Diplomado

Arquitecturas de Seguridad



tech universidad tecnológica



tech universidad tecnológica

Diplomado

Arquitecturas de Seguridad

Modalidad: **Online**
Duración: **6 semanas**
Titulación: **TECH Universidad Tecnológica**
Horas lectivas: **150 h.**
Acceso web: **www.techtitute.com/informatica/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 capacitación 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 capacitación que busca capacitar a los alumnos para el éxito en su profesión.





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

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.

El Diplomado en Arquitecturas de Seguridad 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.

El programa educativo 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 Diplomado está dirigido a aquellas personas interesadas en alcanzar un nivel de conocimiento superior sobre Arquitecturas de Seguridad. El principal objetivo es capacitar al alumno para que aplique en el mundo real los conocimientos adquiridos en este Diplomado, 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 Diplomado 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 **Diplomado en Arquitecturas de Seguridad** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas 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 Diplomado en Arquitecturas de Seguridad. Es la ocasión perfecta para avanzar en tu carrera"

Este Diplomado 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"

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

Este Diplomado 100% online te permitirá compaginar tus estudios con tu labor profesional.

Incluye en su cuadro docente a profesionales pertenecientes al ámbito de la ingeniería 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 Arquitecturas de Seguridad, y con gran experiencia.

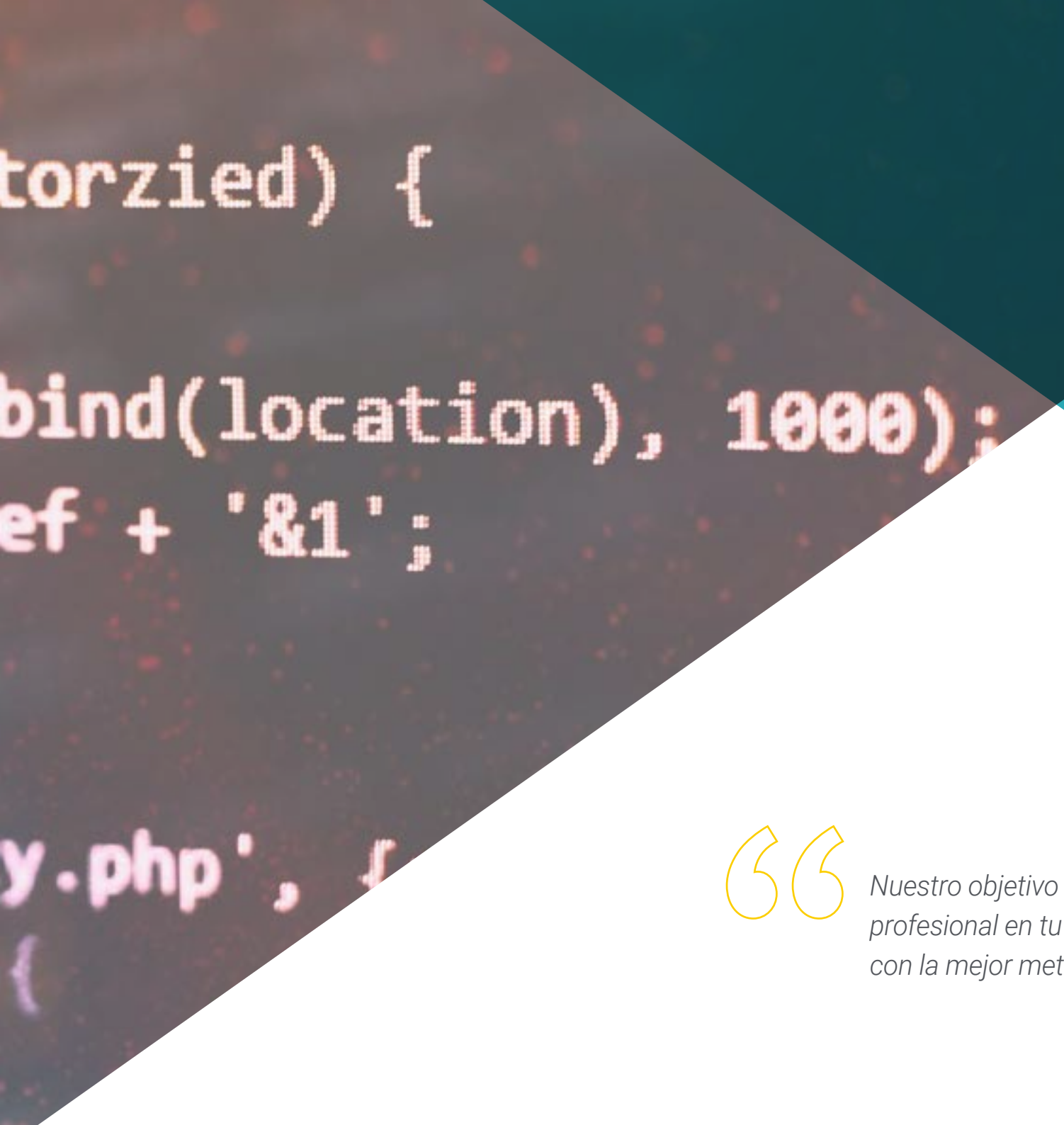


02

Objetivos

El Diplomado 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.





