

Curso Universitario

Criptografía Avanzada



Curso Universitario Criptografía Avanzada

- » Modalidad: online
- » Duración: 6 semanas
- » Titulación: TECH Universidad Tecnológica
- » Acreditación: 6 ECTS
- » Dedicación: 16h/semana
- » Horario: a tu ritmo
- » Exámenes: online

Acceso web: www.techtitute.com/informatica/curso-universitario/criptografia-avanzada

Índice

01

Presentación

pág. 4

02

Objetivos

pág. 8

03

Dirección del curso

pág. 12

04

Estructura y contenido

pág. 16

05

Metodología

pág. 20

06

Titulación

pág. 28

01

Presentación

La criptografía ha aumentado su importancia en los últimos años. No sólo es una disciplina esencial en el cifrado de claves y datos, sino que es un elemento central en un nuevo campo tecnológico que está experimentando un gran auge: el *Blockchain*. Por eso, las compañías del ámbito digital y de desarrollo de aplicaciones y otras herramientas informáticas buscan especialistas con conocimientos avanzados en criptografía. Así, este programa le ofrece al profesional una completa profundización en esta área, preparándole para responder a los retos presentes y futuros de la ciberseguridad. Todo ello, a partir de una metodología de enseñanza online con la que podrá compaginar su trabajo y los estudios de forma cómoda y sencilla.



“

La criptografía es esencial para la ciberseguridad de empresas y para tecnologías como el Blockchain. Por eso, este programa te preparará de forma intensiva para progresar profesionalmente en este importante ámbito informático”

La creciente importancia que ha ido adquiriendo el ámbito de la ciberseguridad ha producido un enorme empuje en la criptografía. Esta disciplina permite codificar, cifrar y encriptar todo tipo de datos, ya sea información sensible de una compañía, transacciones o claves de acceso. Así, es fundamental en el mundo digital de hoy. Además, la aparición de otros ámbitos como el *Blockchain* o la inteligencia artificial le han dado un impulso extra, por lo que se trata de un sector con una gran demanda de profesionales especializados.

Este Curso Universitario en Criptografía Avanzada ofrece, por tanto, la posibilidad de ahondar en este ámbito, preparando al informático para responder a todos los retos presentes y futuros de esta área. A lo largo de este programa el profesional profundizará en cuestiones como la esteganografía y el estegoanálisis, la combinación de cifrados de bloques, la criptografía asimétrica o los algoritmos cuánticos.

A partir de una enseñanza 100% online, este Curso Universitario permitirá al informático avanzar profesionalmente gracias a sus contenidos actualizados y a su cuadro docente, compuesto por especialistas en criptografía que están al tanto de las últimas novedades en esta área y en sus nuevas aplicaciones prácticas.

Este **Curso Universitario en Criptografía Avanzada** contiene el programa educativo 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



Conoce las aplicaciones más novedosas de la criptografía gracias a este Curso Universitario, que se imparte mediante una metodología 100% online”

“ *Podrás profundizar en las mejores técnicas criptográficas a partir de numerosos recursos multimedia: actividades prácticas, resúmenes multimedia, clases magistrales, etc.*”

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

Las empresas tecnológicas necesitan expertos en Criptografía Avanzada y este Curso Universitario te preparará para mejorar profesionalmente.

El sistema de aprendizaje de TECH te permitirá continuar desarrollando tu labor profesional sin interrupciones y sin rígidos horarios.



02

Objetivos

Este Curso Universitario en Criptografía Avanzada tiene como principal objetivo transmitir al profesional los mejores métodos criptográficos, trasladándole, además, las nuevas aplicaciones de esta importante disciplina. Así, se convertirá en un informático especializado en criptografía que puede resolver diferentes problemáticas, ya sea en la seguridad de las claves de acceso a un determinado sistema o en tecnologías emergentes como el *Blockchain*. Con eso se preparará para trabajar en diferentes ámbitos, ampliando sus perspectivas laborales.



