Experto Universitario

Ciberseguridad en Tecnologías Emergentes



tech universidad tecnológica



tech universidad tecnológica

Experto Universitario

Ciberseguridad en Tecnologías Emergentes

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

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

Recientemente han aparecido numerosas tecnologías que se han popularizado de forma rápida. Esto, además de haber proporcionado nuevos servicios a empresas, a usuarios y a clientes, también ha supuesto un problema de seguridad. Las tecnologías emergentes por su propia naturaleza están en continuo desarrollo y no ha alcanzado su estado óptimo de protección, por lo que son objeto de ataques. Para responder a ese reto se ha elaborado este programa, con el que el informático podrá conocer los mejores métodos de ciberseguridad aplicados al internet de las cosas, al *Cloud Computing* o al *Blockchain*. De esta manera, mejorará su perfil profesional, preparándose para afrontar los desafíos de seguridad digital del presente y del futuro.





Prepárate para especializarte en ciberseguridad aplicada al Cloud Computing, el Blockchain o el internet de las cosas con este Experto Universitario, que te convertirá en un profesional muy solicitado las mejores empresas tecnológicas"

Las tecnologías emergentes han llegado para quedarse. Han aparecido en un momento en el que se necesitaban soluciones a diversos problemas. Así, por ejemplo, el internet de las cosas está evolucionando hasta convertirse en un elemento esencial en la vida de muchas personas. Asimismo, el *Blockchain* está ayudando a descentralizar numerosos procesos y el *Cloud Computing* asegura la disponibilidad de recursos de todo tipo, especialmente datos o aplicaciones, en cualquier lugar, con el simple acceso a una conexión de red.

Al tratarse de elementos y servicios de gran utilidad, su popularidad está creciendo rápidamente, y eso produce una descompensación, puesto que, en muchas ocasiones, no disponen de una seguridad adecuada por ser tecnologías aún por desarrollar al 100%. Por eso, cada vez más empresas tanto del ámbito electrónico como de otras áreas, buscan profesionales especializados en ciberseguridad aplicada a estas herramientas.

Este Experto Universitario explora, por tanto, todas las posibilidades de ciberseguridad en este tipo de tecnologías, garantizando al informático una profundización intensiva y completa en este campo, dándole un impulso profesional decisivo en su carrera.

Todo ello, mediante un sistema de enseñanza online especialmente diseñado pensando en el profesional en activo, que podrá compaginar su trabajo con los estudios de forma cómoda y sencilla. Y, además, tendrá a su disposición al mejor cuadro docente compuesto por auténticos especialistas en este importante ámbito de la ciberseguridad.

Este **Experto Universitario en Ciberseguridad en Tecnologías Emergentes** 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 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
- 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

Empresas de todo tipo necesitan especialistas que aporten una seguridad óptima a sus proyectos de Blockchain o de internet de las cosas"

El mejor sistema de enseñanza online estará a tu disposición para que estudies a tu ritmo, sin rígidos horarios ni interrupciones en tu trabajo"

Podrás profundizar, gracias a este programa, en los mejores métodos criptográficos o en los tipos de infraestructura Cloud existentes.

Las tecnologías emergentes son el presente y el futuro: especialízate y mejora tus perspectivas profesionales de forma inmediata.

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

Este Experto Universitario en Ciberseguridad en Tecnologías Emergentes tiene como principal meta convertir al informático en un especialista de referencia en este ámbito, posicionándose como la solución perfecta para cualquier compañía que desee afrontar proyectos en *Blockchain* o *Cloud Computing* con total seguridad. Así, al completar este programa, tendrá un perfil profesional perfecto para la nueva coyuntura tecnológica y digital que lleva un tiempo imponiéndose.





