Experto Universitario
Seguridad IT



tech universidad tecnológica



tech universidad tecnológica

Experto Universitario
Seguridad IT

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

Índice

01 Presentación — pág. 4

02 Objetivos — pág. 8

03 Dirección del curso — pág. 12

04 Estructura y contenido — pág. 16

05 Metodología — pág. 22

06 Titulación — pág. 30

01

Presentación

Las tecnologías de la información son el presente y el futuro en numerosos procesos sociales y empresariales. Así, en la actualidad estas herramientas son imprescindibles para la comunicación interpersonal, para la realización de compras y ventas o para entrar en contacto con clientes y proveedores. Su popularización ha hecho que tengan presencia en todo tipo de ámbitos, por lo que son un objetivo muy codiciado para aquellos que desean explotar sus vulnerabilidades. En ese contexto, el especialista en Seguridad IT se ha convertido en un perfil profesional muy demandado. Por eso, se ha diseñado cuidadosamente este programa, con el que el informático podrá ponerse al tanto en todos los aspectos en ciberseguridad aplicada a estas tecnologías, mejorando sus perspectivas profesionales de forma inmediata.





Este programa te permitirá especializarte en Seguridad IT, lo que te dará acceso a grandes oportunidades profesionales en un área de la informática cada vez más demandada"

El nuevo contexto tecnológico exige por parte del profesional una profundización para adaptarse a las transformaciones existentes en la Seguridad IT. Así, estas tecnologías de la información están omnipresentes y se emplean en todo tipo de procesos del ámbito empresarial y social. Por eso, hay numerosos aspectos que corren el riesgo de ser expuestos a vulnerabilidades explotables.

Esta situación preocupa enormemente a las compañías, que ven cómo una seguridad inadecuada puede poner en peligro su negocio. La solución, pues, es la contratación de profesionales especializados en este ámbito, por lo que el informático enfocado hacia la Seguridad IT es, en la actualidad, uno de los perfiles más buscados y mejor valorados por corporaciones de diferentes áreas y sectores.

Respondiendo a esa demanda, se presenta este Experto Universitario, que se desarrolla mediante un formato 100% online, y que cuenta con un cuadro docente de enorme prestigio internacional en este campo de la ciberseguridad. Además, este programa presenta sus contenidos en diversos formatos multimedia: resúmenes interactivos, vídeos, estudios de caso, clases magistrales, actividades prácticas, etc. Todo para alcanzar el objetivo de proporcionar al profesional las últimas novedades en la seguridad aplicada a las tecnologías de la información.

Este **Experto Universitario en Seguridad IT** contiene el programa más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en Informática y Ciberseguridad
- Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que está concebido recogen una información científica y práctica sobre aquellas disciplinas indispensables para el ejercicio profesional
- Los ejercicios prácticos donde realizar el proceso de autoevaluación para mejorar el aprendizaje
- Su especial hincapié en metodologías innovadoras
- Las lecciones teóricas, preguntas al experto, foros de discusión de temas controvertidos y trabajos de reflexión individual
- La disponibilidad de acceso a los contenidos desde cualquier dispositivo fijo o portátil con conexión a internet

Con este programa podrás profundizar en aspectos relevantes de la Seguridad IT como el desarrollo seguro en comunicaciones y operación software”

El sistema de enseñanza 100% online de TECH te permitirá compaginar tu trabajo con los estudios, ya que se adapta a todas tus circunstancias personales y profesionales"

El profesorado de este programa está compuesto por profesionales en activo que conocen todas las novedades en esta área de la ciberseguridad.

Tu perfil profesional mejorará una vez completes este Experto Universitario, que se imparte a partir de numerosos recursos multimedia.

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 curso académico. Para ello, contará con la ayuda de un novedoso sistema de vídeo interactivo realizado por reconocidos expertos.



02

Objetivos

El principal objetivo de este Experto Universitario en Seguridad IT es ofrecer al profesional las mejores herramientas para poder adaptarse al nuevo contexto informático, transformado por el proceso de digitalización que se ha extendido por todos los ámbitos de la sociedad. Así, estará en la mejor posición para trabajar como especialista en ciberseguridad en cualquier compañía que desee proteger su negocio de las nuevas amenazas informáticas.