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

Objetivo general

- Capacitar 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

Especialízate en la principal universidad online privada de habla hispana del mundo"





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

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 educativo 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 EE.UU
  - 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 *Phising*

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

04

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.

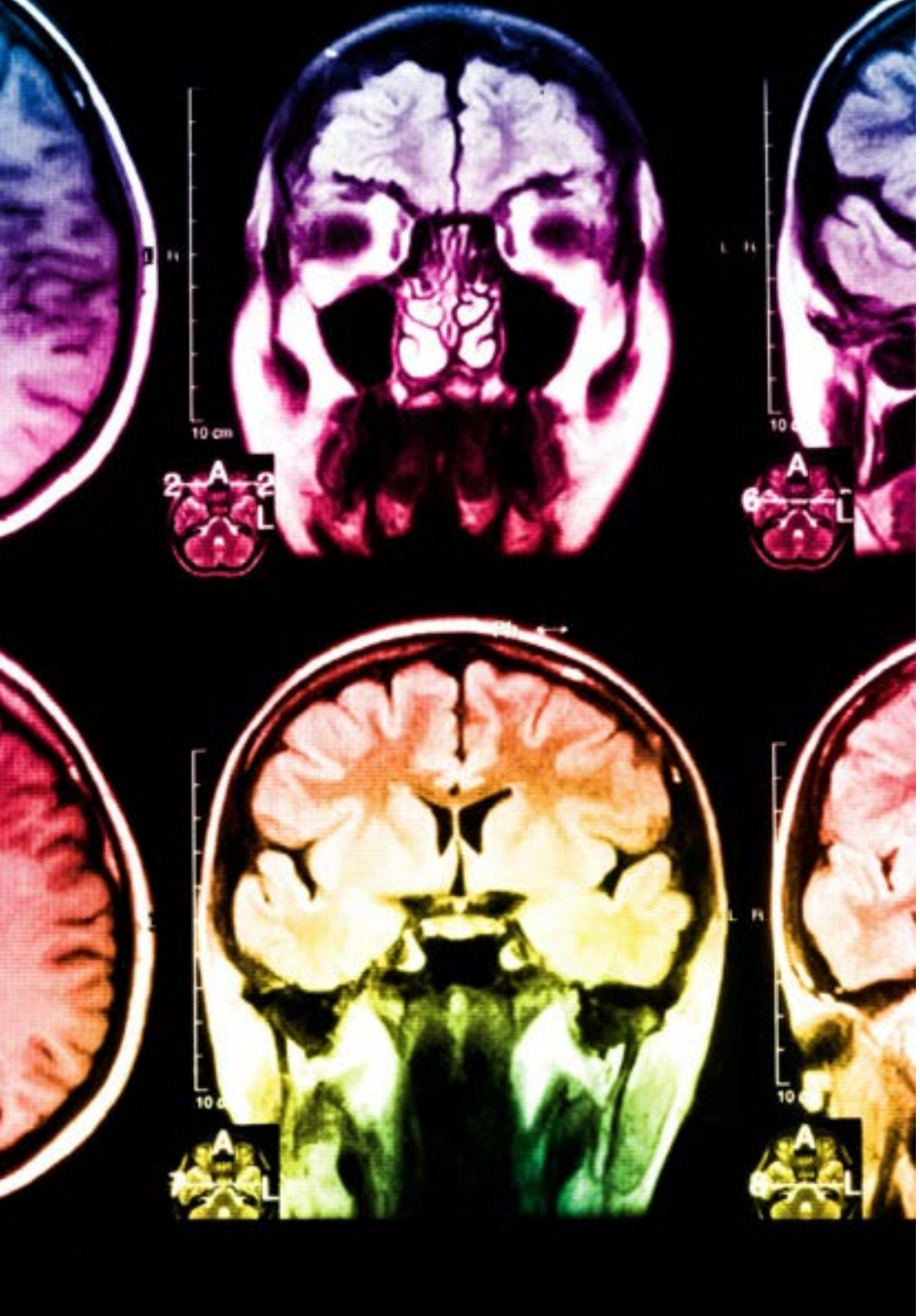
Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el Relearning.

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.