Serás el profesional más solicitado de tu entorno cuando completes este Experto Universitario"

Objetivos generales

- Examinar la ciencia de la criptología y la relación con sus ramas: criptografía, criptoanálisis, esteganografía y estegoanálisis
- Analizar los tipos de criptografía según el tipo de algoritmo y según su uso
- Compilar los sistemas de gestión de claves
- Evaluar las distintas aplicaciones prácticas
- Examinar los certificados digitales
- Examinar la Infraestructura de Clave Pública (PKI)
- Analizar las últimas tendencias y retos
- 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
- Evaluar las opciones de conectividad IoT para afrontar un proyecto, con especial énfasis en tecnologías LPWAN
- Presentar las especificaciones básicas de las principales tecnologías LPWAN para el IoT
- Desarrollar las especificaciones de seguridad de cada tecnología LPWAN
- Analizar de forma comparativa la seguridad de las tecnologías LPWAN



Objetivos específicos

Módulo 1. Criptografía en IT

- Compilar las operaciones fundamentales (XOR, números grandes, sustitución y transposición) y los diversos componentes (funciones One-Way, Hash, generadores de números aleatorios)
- Analizar las técnicas criptográficas
- Desarrollar los diferentes algoritmos criptográficos
- Demostrar el uso de las firmas digitales y su aplicación en los certificados digitales
- Evaluar los sistemas de manejo de claves y la importancia de la longitud de las claves criptográficas
- Examinar los algoritmos derivación de claves
- Analizar el ciclo de vida de las claves
- Evaluar los modos de cifrado de bloque y de flujo
- Determinar los generadores de números pseudoaleatorios
- Desarrollar casos reales de aplicación de criptografía, como Kerberos, PGP o tarjetas inteligentes
- Examinar asociaciones y organismos relacionados, como ISO, NIST o NCSC
- Determinar los retos en la criptografía de la computación cuántica

Módulo 2. 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

Módulo 3. Seguridad en Comunicaciones de Dispositivos Iot

- Presentar la arquitectura simplificada del IoT
- Fundamentar las diferencias entre tecnologías de conectividad generalistas y tecnologías de conectividad para el IoT
- Establecer el concepto del triángulo de hierro de la conectividad del IoT
- Analizar las especificaciones de seguridad de la tecnología LoRaWAN, de la tecnología NB-IoT y de la tecnología WiSUN
- Fundamentar la elección de la tecnología IoT adecuada para cada proyecto

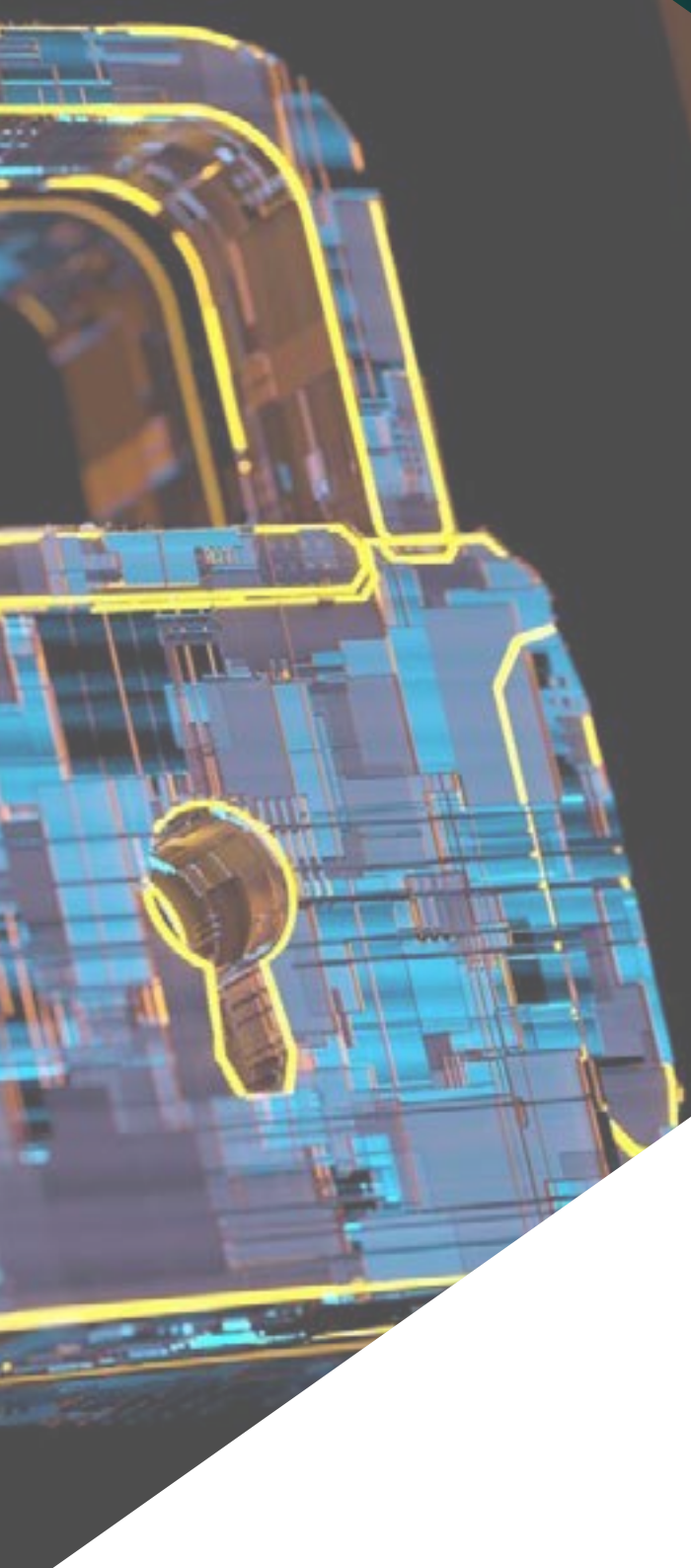
Todos tus objetivos profesionales estarán a tu alcance: matricúlate y conviértete en un especialista en Ciberseguridad en Tecnologías Emergentes”