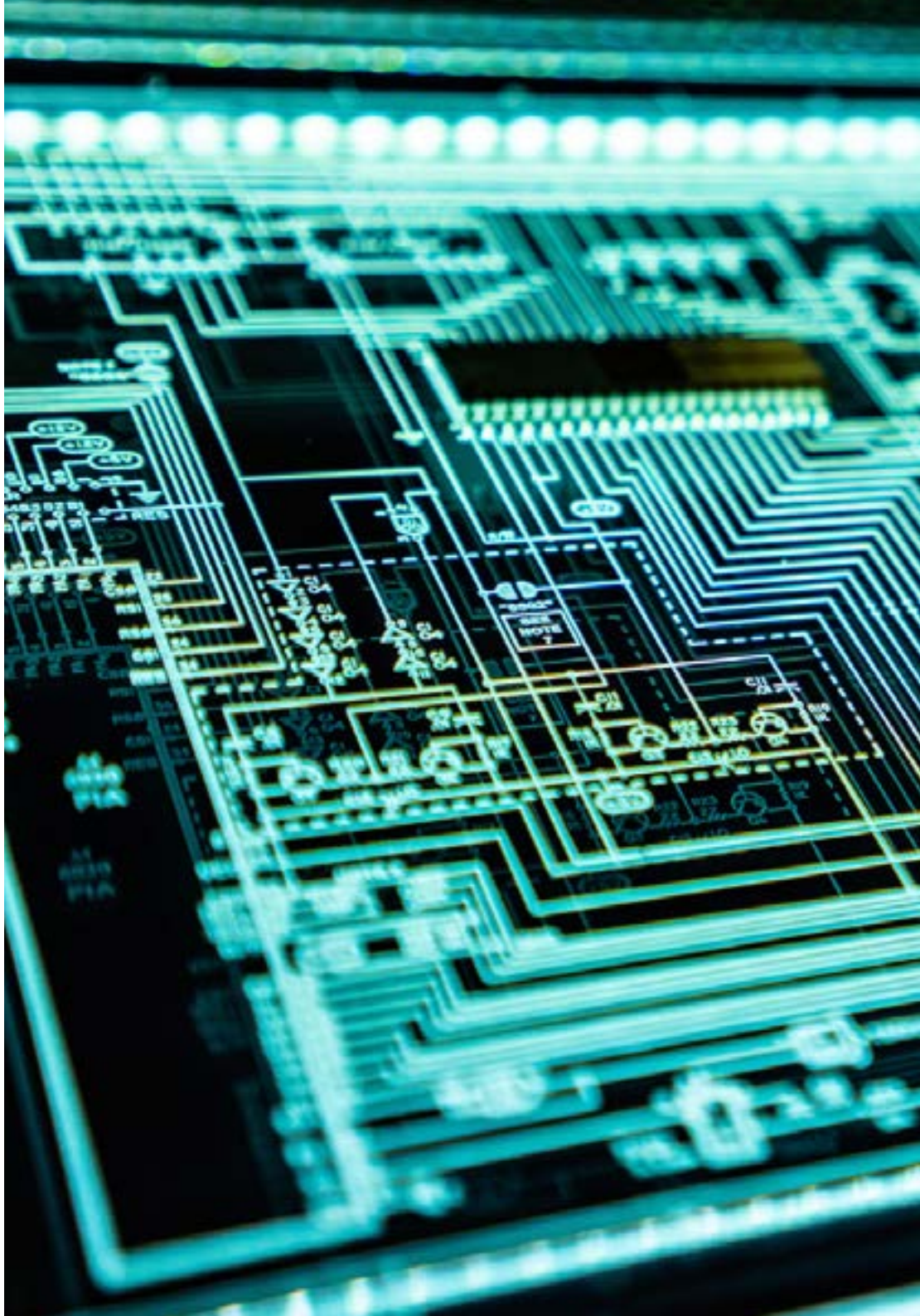




El objetivo de TECH es proporcionarte los conocimientos más actualizados para que puedas desarrollar tu trabajo con las máximas garantías, convirtiéndote en un profesional de referencia en el sector”