“

*Alcanza todos tus objetivos profesionales
especializándote en Criptografía Avanzada
gracias a este Curso Universitario”*

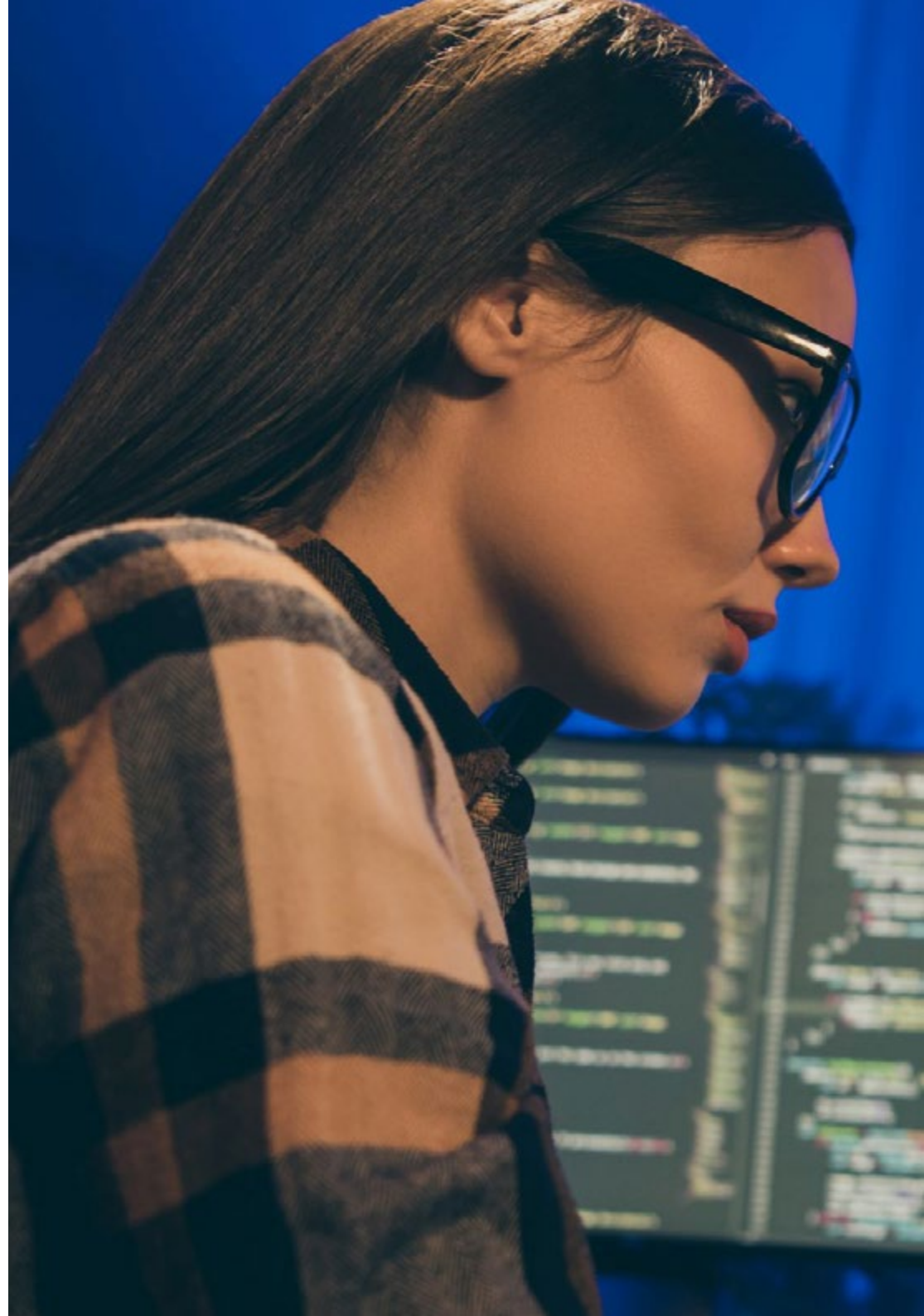


Objetivos generales

- ♦ 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

“

La criptografía será esencial en tu futuro profesional: matricúlate ya y prepárate para recibir importantes oportunidades en el área de la ciberseguridad”