03

Dirección del curso

La compleja coyuntura actual exige por parte del profesional una actualización y profundización constante. Las tecnologías emergentes no solo se están abriendo paso, sino que van transformándose de forma continua según surgen nuevos avances. Por eso, es necesario contar con los mejores especialistas en esta área, y este Experto Universitario cuenta con ellos, así que el informático podrá ponerse al día de todas las novedades a partir de la enseñanza de profesionales en activo.





El cuadro docente más experimentado, que trabaja en el sector de la ciberseguridad, te proporcionará los conocimientos y técnicas más avanzadas"

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. 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

D. del Valle Arias, Jorge

- Smart Cities Business Growth Manager Spain en Itron Inc.
- Consultor IoT
- Director de División IoT en Diode España
- Sales Manager IoT & Celular en Aicox Soluciones
- Fundador y CEO de Sensor Intelligence
- Director de Operaciones en Codium Networks
- Jefe del Área de Electrónica en Aitemin
- Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid
- Executive MBA por la International Graduate School de La Salle de Madrid

D. Ortega, Octavio

- Programador de Aplicaciones Informáticas y Desarrollo de Webs.
- Diseño de Webs y APPS para clientes, CRDS para Investigaciones realizadas por el Instituto de Salud Carlos III, tiendas online, aplicaciones para Android, etc
- Docente Seguridad Informática
- Licenciado en Psicología por la Universidad Oberta de Catalunya
- Técnico Superior Universitario en Análisis, Diseño y Soluciones del Software
- Técnico Superior Universitario en Programación Avanzada

Podrás responder de forma adecuada a todo tipo de amenazas de ciberseguridad. Matricúlate y conviértete en un gran especialista”

04

Estructura y contenido

Este Experto Universitario en Ciberseguridad en Tecnologías Emergentes está compuesto por 3 módulos especializados que se desarrollarán a lo largo de 450 horas de aprendizaje intensivo. Y, a partir de esa estructura, el informático podrá ahondar en aspectos relevantes de la ciberseguridad como los fundamentos matemáticos de la criptografía, el uso de algoritmos en seguridad, la seguridad en *Clouds* públicos y las principales vulnerabilidades de seguridad del IoT.