Objetivos generales

- Generar conocimiento especializado sobre un sistema de información, tipos y aspectos de seguridad que deben ser tenidos en cuenta
- Identificar las vulnerabilidades de un Sistema de Información
- Aplicar las medidas de seguridad más adecuadas dependiendo de las amenazas
- Desarrollar la normativa legal y tipificación del delito atacando a un Sistema de Información
- Determinar la política y plan de seguridad en el sistema de información de una compañía, completando el diseño y puesta en marcha del Plan de Contingencia
- Generar conocimiento especializado sobre el ecosistema de seguridad informática
- Evaluar el conocimiento en término de ciberseguridad
- Desarrollar las mejores prácticas en el desarrollo seguro
- Presentar los riesgos que supone a las compañías no tener un entorno de seguridad informática
- Examinar el proceso de diseño de una estrategia de seguridad al desplegar servicios corporativos en *Cloud*
- Identificar los ámbitos de seguridad en *Cloud*
- Analizar los servicios y herramientas en cada uno de los ámbitos de seguridad
- Evaluar las diferencias en las implementaciones concretas de diferentes vendedores de *Cloud* pública



Objetivos específicos

Módulo 1. Seguridad en el diseño y desarrollo de sistemas

- Evaluar la seguridad de un sistema de información en todos sus componentes y capas
- Identificar los tipos de amenazas de seguridad actuales y su tendencia
- Establecer directrices de seguridad definiendo políticas y planes de seguridad y contingencia
- Analizar estrategias y herramientas para asegurar la integridad y seguridad de los sistemas de información
- Aplicar las técnicas y herramientas específicas para cada tipo de ataque o vulnerabilidad de seguridad
- Proteger la información sensible almacenada en el sistema de información
- Disponer del marco legal y tipificación del delito, completando la visión con la tipificación del delincuente y su víctima

Módulo 2. Seguridad en comunicaciones y operación software

- Desarrollar conocimiento especializado en materia de seguridad física y lógica
- Demostrar el conocimiento en comunicaciones y redes
- Identificar principales ataques maliciosos
- Establecer un marco de desarrollo seguros
- Demostrar conocer las principales normativas de sistemas de gestión de la seguridad de la información
- Fundamentar el funcionamiento de un centro de operaciones en materias de ciberseguridad
- Demostrar la importancia de contar con prácticas en ciberseguridad para catástrofes organizativas

Módulo 3. Seguridad en entornos *Cloud*

- Identificar riesgos de un despliegue de infraestructura en *Cloud* pública
- Definir los requerimientos de seguridad
- Desarrollar un plan de seguridad para un despliegue en *Cloud*
- Identificar los servicios *Cloud* a desplegar para la ejecución de un plan de seguridad
- Determinar la operativa necesaria para los mecanismos de prevención
- Establecer las directrices para un sistema de *Logging* y monitorización
- Proponer acciones de respuesta ante incidentes

Podrás progresar profesionalmente de forma rápida, ya que tus nuevos conocimientos te situarán como un especialista muy demandado”

03

Dirección del curso

La seguridad en las tecnologías de la información es un área que evoluciona constantemente, por lo que se necesitan los conocimientos más avanzados que solo un profesional en activo puede proporcionar. Por eso, TECH ha puesto su empeño en hacer que prestigiosos especialistas en este campo se encarguen de la docencia del programa, haciendo que el alumno disponga de las mejores habilidades para desenvolverse de forma efectiva en el diseño de la protección de cualquier empresa.





Este programa es lo que necesitas: tendrás a tu alcance los mayores especialistas en Seguridad IT a nivel internacional"

Dirección



D. Olalla Bonal, Martín

- Client Technical Specialist Blockchain en IBM
- Arquitecto *Blockchain*
- Arquitecto de Infraestructura en Banca
- Gestión de proyectos y puesta en producción de soluciones
- Técnico en Electrónica Digital
- Docente: Formación *Hyperledger Fabric* a empresas
- Docente: Formación *Blockchain* orientado a negocio en empresas



Profesores

D. Nogales Ávila, Javier

- Enterprise Cloud and sourcing senior consultant. Quint
- Cloud and Technology Consultant. Indra
- Associate Technology Consultant. Accenture
- Graduado por la Universidad de Jaén y University of Technology and Economics of Budapest (BME)
- Grado en Ingeniería de Organización Industrial

D. Gómez Rodríguez, Antonio

- Ingeniero de soluciones Cloud en Oracle
- Director de Proyectos en Sopra Group
- Director de Proyectos en Everis
- Jefe de Proyectos en Empresa pública de Gestion de Programas Culturales. Consejería de Cultura de Andalucía
- Analista de Sistemas de Información. Sopra Group
- Licenciado en Ingeniería Superior de Telecomunicación por la Universidad Politécnica de Cataluña
- Postgrado en Tecnologías y Sistemas de Información, Instituto Catalán de Tecnología
- E-Business Master, Escuela de Negocios La Salle

Dña. Jurado Jabonero, Lorena

- Responsable de Seguridad de la Información (CISO) en Grupo Pascual
- Graduada en Ingeniería Informática por la Universidad Alfonso X El Sabio
- Ingeniero Técnico en Informática de Gestión por la Universidad Politécnica de Madrid
- Conocimientos: ISO 27001, ISO 27701, ISO 22301, ISO 20000, RGPD/LOPDGDD, NIST CSF, CSA, ITIL, PCI, etc.

