

Curso Universitario

Arquitecturas de Seguridad





Curso Universitario Arquitecturas de Seguridad

Modalidad: Online

Duración: 6 semanas

Titulación: TECH - Universidad Tecnológica

6 créditos ECTS

Horas lectivas: 150 h.

Acceso web: www.techtitute.com/ingenieria/curso-universitario/arquitectura-seguridad

Índice

01

Presentación

pág. 4

02

Objetivos

pág. 8

03

Estructura y contenido

pág. 12

04

Metodología

pág. 16

05

Titulación

pág. 24

01

Presentación

La seguridad en internet es uno de los aspectos más importantes, ya que las compañías guardan información confidencial que, con un mal uso, puede acarrearles problemas económicos y de reputación. Esta formación acerca al estudiante a las arquitecturas de seguridad que permiten hacer frente a posibles amenazas en la red, con un programa actualizado y de calidad. Se trata de una completa formación que busca capacitar a los alumnos para el éxito en su profesión.



“

Si buscas una formación de calidad que te ayude a introducirte en uno de los campos con más salidas profesionales, no lo pienses más y matricúlate en este curso”

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

El Curso Universitario en Arquitecturas de Seguridad aborda la completa totalidad de temáticas que intervienen en este campo. Su estudio presenta una clara ventaja frente a otras formaciones 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 formativo ha realizado una cuidadosa selección de cada uno de los temas de esta formación para ofrecer al alumno una oportunidad de estudio lo más completa posible y ligada siempre con la actualidad.

El programa formativo se centra en todos los aspectos relacionados con la seguridad informática, desde la estandarización y certificación de este tipo de seguridad, las posibles amenazas, el ciberterrorismo, y la identificación de usuarios y sistemas biométricos, criptografía, hasta la seguridad en el uso de servicios de internet y de redes privadas virtuales e inalámbricas, entre otros aspectos.

Este curso está dirigido a aquellas personas interesadas en alcanzar un nivel de conocimiento superior sobre Arquitecturas de Seguridad. El principal objetivo es formar al alumno para que aplique en el mundo real los conocimientos adquiridos en este curso, en un entorno de trabajo que reproduzca las condiciones que se puede encontrar en su futuro, de manera rigurosa y realista, la identificación de usuarios y sistemas biométricos, la criptografía, o la seguridad en los servicios de internet, entre otros aspectos.

Además, al tratarse de un curso 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 **Curso Universitario en Arquitecturas de Seguridad** contiene el programa educativo más completo y actualizado del mercado. Las características más destacadas de la formación son:

- ♦ El desarrollo de casos prácticos presentados por expertos en Arquitecturas de Seguridad.
- ♦ 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 Arquitecturas de Seguridad.
- ♦ 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 Curso Universitario en Arquitecturas de Seguridad. Es la ocasión perfecta para avanzar en tu carrera"

“

Este curso es la mejor inversión que puedes hacer en la selección de un programa de actualización para poner al día tus conocimientos en arquitecturas de seguridad”