Los contenidos más completos en ciberseguridad aplicada a tecnologías emergentes están en este programa. No esperes más y matricúlate”

Módulo 1. Criptografía en IT

1.1. Criptografía
- 1.1.1. Criptografía
- 1.1.2. Fundamentos matemáticos

1.2. Criptología
- 1.2.1. Criptología
- 1.2.2. Criptoanálisis
- 1.2.3. Esteganografía y estegoanálisis

1.3. Protocolos criptográficos
- 1.3.1. Bloques básicos
- 1.3.2. Protocolos básicos
- 1.3.3. Protocolos intermedios
- 1.3.4. Protocolos avanzados
- 1.3.5. Protocolos exotéricos

1.4. Técnicas criptográficas
- 1.4.1. Longitud de claves
- 1.4.2. Manejo de claves
- 1.4.3. Tipos de algoritmos
- 1.4.4. Funciones resumen. Hash
- 1.4.5. Generadores de números pseudoaleatorios
- 1.4.6. Uso de algoritmos

1.5. Criptografía simétrica
- 1.5.1. Cifrados de bloque
- 1.5.2. DES (*Data Encryption Standard*)
- 1.5.3. Algoritmo RC4
- 1.5.4. AES (*Advanced Encryption Standard*)
- 1.5.5. Combinación de cifrados de bloques
- 1.5.6. Derivación de claves



1.6. Criptografía asimétrica
- 1.6.1. Diffie-Hellman
- 1.6.2. DSA (*Digital Signature Algorithm*)
- 1.6.3. RSA (*Rivest, Shamir y Adleman*)
- 1.6.4. Curva elíptica
- 1.6.5. Criptografía asimétrica. Tipología

1.7. Certificados digitales
- 1.7.1. Firma digital
- 1.7.2. Certificados X509
- 1.7.3. Infraestructura de clave pública (PKI)

1.8. Implementaciones
- 1.8.1. Kerberos
- 1.8.2. IBM CCA
- 1.8.3. *Pretty Good Privacy* (PGP)
- 1.8.4. ISO *Authentication Framework*
- 1.8.5. SSL y TLS
- 1.8.6. Tarjetas inteligentes en medios de pago (EMV)
- 1.8.7. Protocolos de telefonía móvil
- 1.8.8. *Blockchain*

1.9. Esteganografía
- 1.9.1. Esteganografía
- 1.9.2. Estegoanálisis
- 1.9.3. Aplicaciones y usos

1.10. Criptografía cuántica
- 1.10.1. Algoritmos cuánticos
- 1.10.2. Protección de algoritmos frente a computación cuántica
- 1.10.3. Distribución de claves cuántica

Módulo 2. Seguridad en entornos *Cloud*

2.1. Seguridad en entornos *Cloud Computing*
- 2.1.1. Seguridad en entornos *Cloud Computing*
- 2.1.2. Seguridad en entornos *Cloud Computing*. Amenazas y riesgos seguridad
- 2.1.3. Seguridad en entornos *Cloud Computing*. Aspectos clave de seguridad

2.2. Tipos de infraestructura *Cloud*
- 2.2.1. Público
- 2.2.2. Privado
- 2.2.3. Híbrido

2.3. Modelo de gestión compartida
- 2.3.1. Elementos de seguridad gestionados por proveedor
- 2.3.2. Elementos gestionados por cliente
- 2.3.3. Definición de la estrategia para seguridad

2.4. Mecanismos de prevención
- 2.4.1. Sistemas de gestión de autenticación
- 2.4.2. Sistema de gestión de autorización: políticas de acceso
- 2.4.3. Sistemas de gestión de claves

2.5. Securización de sistemas
- 2.5.1. Securización de los sistemas de almacenamiento
- 2.5.2. Protección de los sistemas de base de datos
- 2.5.3. Securización de datos en tránsito

2.6. Protección de infraestructura
- 2.6.1. Diseño e implementación de red segura
- 2.6.2. Seguridad en recursos de computación
- 2.6.3. Herramientas y recursos para protección de infraestructura

2.7. Detección de las amenazas y ataques
- 2.7.1. Sistemas de auditoría, *Logging* y monitorización
- 2.7.2. Sistemas de eventos y alarmas
- 2.7.3. Sistemas SIEM