04

Estructura y contenido

Para alcanzar los objetivos propuestos, este Experto Universitario en Seguridad IT ha sido dividido en 3 módulos especializados, que podrán ser completados a lo largo de 450 horas de aprendizaje. Así, a lo largo de este programa, el informático podrá conocer los últimos avances en seguridad informática en comunicaciones y operación software, la seguridad en entornos *Cloud Computing*, la segurización de los sistemas de almacenamiento o los sistemas de autorización, entre muchos otros aspectos relevantes en esta área.





Este programa te permitirá aplicar las mejores técnicas de análisis forense aplicadas a la Seguridad IT”

Módulo 1. Seguridad en el diseño y desarrollo de sistemas

1.1. Sistemas de Información
- 1.1.1. Dominios de un sistema de información
- 1.1.2. Componentes de un sistema de información
- 1.1.3. Actividades de un sistema de información
- 1.1.4. Ciclo de vida de un sistema de información
- 1.1.5. Recursos de un sistema de información

1.2. Sistemas de información. Tipología
- 1.2.1. Tipos de sistemas de información
  - 1.2.1.1. Empresarial
  - 1.2.1.2. Estratégicos
  - 1.2.1.3. Según el ámbito de la aplicación
  - 1.2.1.4. Específicos
- 1.2.2. Sistemas de Información. Ejemplos reales
- 1.2.3. Evolución de los sistemas de información: etapas
- 1.2.4. Metodologías de los sistemas de información

1.3. Seguridad de los sistemas de información. Implicaciones legales
- 1.3.1. Acceso a datos
- 1.3.2. Amenazas de seguridad: vulnerabilidades
- 1.3.3. Implicaciones legales: delitos
- 1.3.4. Procedimientos de mantenimiento de un sistema de información

1.4. Seguridad de un sistema de información. Protocolos de seguridad
- 1.4.1. Seguridad de un sistema de información
  - 1.4.1.1. Integridad
  - 1.4.1.2. Confidencialidad
  - 1.4.1.3. Disponibilidad
  - 1.4.1.4. Autenticación
- 1.4.2. Servicios de seguridad
- 1.4.3. Protocolos de seguridad de la información. Tipología
- 1.4.4. Sensibilidad de un sistema de información

1.5. Seguridad en un sistema de información. Medidas y sistemas de control de acceso
- 1.5.1. Medidas de seguridad
- 1.5.2. Tipo de medidas de seguridad
  - 1.5.2.1. Prevención
  - 1.5.2.2. Detección
  - 1.5.2.3. Corrección
- 1.5.3. Sistemas de control de acceso. Tipología
- 1.5.4. Criptografía

1.6. Seguridad en redes e internet
- 1.6.1. *Firewalls*
- 1.6.2. Identificación digital
- 1.6.3. Virus y gusanos
- 1.6.4. *Hacking*
- 1.6.5. Ejemplos y casos reales

1.7. Delitos informáticos
- 1.7.1. Delito informático
- 1.7.2. Delitos informáticos. Tipología
- 1.7.3. Delito Informático. Ataque. Tipologías
- 1.7.4. El caso de la realidad virtual
- 1.7.5. Perfiles de delincuentes y víctimas. Tipificación del delito
- 1.7.6. Delitos informáticos. Ejemplos y casos reales

1.8. Plan de seguridad en un sistema de información
- 1.8.1. Plan de seguridad. Objetivos
- 1.8.2. Plan de seguridad. Planificación
- 1.8.3. Plan de riesgos. Análisis
- 1.8.4. Política de seguridad. Implementación en la organización
- 1.8.5. Plan de seguridad. Implementación en la organización
- 1.8.6. Procedimientos de seguridad. Tipos
- 1.8.7. Planes de seguridad. Ejemplos

1.9. Plan de contingencia
- 1.9.1. Plan de contingencia. Funciones
- 1.9.2. Plan de emergencia: elementos y objetivos
- 1.9.3. Plan de contingencia en la organización. Implementación
- 1.9.4. Planes de contingencia. Ejemplos