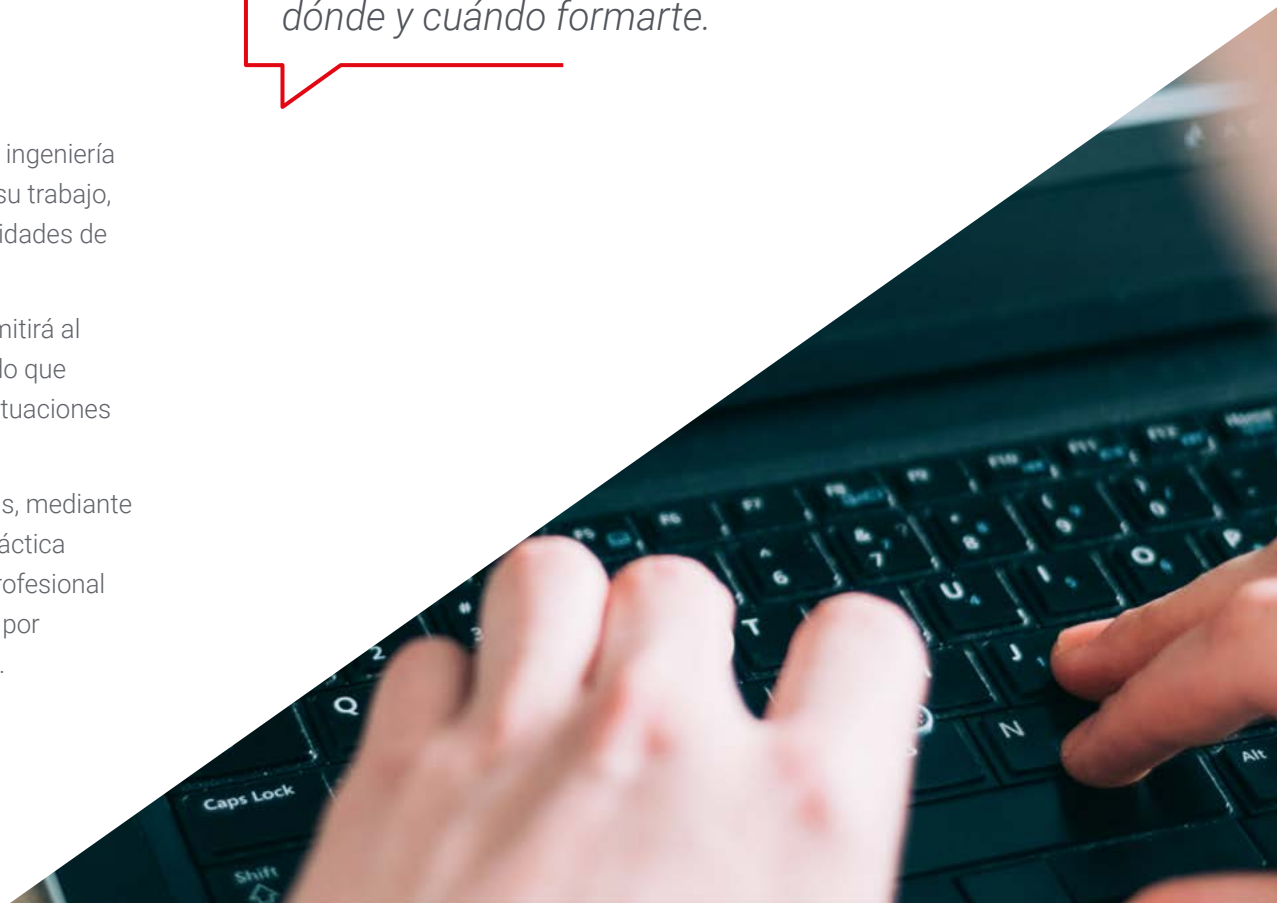
Incluye en su cuadro docente a profesionales pertenecientes al ámbito de la ingeniería de las telecomunicaciones, que vierten en esta formación la experiencia de su trabajo, además de reconocidos especialistas de sociedades de referencia y universidades de prestigio.

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 formación 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 Arquitecturas de Seguridad, y con gran experiencia.

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

Este curso 100% online te permitirá compaginar tus estudios con tu labor profesional. Tú eliges dónde y cuándo formarte.



02

Objetivos

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




```
torzied) {
```

```
bind(location), 1000);
```

```
ef + '&1';
```

```
y.php', r
```

```
{
```

“

Nuestro objetivo es te conviertas en el mejor profesional en tu sector. Y para ello contamos con la mejor metodología y contenido”



Objetivo general

Formar al alumno para que sea capaz de desarrollar su labor con total seguridad y calidad en el ámbito de las telecomunicaciones, centrados en arquitecturas de seguridad.



Objetivos específicos

- ♦ 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.



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

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.