Objetivos específicos

- ◆ 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

03

Dirección del curso

La criptografía es un área muy compleja para la que se quiere la mejor preparación. La aparición de nuevos sectores tecnológicos, para los que la criptografía es un elemento básico, ha propiciado un gran auge en este campo, y su enorme dificultad exige el acompañamiento de especialistas para conocer sus entresijos. Por eso, TECH ha reunido a un cuadro docente de gran prestigio que orientará al alumno a lo largo de todo el proceso de aprendizaje, garantizando que todos los elementos clave de la criptografía actual sean asimilados de forma ágil y sencilla.



“

El profesorado de TECH te orientará para que las 150 horas de aprendizaje de este Curso Universitario sean efectivas y te impulsen profesionalmente”

Dirección



D. Olalla Bonal, Martín

- ♦ Client Technical Specialist Blockchain en IBM
- ♦ Blockchain Technical Specialist en IBM SPGI
- ♦ 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. 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



“

Nuestro equipo docente te brindará todos sus conocimientos para que estés al día de la información más actualizada en la materia”

04

Estructura y contenido

El Curso Universitario en Criptografía Avanzada ha sido diseñado para responder a la demanda actual de especialistas en esta disciplina, y su módulo específico ayudará al profesional a ahondar en aspectos relevantes de la ciberseguridad como la criptografía asimétrica, los certificados digitales, los protocolos de telefonía móvil, la protección de algoritmos frente a la computación cuántica o la distribución cuántica de claves. Todo ello, a partir de 150 horas de aprendizaje repartidas a lo largo de 6 semanas.