2.8. Respuesta ante incidentes
- 2.8.1. Plan de respuesta a incidentes
- 2.8.2. La continuidad de negocio
- 2.8.3. Análisis forense y remediación de incidentes de la misma naturaleza

2.9. Seguridad en Clouds públicos
- 2.9.1. AWS (Amazon Web Services)
- 2.9.2. Microsoft Azure
- 2.9.3. Google GCP
- 2.9.4. Oracle Cloud

2.10. Normativa y cumplimiento
- 2.10.1. Cumplimiento de normativas de seguridad
- 2.10.2. Gestión de riesgos
- 2.10.3. Personas y proceso en las organizaciones

Módulo 3. Seguridad en comunicaciones de dispositivos IoT

3.1. De la telemetría al IoT
- 3.1.1. Telemetría
- 3.1.2. Conectividad M2M
- 3.1.3 Democratización de la telemetría

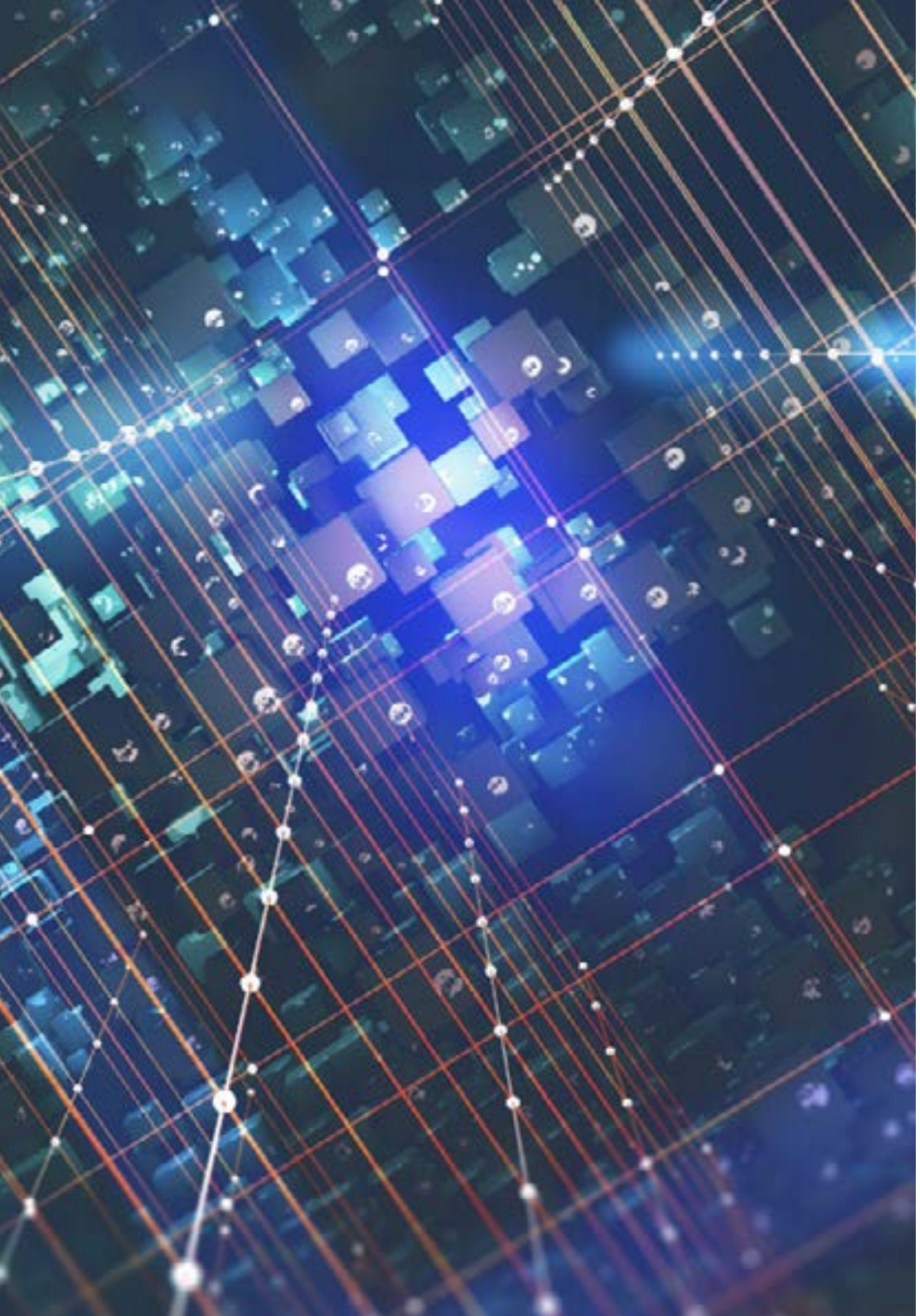
3.2. Modelos de referencia IoT
- 3.2.1. Modelo de referencia IoT
- 3.2.2. Arquitectura simplificada IoT

