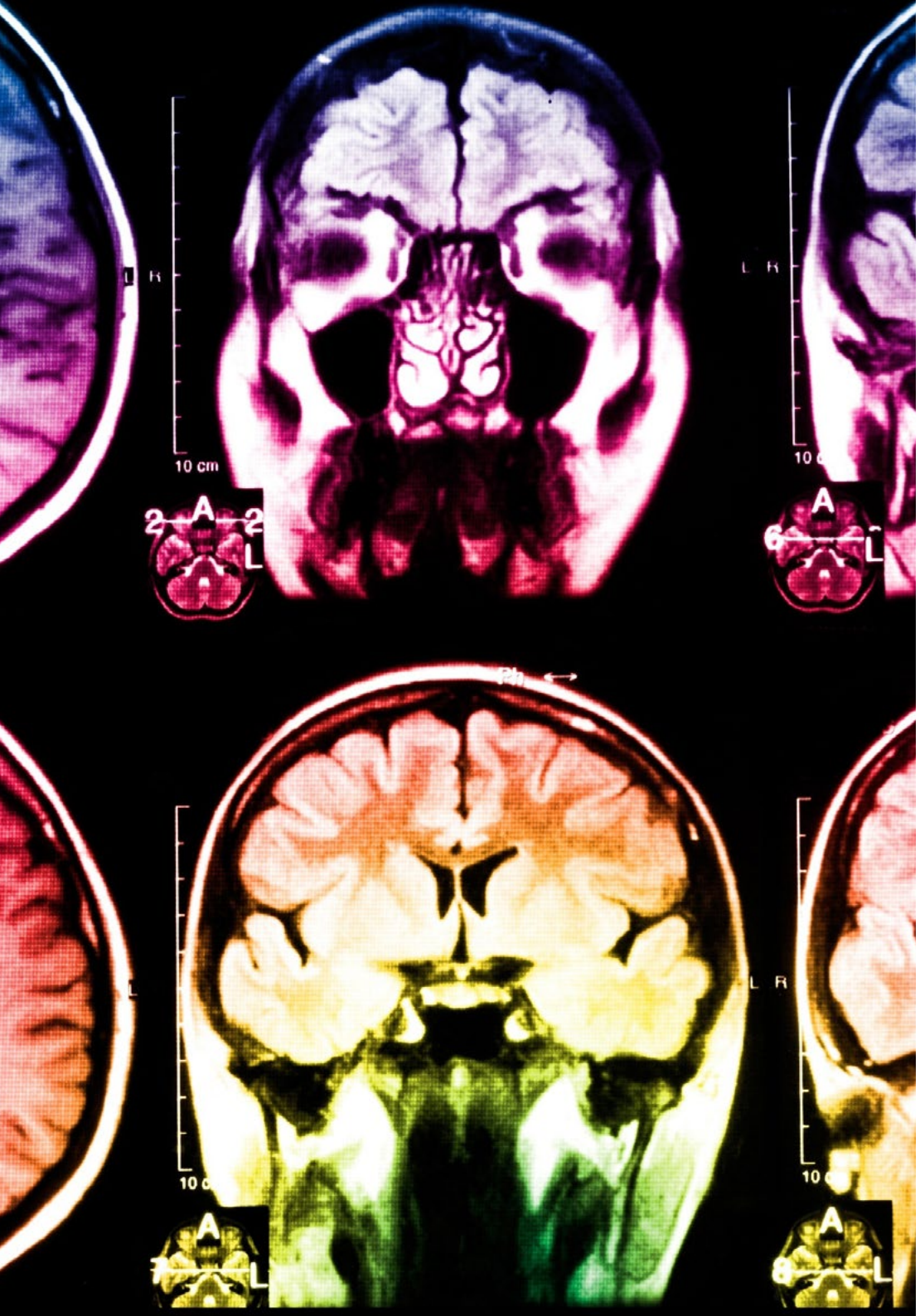
Por otro lado, también en aras de favorecer al máximo el contacto mentor-alumno, se proporciona un amplio abanico de posibilidades de comunicación, tanto en tiempo real como en diferido (mensajería interna, foros de discusión, servicio de atención telefónica, email de contacto con secretaría técnica,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