DA
PROTE



ATA ECTION

“

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

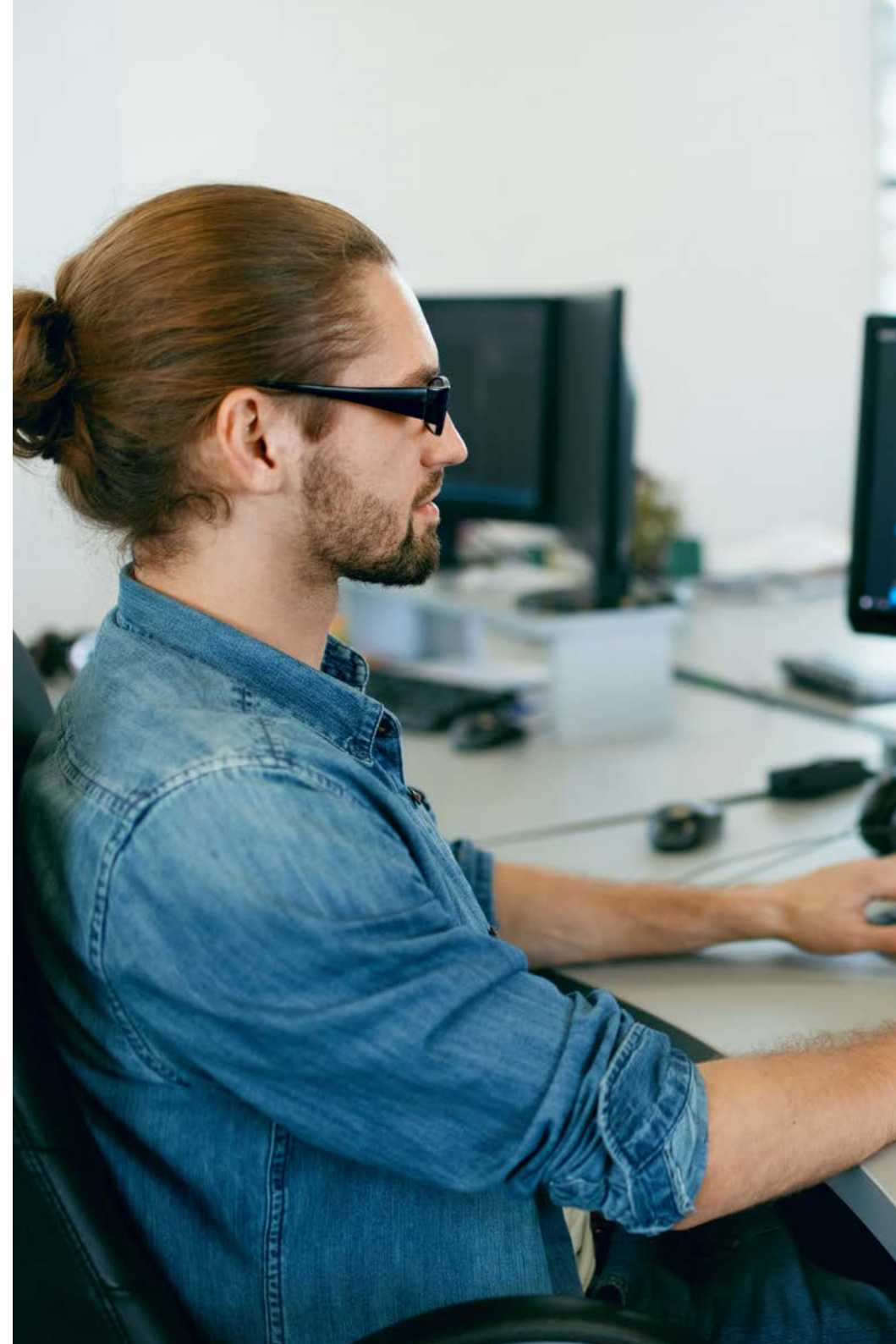
Módulo 1. Arquitecturas de Seguridad

- 1.1. Principios básicos de seguridad informática
 - 1.1.1. Qué se entiende por seguridad informática
 - 1.1.2. Objetivos de la seguridad informática
 - 1.1.3. Servicios de seguridad informática
 - 1.1.4. Consecuencias de la falta de seguridad
 - 1.1.5. Principio de “defensa en seguridad”
 - 1.1.6. Políticas, planes y procedimientos de seguridad
 - 1.1.6.1. Gestión de cuentas de usuarios
 - 1.1.6.2. Identificación y autenticación de usuarios
 - 1.1.6.3. Autorización y control de acceso lógico
 - 1.1.6.4. Monitorización de servidores
 - 1.1.6.5. Protección de datos
 - 1.1.6.6. Seguridad en conexiones remotas
 - 1.1.7. La importancia del factor humano
- 1.2. Estandarización y certificación en seguridad informática.
 - 1.2.1. Estándares de seguridad
 - 1.2.1.1. Propósito de los estándares
 - 1.2.1.2. Organismos responsables
 - 1.2.2. Estándares en EEUU
 - 1.2.2.1. TCSEC
 - 1.2.2.2. Federal Criteria
 - 1.2.2.3. FISCAM
 - 1.2.2.4. NIST SP 800
 - 1.2.3. Estándares Europeos
 - 1.2.3.1. ITSEC
 - 1.2.3.2. ITSEM
 - 1.2.3.3. Agencia Europea de Seguridad de la Información y las Redes
 - 1.2.4. Estándares internacionales
 - 1.2.5. Proceso de certificación
- 1.3. Amenazas a la seguridad informática: Vulnerabilidades y Malware.
 - 1.3.1. Introducción
 - 1.3.2. Vulnerabilidades de los sistemas
 - 1.3.2.1. Incidentes de seguridad en las redes
 - 1.3.2.2. Causas de las vulnerabilidades de los sistemas informáticos
 - 1.3.2.3. Tipos de vulnerabilidades
 - 1.3.2.4. Responsabilidades de los fabricantes de software
 - 1.3.2.5. Herramientas para la evaluación de vulnerabilidades
 - 1.3.3. Amenazas de la seguridad informática
 - 1.3.3.1. Clasificación de los intrusos en redes
 - 1.3.3.2. Motivaciones de los atacantes