3.3. Vulnerabilidades de seguridad del IoT
- 3.3.1. Dispositivos IoT
- 3.3.2. Dispositivos IoT. Casuística de uso
- 3.3.3. Dispositivos IoT. Vulnerabilidades

3.4. Conectividad del IoT
- 3.4.1. Redes PAN, LAN, WAN
- 3.4.2. Tecnologías inalámbricas no IoT
- 3.4.3. Tecnologías inalámbricas LPWAN

3.5. Tecnologías LPWAN
- 3.5.1. El triángulo de hierro de las redes LPWAN
- 3.5.2. Bandas de frecuencia libres vs. Bandas licenciadas
- 3.5.3. Opciones de tecnologías LPWAN





3.6. Tecnología LoRaWAN
- 3.6.1. Tecnología LoRaWAN
- 3.6.2. Casos de uso LoRaWAN. Ecosistema
- 3.6.3. Seguridad en LoRaWAN

3.7. Tecnología Sigfox
- 3.7.1. Tecnología Sigfox
- 3.7.2. Casos de uso Sigfox. Ecosistema
- 3.7.3. Seguridad en Sigfox

3.8. Tecnología Celular IoT
- 3.8.1. Tecnología Celular IoT (NB-IoT y LTE-M)
- 3.8.2. Casos de uso Celular IoT. Ecosistema
- 3.8.3. Seguridad en Celular IoT

3.9. Tecnología WiSUN
- 3.9.1. Tecnología WiSUN
- 3.9.2. Casos de uso WiSUN. Ecosistema
- 3.9.3. Seguridad en WiSUN

3.10. Otras tecnologías IoT
- 3.10.1. Otras tecnologías IoT
- 3.10.2. Casos de uso y ecosistema de otras tecnologías IoT
- 3.10.3. Seguridad en otras tecnologías IoT

El mejor profesorado te pondrá al día de la seguridad en tecnologías emergentes a partir de los contenidos más novedosos”

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.