1.10. Gobierno de la seguridad de sistemas de información
- 1.10.1. Normativa legal
- 1.10.2. Estándares
- 1.10.3. Certificaciones
- 1.10.4. Tecnologías

Módulo 2. Seguridad en comunicaciones y operación software

2.1. Seguridad informática en comunicaciones y operación software
- 2.1.1. Seguridad informática
- 2.1.2. Ciberseguridad
- 2.1.3. Seguridad en la nube

2.2. Seguridad informática en comunicaciones y operación software. Tipología
- 2.2.1. Seguridad física
- 2.2.2. Seguridad lógica

2.3. Seguridad en comunicaciones
- 2.3.1. Principales elementos
- 2.3.2. Seguridad de redes
- 2.3.3. Mejores prácticas

2.4. Ciberinteligencia
- 2.4.1. Ingeniería social
- 2.4.2. *Deep web*
- 2.4.3. *Phishing*
- 2.4.4. *Malware*

2.5. Desarrollo seguro en comunicaciones y operación software
- 2.5.1. Desarrollo seguro. Protocolo HTTP
- 2.5.2. Desarrollo seguro. Ciclo de vida
- 2.5.3. Desarrollo seguro. Seguridad PHP
- 2.5.4. Desarrollo seguro. Seguridad NET
- 2.5.5. Desarrollo seguro. Mejores prácticas

2.6. Sistemas de gestión de la seguridad de la información en comunicaciones y operación software
- 2.6.1. GDPR
- 2.6.2. ISO 27021
- 2.6.3. ISO 27017/18

2.7. Tecnologías SIEM
- 2.7.1. Tecnologías SIEM
- 2.7.2. Operativa de SOC
- 2.7.3. SIEM *Vendors*

2.8. El rol de la seguridad en las organizaciones
- 2.8.1. Roles en las organizaciones
- 2.8.2. Rol de los especialistas IoT en las compañías
- 2.8.3. Certificaciones reconocidas en el mercado

2.9. Análisis forense
- 2.9.1. Análisis forense
- 2.9.2. Análisis forense. Metodología
- 2.9.3. Análisis forense. Herramientas e implantación

2.10. La ciberseguridad en la actualidad
- 2.10.1. Principales ataques informáticos
- 2.10.2. Previsiones de empleabilidad
- 2.10.3. Retos

Módulo 3. Seguridad en entornos *Cloud*

3.1. Seguridad en entornos *Cloud Computing*
- 3.1.1. Seguridad en entornos *Cloud Computing*
- 3.1.2. Seguridad en entornos *Cloud Computing.* Amenazas y riesgos seguridad
- 3.1.3. Seguridad en entornos *Cloud Computing.* Aspectos clave de seguridad

3.2. Tipos de infraestructura *Cloud*
- 3.2.1. Público
- 3.2.2. Privado
- 3.2.3. Híbrido

3.3. Modelo de gestión compartida
- 3.3.1. Elementos de seguridad gestionados por proveedor
- 3.3.2. Elementos gestionados por cliente
- 3.3.3. Definición de la estrategia para seguridad

3.4. Mecanismos de prevención
- 3.4.1. Sistemas de gestión de autenticación
- 3.4.2. Sistema de gestión de autorización: políticas de acceso
- 3.4.3. Sistemas de gestión de claves