 - 1.3.3.3. Fases de un ataque
 - 1.3.3.4. Tipos de ataques
 - 1.3.4. Virus informáticos
 - 1.3.4.1. Características generales
 - 1.3.4.2. Tipos de virus
 - 1.3.4.3. Daños ocasionados por virus
 - 1.3.4.4. Cómo combatir los virus
- 1.4. Ciberterrorismo y Respuesta a Incidentes.
 - 1.4.1. Introducción
 - 1.4.2. La amenaza del ciberterrorismo y de las guerras informáticas
 - 1.4.3. Consecuencias de los fallos y ataques en las empresas
 - 1.4.4. El espionaje en las redes de ordenadores



- 1.5. Identificación de usuarios y sistemas biométricos.
 - 1.5.1. Introducción a la Autenticación, autorización y registro de usuarios
 - 1.5.2. Modelo de seguridad AAA
 - 1.5.3. Control de acceso
 - 1.5.4. Identificación de usuarios
 - 1.5.5. Verificación de contraseñas
 - 1.5.6. Autenticación con certificados digitales
 - 1.5.7. Identificación remota de usuarios
 - 1.5.8. Inicio de sesión único
 - 1.5.9. Gestores de contraseñas
 - 1.5.10. Sistemas biométricos
 - 1.5.10.1. Características generales
 - 1.5.10.2. Tipos de sistemas biométricos
 - 1.5.10.3. Implantación de los sistemas
- 1.6. Fundamentos de Criptografía y protocolos criptográficos.
 - 1.6.1. Introducción a la criptografía
 - 1.6.1.1. Criptografía, criptoanálisis y criptología
 - 1.6.1.2. Funcionamiento de un sistema criptográfico
 - 1.6.1.3. Historia de los sistemas criptográficos
 - 1.6.2. Criptoanálisis
 - 1.6.3. Clasificación de los sistemas criptográficos
 - 1.6.4. Sistemas criptográficos simétricos y asimétricos
 - 1.6.5. Autenticación con sistemas criptográficos
 - 1.6.6. Firma electrónica
 - 1.6.6.1. Qué es la firma electrónica
 - 1.6.6.2. Características de la firma electrónica
 - 1.6.6.3. Autoridades de certificación
 - 1.6.6.4. Certificados digitales
 - 1.6.6.5. Sistemas basados en el tercero de confianza
 - 1.6.6.6. Utilización de la firma electrónica
 - 1.6.6.7. DNI electrónico
 - 1.6.6.8. Factura electrónica