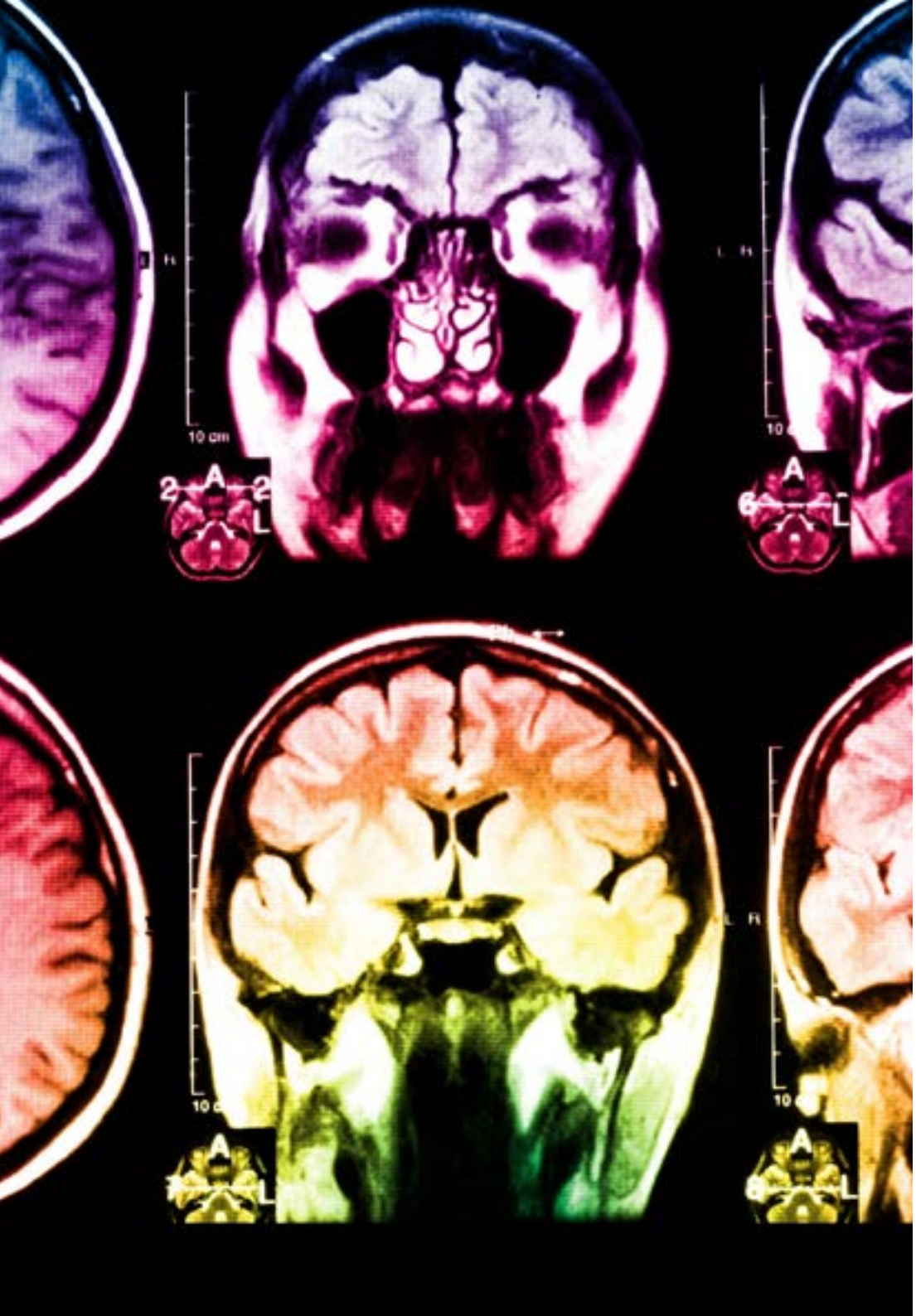
Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el Relearning.

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.

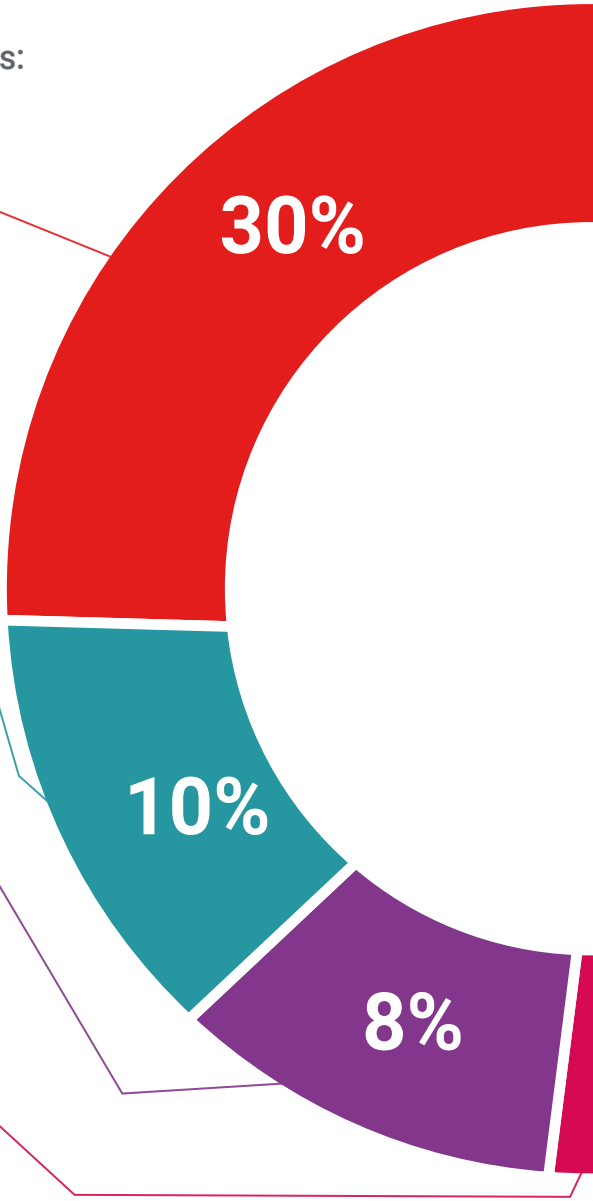
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