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

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

**La eficacia del método se justifica con cuatro logros fundamentales:**

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



## La metodología universitaria mejor valorada por sus alumnos

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

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

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

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

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

### Material de estudio

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

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

### Prácticas de habilidades y competencias

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

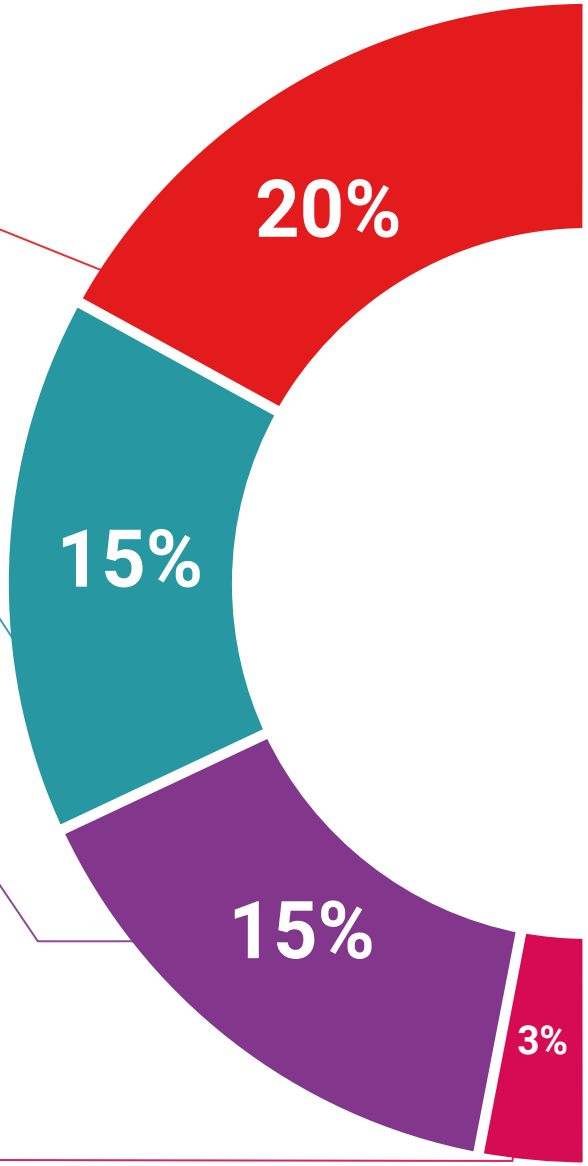
### Resúmenes interactivos

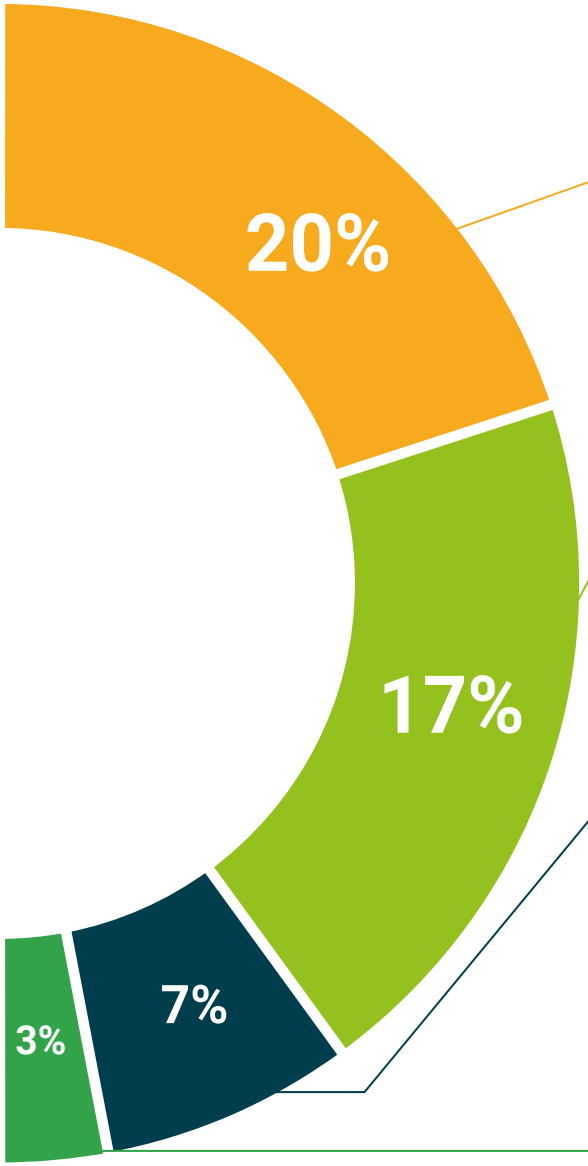
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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