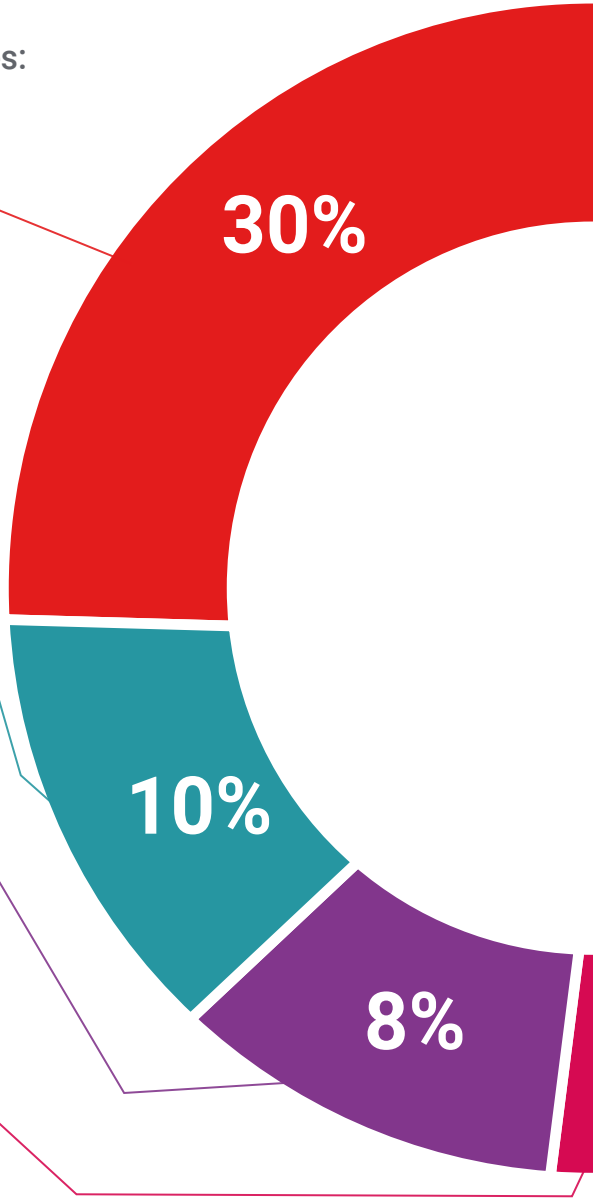
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

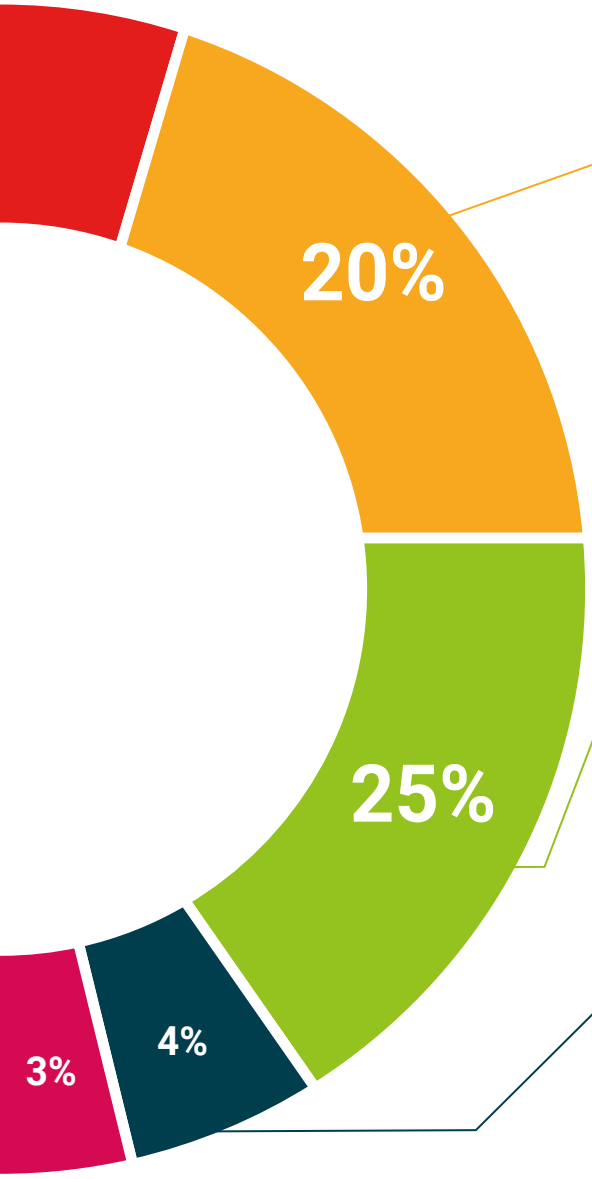
Prácticas de habilidades y competencias

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.

05

Titulación

El Diplomado en Arquitecturas de Seguridad 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 tu titulación universitaria sin desplazamientos ni farragosos trámites”

Este **Diplomado en Arquitecturas de Seguridad** 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 Arquitecturas de Seguridad**

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

Arquitecturas de Seguridad

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

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

Arquitecturas de Seguridad

Modalidad: **Online**

Duración: **6 semanas**

Titulación: **TECH Universidad Tecnológica**

Horas lectivas: **150 h.**

Diplomado

Arquitecturas de Seguridad



tech universidad tecnológica