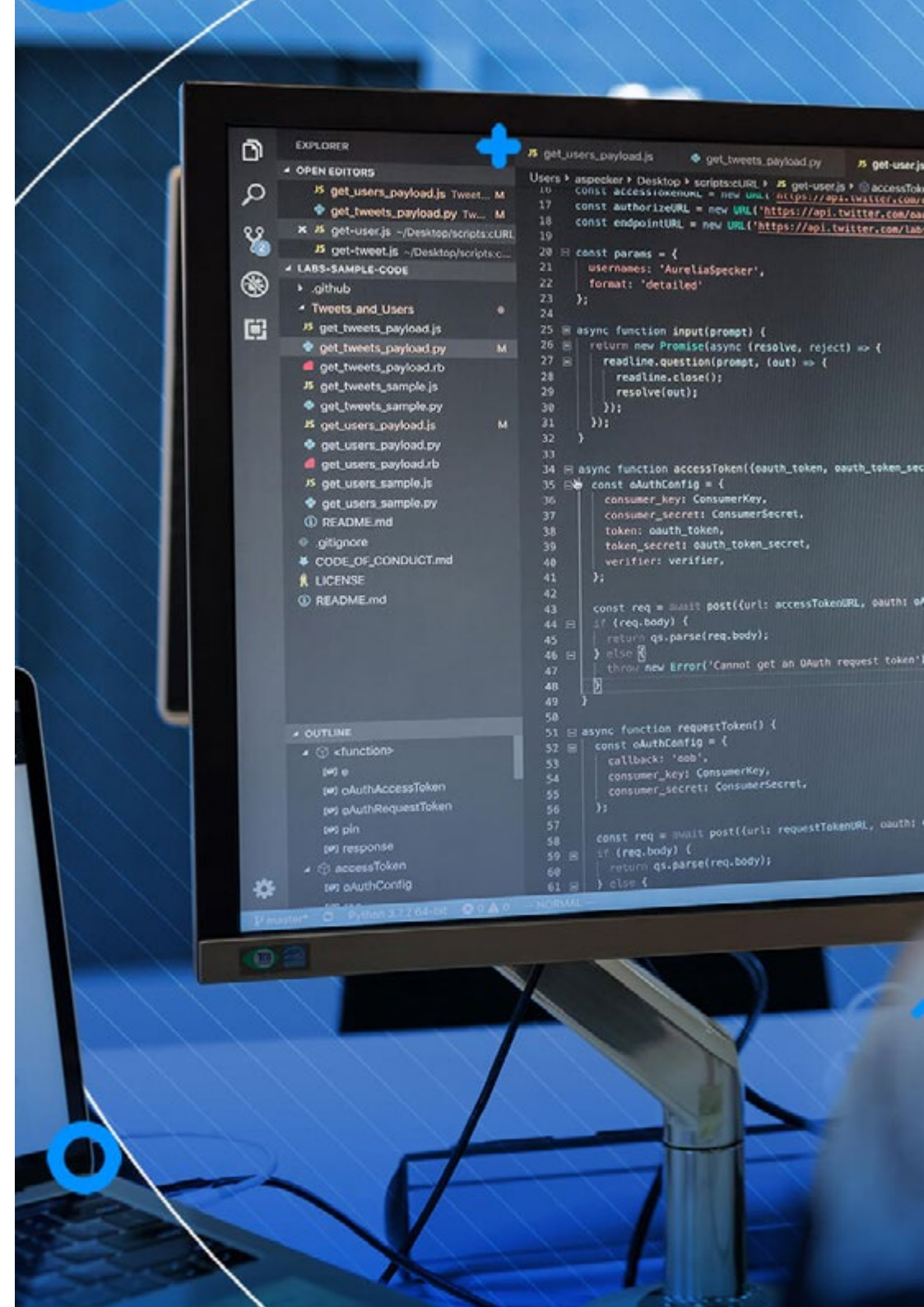


“

El temario más actualizado en Criptografía Avanzada te preparará para conocer todas las claves de la protección de algoritmos frente a la computación cuántica”

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 exóticos
- 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. Procesamiento de datos en tiempo real
 - 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

“

Este programa lo tiene todo: un profesorado de alto nivel, una metodología flexible que se adapta al profesional y los contenidos más completos en criptografía y ciberseguridad”

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 tomaran 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.