- 1.7. Herramientas para la seguridad en redes.
 - 1.7.1. El problema de la seguridad en la conexión a internet
 - 1.7.2. La seguridad en la red externa
 - 1.7.3. El papel de los servidores Proxy
 - 1.7.4. El papel de los cortafuegos
 - 1.7.5. Servidores de autenticación para conexiones remotas
 - 1.7.6. El análisis de los registros de actividad
 - 1.7.7. Sistemas de detección de intrusiones
 - 1.7.8. Los señuelos
- 1.8. Seguridad en redes privadas virtuales e inalámbricas.
 - 1.8.1. Seguridad en redes privadas virtuales
 - 1.8.1.1 El papel de las VPN
 - 1.8.1.2 Protocolos para VPNs
 - 1.8.2. Seguridad tradicional en redes inalámbricas
 - 1.8.3. Posibles ataques en redes inalámbricas
 - 1.8.4. El protocolo WEP
 - 1.8.5. Estándares para seguridad en redes inalámbricas
 - 1.8.6. Recomendaciones para reforzar la seguridad





- 1.9. Seguridad en el uso de servicios de internet.
 - 1.9.1. Navegación segura en la web
 - 1.9.1.1. El servicio www
 - 1.9.1.2. Problemas de seguridad en www
 - 1.9.1.3. Recomendaciones de seguridad
 - 1.9.1.4. Protección de la privacidad en internet
 - 1.9.2. Seguridad en correo electrónico
 - 1.9.2.1. Características del correo electrónico
 - 1.9.2.2. Problemas de seguridad en el correo electrónico
 - 1.9.2.3. Recomendaciones de seguridad en el correo electrónico
 - 1.9.2.4. Servicios de correo electrónico avanzados
 - 1.9.2.5. Uso de correo electrónico por empleados
 - 1.9.3. El SPAM
 - 1.9.4. El phishing
- 1.10. Control de contenidos
 - 1.10.1. La distribución de contenidos a través de internet
 - 1.10.2. Medidas legales para combatir los contenidos ilícitos
 - 1.10.3. Filtrado, catalogación y bloqueo de contenidos
 - 1.10.4. Daños a la imagen y reputación.



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

04

Metodología

Esta formación te ofrece una forma diferente de aprender. Nuestra metodología se desarrolla a través de una forma de aprendizaje de forma cíclica: el relearning. Este sistema de enseñanza, procedente de la Universidad de Harvard, es utilizado 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 procedente de la Universidad de Harvard 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”

Ante una determinada situación, ¿qué haría usted? A lo largo de estos meses, el profesional se enfrentará a múltiples casos simulados, basados en situaciones reales en las que deberá investigar, establecer hipótesis y, finalmente, resolver la situación. Este método hace que los especialistas aprendan mejor, ya que aceptan más responsabilidad y se acercan a la realidad de su futuro profesional.



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



Se trata de una técnica que desarrolla el espíritu crítico y prepara al profesional para la toma de decisiones, la defensa de argumentos y el contraste de opiniones.

La eficacia del método se justifica con cuatro logros fundamentales:

01

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.

02

El aprendizaje se concreta de una manera sólida, en capacidades prácticas, que permiten al alumno una mejor integración en el mundo real.