### Lecturas complementarias

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






### *Case Studies*

Completarás una selección de los mejores *case studies* de la materia. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.

### Testing & Retesting

Evaluamos y reevaluamos periódicamente tu conocimiento a lo largo del programa. Lo hacemos sobre 3 de los 4 niveles de la Pirámide de Miller.

### 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 nuestras futuras decisiones difíciles.

### Guías rápidas de actuación

TECH ofrece los contenidos más relevantes del curso en forma de fichas o guías rápidas de actuación. Una manera sintética, práctica y eficaz de ayudar al estudiante a progresar en su aprendizaje.

05

# Titulación

Este programa en Seguridad Informática para las Comunicaciones garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Experto Universitario expedido por TECH Universidad.

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

Este programa te permitirá obtener el título de **Experto Universitario en Seguridad Informática para las Comunicaciones** emitido por TECH Universidad.

TECH es una Universidad española oficial, que forma parte del Espacio Europeo de Educación Superior (EEES). Con un enfoque centrado en la excelencia académica y la calidad universitaria a través de la tecnología.

Este título propio contribuye de forma relevante al desarrollo de la educación continua y actualización del profesional, garantizándole la adquisición de las competencias en su área de conocimiento y aportándole un alto valor curricular universitario a su formación.

Es 100% válido en todas las Oposiciones, Carrera Profesional y Bolsas de Trabajo de cualquier Comunidad Autónoma española.

Además, el riguroso sistema de garantía de calidad de TECH asegura que cada título otorgado cumpla con los más altos estándares académicos, brindándole al egresado la confianza y la credibilidad que necesita para destacarse en su carrera profesional.

Título: **Experto Universitario en Seguridad Informática para las Comunicaciones**

Modalidad: **online**

Duración: **3 meses**

Acreditación: **18 ECTS**


tech universidad

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

**Experto Universitario en Seguridad Informática para las Comunicaciones**

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 es una universidad Oficial Española legalmente reconocida mediante la Ley 1/2024, del 16 de abril, de la Comunidad Autónoma de Canarias, publicada en el Boletín Oficial del Estado (BOE) núm. 181, de 27 de julio de 2024 (pág. 96.369) e integrada en el Registro de Universidades, Centros y Títulos (RUCT) del Ministerio de Ciencia, Innovación y Universidades con el código 104.

En San Cristóbal de la Laguna, a 28 de febrero de 2024

Dr. Pedro Navarro Illana
Rector

código único TECH: AFWDR23S 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 realizará las gestiones oportunas para su obtención, con un coste adicional.

tech universidad

# Experto Universitario
## Seguridad Informática para las Comunicaciones

- Modalidad: **online**
- Duración: **3 meses**
- Titulación: **TECH Universidad**
- Acreditación: **18 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

# Experto Universitario
## Seguridad Informática para las Comunicaciones

tech universidad