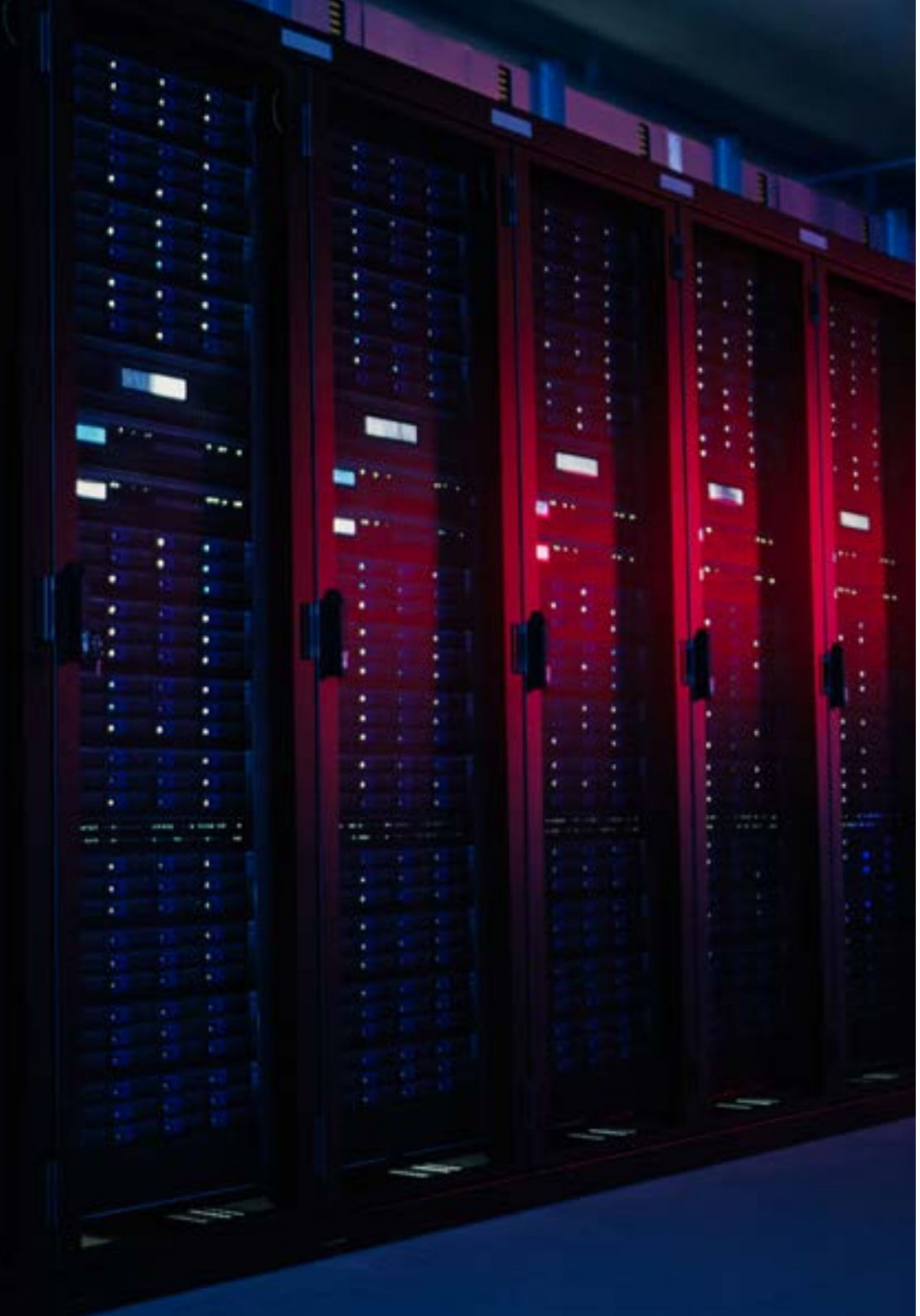
3.5. Securización de sistemas
- 3.5.1. Securización de los sistemas de almacenamiento
- 3.5.2. Protección de los sistemas de base de datos
- 3.5.3. Securización de datos en tránsito

3.6. Protección de infraestructura
- 3.6.1. Diseño e implementación de red segura
- 3.6.2. Seguridad en recursos de computación
- 3.6.3. Herramientas y recursos para protección de infraestructura

3.7. Detección de las amenazas y ataques
- 3.7.1. Sistemas de auditoría, *Logging* y monitorización
- 3.7.2. Sistemas de eventos y alarmas
- 3.7.3. Sistemas SIEM

3.8. Respuesta ante incidentes
- 3.8.1. Plan de respuesta a incidentes
- 3.8.2. La continuidad de negocio
- 3.8.3. Análisis forense y remediación de incidentes de la misma naturaleza





3.9. Seguridad en *Clouds* públicos
- 3.9.1. AWS (Amazon Web Services)
- 3.9.2. Microsoft Azure
- 3.9.3. Google GCP
- 3.9.4. Oracle Cloud

3.10. Normativa y cumplimiento
- 3.10.1. Cumplimiento de normativas de seguridad
- 3.10.2. Gestión de riesgos
- 3.10.3. Personas y proceso en las organizaciones

El temario más completo y actualizado del mercado está ahora a tu alcance. Matricúlate, no te arrepentirás"

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.