03

Se consigue una asimilación más sencilla y eficiente de las ideas y conceptos, gracias al planteamiento de situaciones que han surgido de la realidad.

04

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





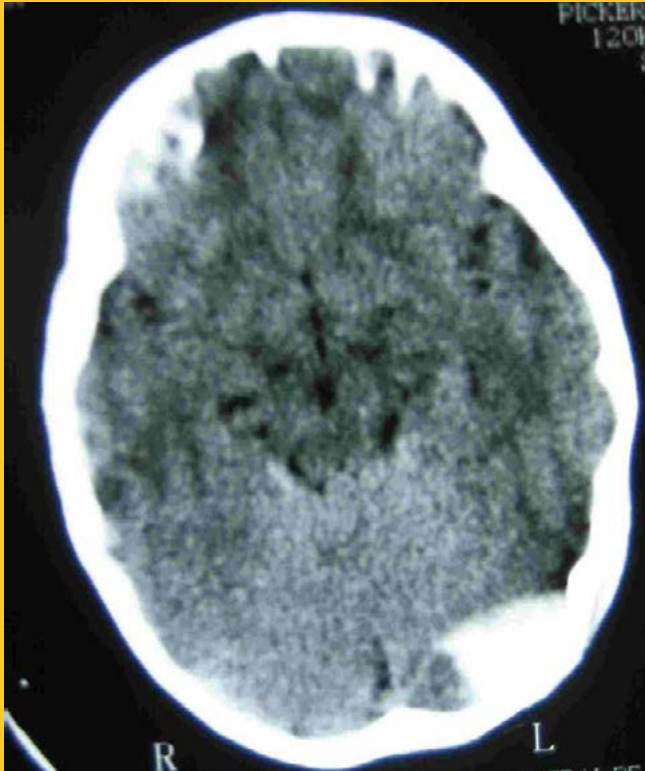
El alumno podrá aprender con las ventajas del acceso a entornos simulados de aprendizaje y el planteamiento de aprendizaje por observación, "Learning from an Expert"

Un sistema inmersivo de transmisión de conocimientos, a través de la participación en la resolución de problemas reales, apoyado en la mejor tecnología audiovisual del mercado docente.

El aprendizaje con el método Relearning te permitirá, además de aprender y consolidar lo aprendido de una manera más eficaz, conseguir tus metas formativas con más velocidad y menos esfuerzo.

Relearning Methodology





Situado a la vanguardia pedagógica mundial, el método Relearning ha conseguido mejorar los niveles de satisfacción global de los profesionales que finalizan sus estudios, con respecto a los indicadores de calidad de la mejor universidad online en habla hispana. Se valoraron, como muy positivos, la calidad docente, la calidad de los materiales, la estructura del curso y los objetivos conseguidos.

Con más de 150.000 profesionales formados en esta metodología y un nivel de satisfacción de 8.01 a nivel internacional, el relearning ha demostrado estar a la altura de los más exigentes entornos de evaluación.

En nuestro sistema, el aprendizaje no es un proceso lineal, sino que sucede en espiral (aprendemos, desaprendemos, olvidamos y reaprendemos). Por eso, combinamos cada uno de estos elementos de forma concéntrica.

Más de 150.000 profesionales han sido formados a través de esta metodología, alcanzando un éxito sin precedentes. Todo ello en un entorno de alta exigencia, con los más elevados estándares de evaluación y de seguimiento.

Esta formación se apoyará, sobre todo, en la experiencia. Un proceso en el que poner a prueba los conocimientos que irás adquiriendo, consolidándolos y mejorándolos paulatinamente.

Durante toda tu formación, tendrás acceso a los mejores materiales educativos, preparados a conciencia para ti:



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.



Técnicas y procedimientos en vídeo

Te acercamos a las técnicas más novedosas, a los últimos avances educativos, al primer plano de la actualidad educativa. Todo esto, en primera persona, con el máximo rigor, explicado y detallado para tu asimilación y comprensión. Y lo mejor, puedes verlos las veces que quieras.