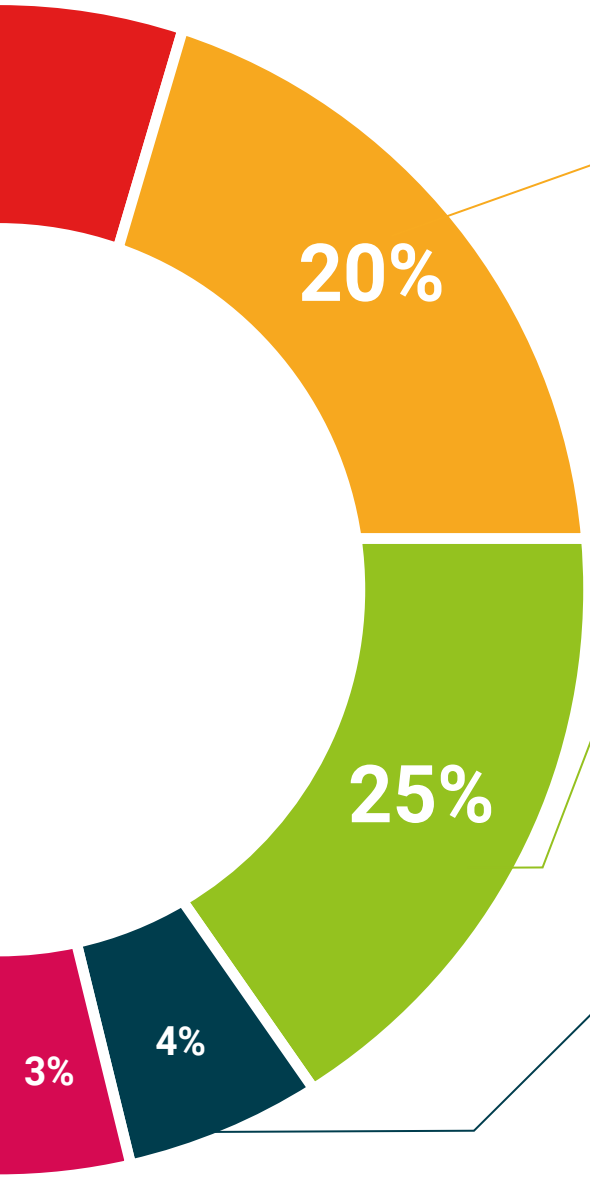
Prácticas de habilidades y competencias

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 Ciberseguridad en Tecnologías Emergentes 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 Ciberseguridad en Tecnologías Emergentes** 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 Ciberseguridad en Tecnologías Emergentes**

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

Ciberseguridad en Tecnologías Emergentes

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

Ciberseguridad en Tecnologías Emergentes

Modalidad: **Online**

Duración: **6 meses**

Titulación: **TECH Universidad Tecnológica**

Horas lectivas: **450 h.**

Experto Universitario

Ciberseguridad en Tecnologías Emergentes



tech universidad tecnológica