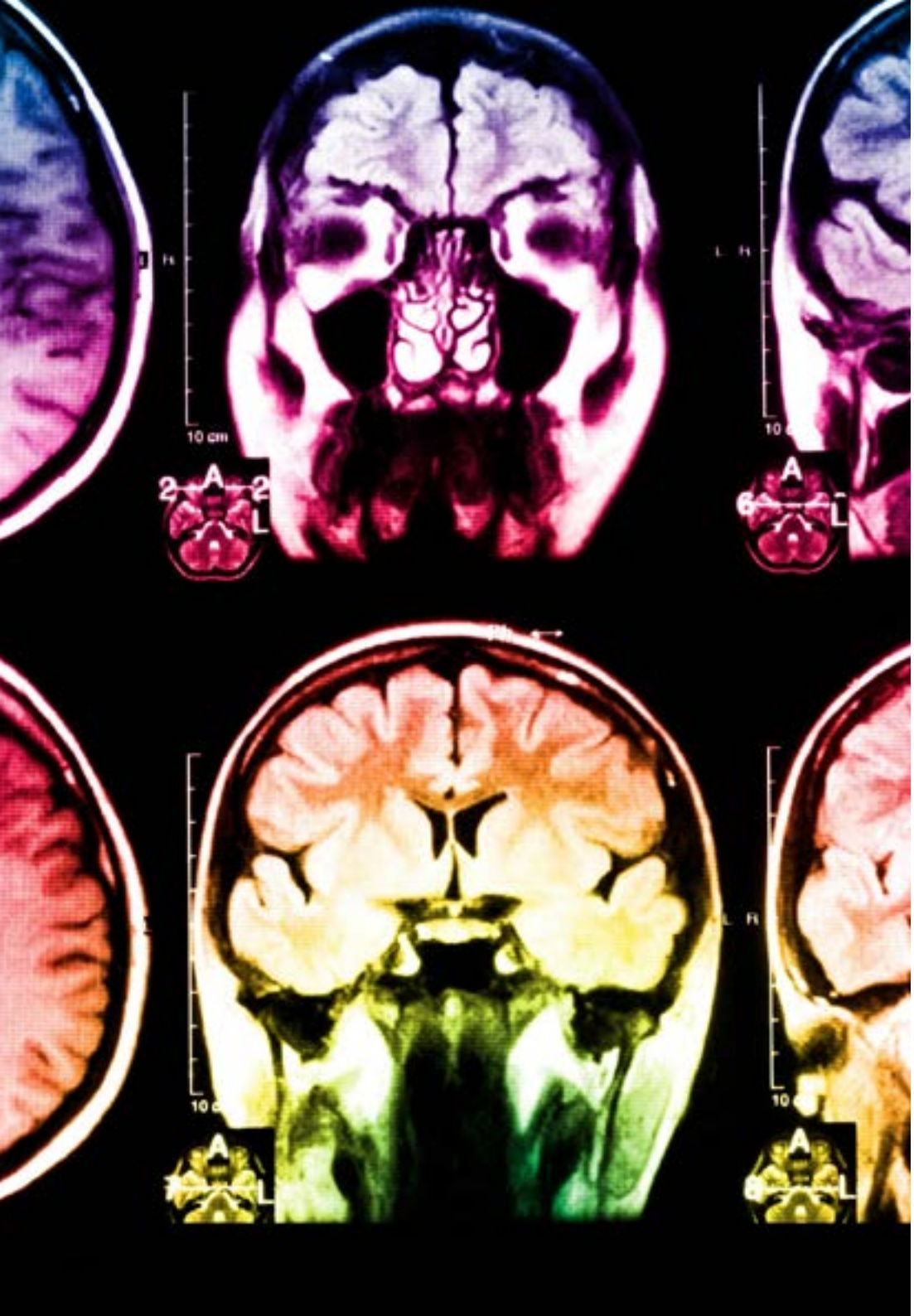
Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el Relearning.

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.