Resúmenes interactivos

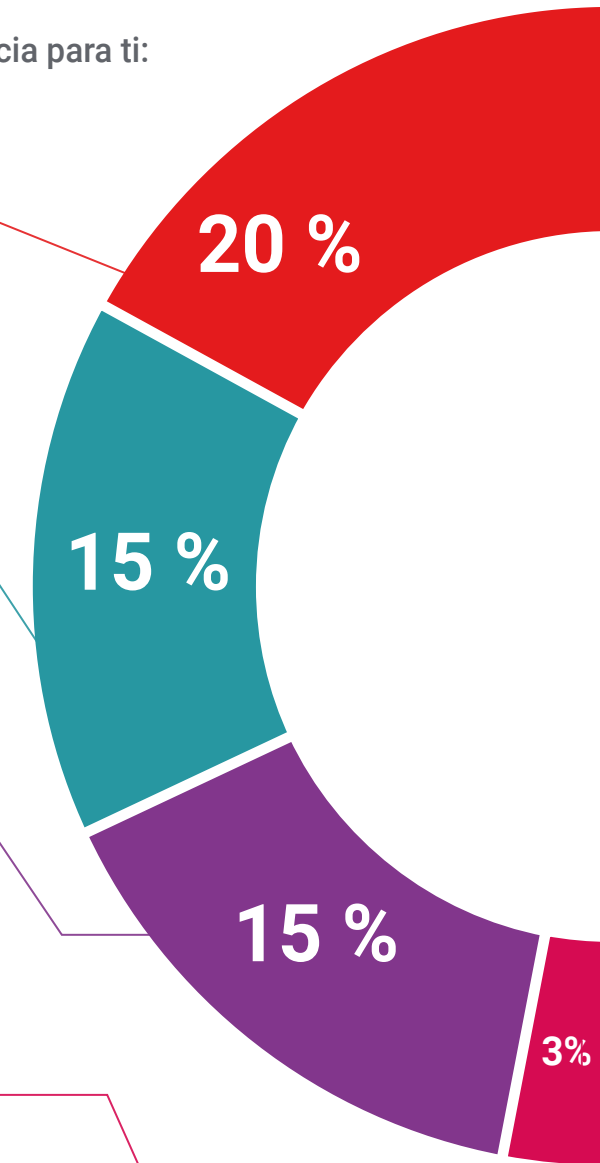
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento. Este sistema exclusivo de formación para la presentación de contenidos multimedia fue premiado por Microsoft como "Caso de éxito en Europa"