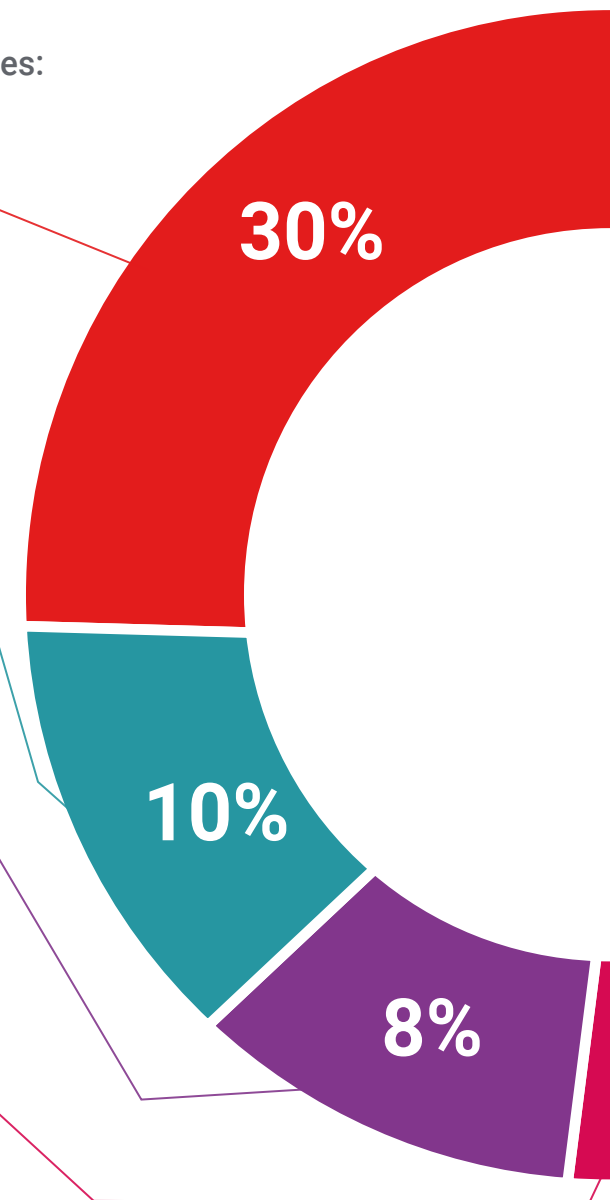
Prácticas de habilidades y competencias

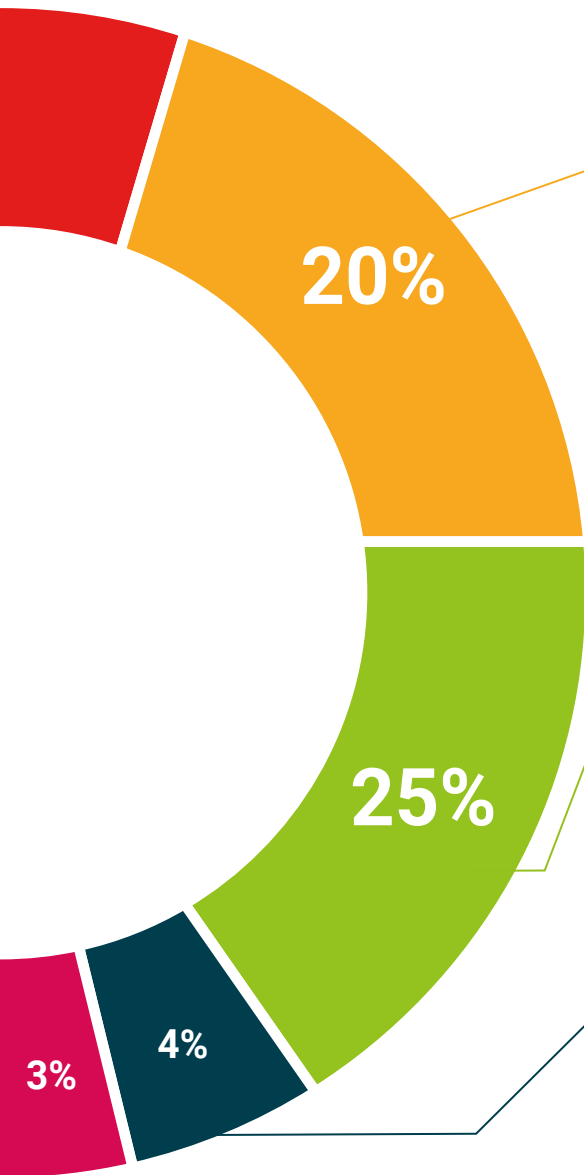
Realizarán actividades de desarrollo de competencias y habilidades específicas en cada área temática. Prácticas y dinámicas para adquirir y desarrollar las destrezas y habilidades que un especialista precisa desarrollar en el marco de la globalización que vivimos.



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 Curso Universitario en Criptografía Avanzada garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Curso Universitario expedido por TECH Universidad Tecnológica.



“

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

Este **Curso Universitario en Criptografía Avanzada** 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 **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 reunirá los requisitos comúnmente exigidos por las bolsas de trabajo, oposiciones y comités evaluadores de carreras profesionales.

Título: **Curso Universitario en Criptografía Avanzada**

ECTS: **6**

N.º Horas Oficiales: **150 h.**



*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.



Curso Universitario Criptografía Avanzada

- » Modalidad: online
- » Duración: 6 semanas
- » Titulación: TECH Universidad Tecnológica
- » Acreditación: 6 ECTS
- » Dedicación: 16h/semana
- » Horario: a tu ritmo
- » Exámenes: online

Curso Universitario

Criptografía Avanzada