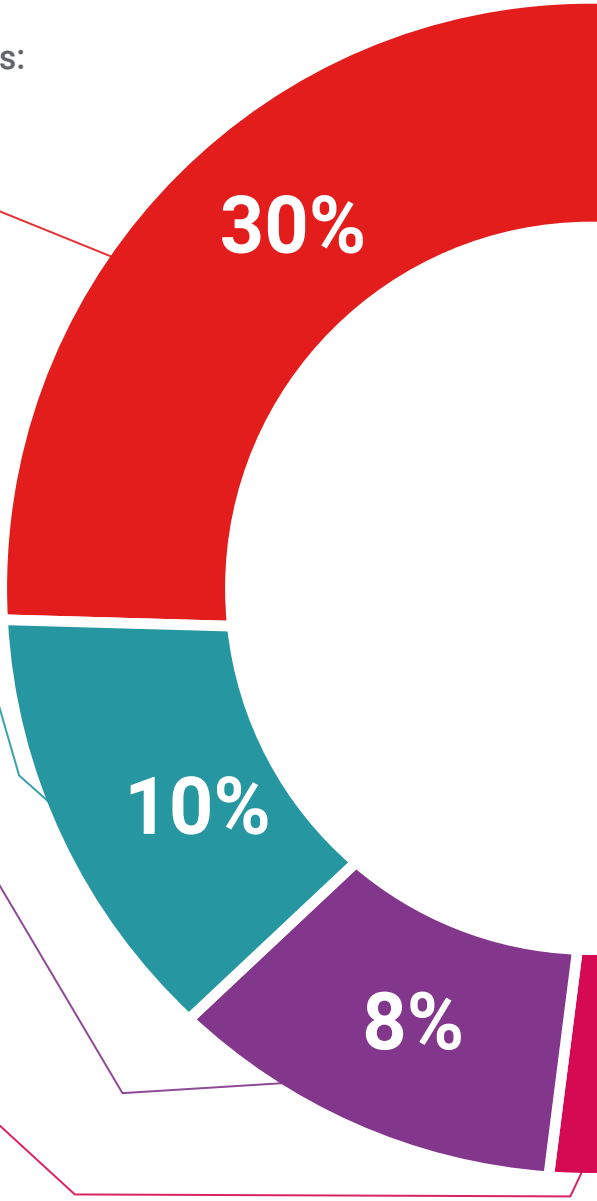
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

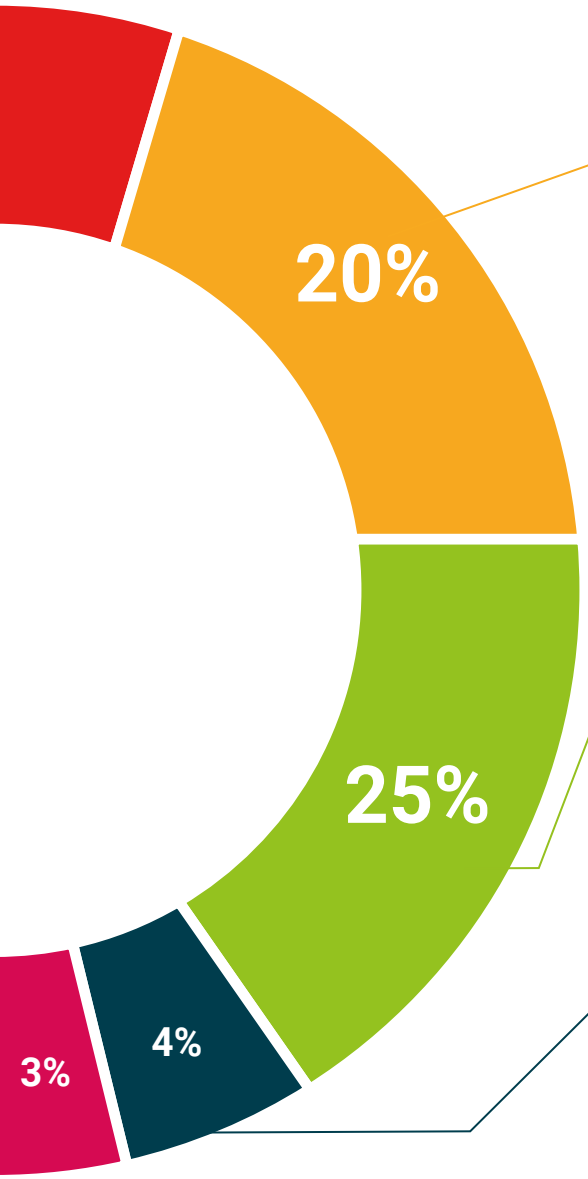
Prácticas de habilidades y competencias

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 Seguridad IT 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 Seguridad IT** 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 **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 Seguridad IT**

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

Seguridad IT

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

Este título propio se deberá acompañar siempre del título universitario habilitante expedido por la autoridad competente para ejercer profesionalmente en cada país. código único TECH: AFWOR23S techtitute.com/titulos

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



tech universidad tecnológica

Experto Universitario
Seguridad IT

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

Experto Universitario
Seguridad IT



tech universidad tecnológica