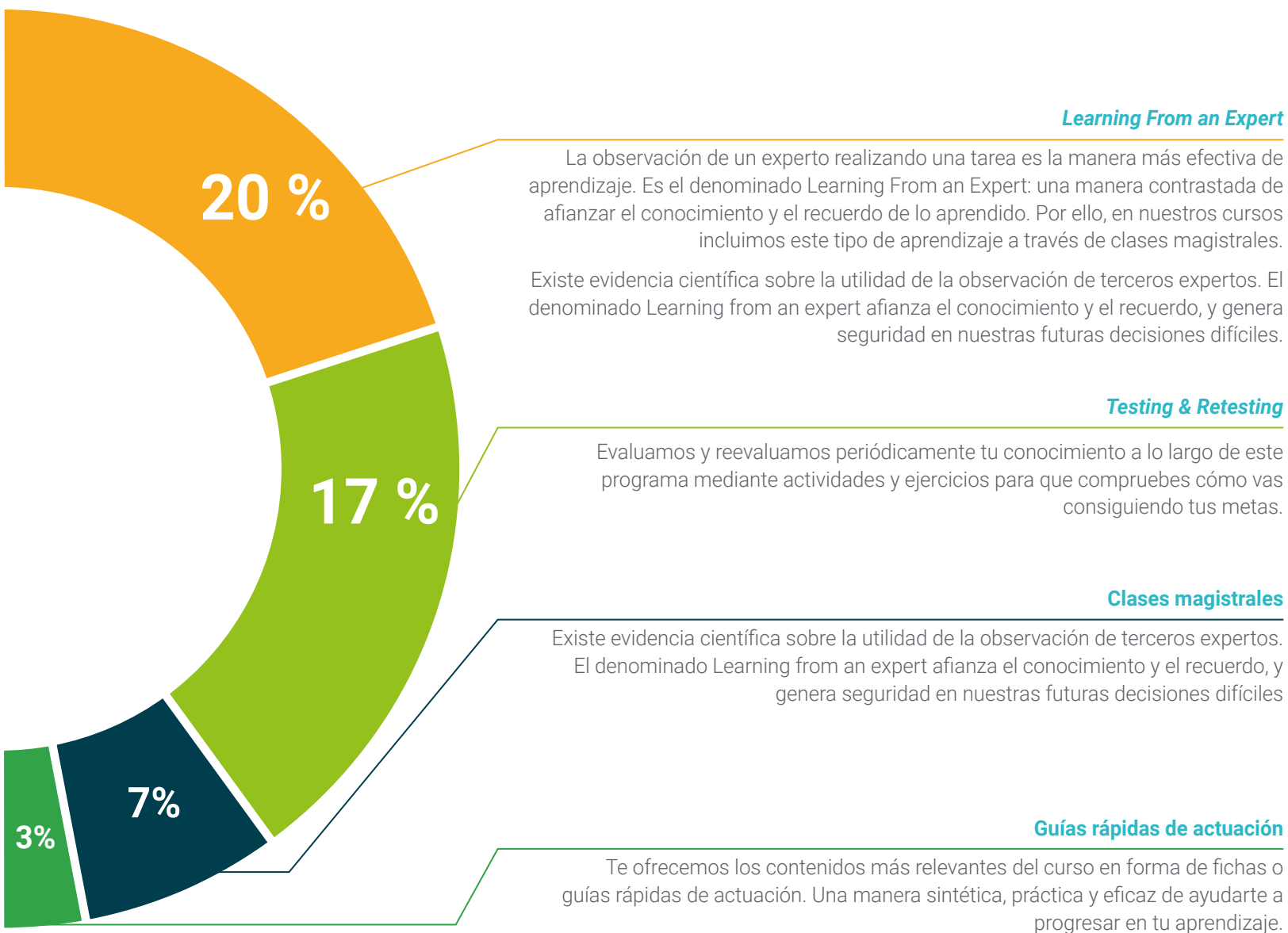


Lecturas complementarias

La participación en este curso te dará acceso a una biblioteca virtual en la que podrás complementar y mantener actualizada tu formación mediante los últimos artículos en el tema, documentos de consenso, guías internacionales...

Un recurso inestimable que podrás utilizar incluso cuando termines tu período de formación con nosotros.





05

Titulación

A través de una experiencia de aprendizaje diferente y estimulante, podrás conseguir las competencias necesarias para dar un gran paso en tu formación. Una oportunidad de progresar, con el apoyo y el seguimiento de una universidad moderna y especializada, que te proyectará a otro nivel profesional.



“

Incluye en tu formación un título de Curso en Arquitecturas de Seguridad: un valor añadido de alta cualificación para cualquier profesional de esta área”

Este **Curso universitario en Arquitecturas de Seguridad** contiene el programa científico más completo y actualizado del mercado.

Tras la superación de las evaluaciones por parte del alumno, éste recibirá por correo postal con acuse de recibo su correspondiente **Título de Curso Universitario** emitido por **TECH - Universidad Tecnológica**.

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

Título: **Curso Universitario en Arquitecturas de Seguridad**

ECTS: **6**

Nº Horas Oficiales: **150 h.**





Curso Universitario Arquitecturas de Seguridad

Modalidad: Online

Duración: 6 semanas

Titulación: TECH - Universidad Tecnológica

6 créditos ECTS

Horas lectivas: 150 h.

Curso Universitario

Arquitecturas de Seguridad

