Experto Universitario

Administración de la Seguridad en Tecnologías de la Información



tech universidad tecnológica



tech universidad tecnológica

Experto Universitario

Administración de la Seguridad en Tecnologías de la Información

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

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

La integración de las tecnologías de la información en numerosas empresas ha provocado un efecto colateral: han aumentado los riesgos de su seguridad informática. Ahora, las compañías necesitan estar atentas a diversos ataques y vulnerabilidades que pueden afectar a su correcto funcionamiento y a sus servicios. Por eso, es imprescindible disponer en la empresa de un especialista que se encargue de administrar la seguridad en torno a estas tecnologías. Este programa le ofrece al profesional la oportunidad de conocer los métodos de protección informática más avanzados en esta área, puesto que profundizará en aspectos como la evaluación de riesgos basados en parámetros de negocio, la gestión de identidades y accesos o los test de intrusión.





Cada vez más empresas necesitan especialistas en administración de seguridad aplicada a las tecnologías de la información. Este programa te permitirá progresar profesionalmente, profundizando en cuestiones como el plan de continuidad del negocio asociado a la seguridad"

Es un hecho: apenas quedan empresas que no empleen herramientas digitales e informáticas en sus procesos internos. Actividades y operaciones como la identificación de empleados, sistemas logísticos o el contacto con proveedores y clientes ahora se llevan a cabo, fundamentalmente, mediante tecnologías de la información. Pero estas tecnologías han de estar sujetas a un adecuado diseño y vigilancia, puesto que pueden ser explotadas para obtener datos o para vulnerar el acceso a aspectos delicados de la compañía.

Por esa razón, el especialista en Administración de seguridad es una figura cada vez más demandada, y no puede ser cubierta por cualquier informático. Se necesitan conocimientos muy actualizados que tengan en cuenta las últimas novedades en ciberseguridad. Así, este Experto Universitario ha sido diseñado para ofrecer al profesional los últimos avances en esta área, ahondando en cuestiones como las auditorías de seguridad, la seguridad de equipos terminales, o la respuesta más eficaz a diferentes incidentes.

Este programa, asimismo, se desarrolla en un formato 100% online que se adapta a las circunstancias del profesional, permitiéndole estudiar cuando, donde y como quiera. Contará, además, con un cuadro docente de gran prestigio en el ámbito de la ciberseguridad que se apoyará en numerosos recursos multimedia para que el proceso de aprendizaje sea cómodo, rápido y eficaz.

Este **Experto Universitario en Administración de la Seguridad en Tecnologías de la Información** 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

Este programa te permitirá profundizar en aspectos como el ciclo de vida de un plan de Continuidad de Negocio o la gestión de vulnerabilidades”

TECH pone a tu disposición los mejores recursos multimedia: estudios de caso, actividades teórico-prácticas, vídeos, resúmenes interactivos, etc. Todo para que el proceso de aprendizaje sea ágil y puedas aprovechar cada minuto invertido"

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

Estudia a tu ritmo, sin interrupciones ni rígidos horarios: el método de enseñanza de TECH es así de cómodo.

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

Teniendo en cuenta la creciente complejidad del ámbito de la ciberseguridad, este Experto Universitario en Administración de la Seguridad en Tecnologías de la Información tiene como principal meta acercar al profesional las novedades más importantes en este ámbito. De este modo, podrá convertirse en un gran especialista en la materia, pudiendo trabajar gestionando y dirigiendo el área de ciberseguridad de empresas de todo tipo de sectores.





TECH te ayuda a alcanzar tus objetivos gracias a este programa, con el que podrás optar a importantes puestos profesionales en las empresas más importantes a nivel nacional e internacional”

Objetivos generales

- Desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI)
- Identificar los elementos claves que conforman un SGSI
- Evaluar los diferentes modelos de arquitectura de seguridad para establecer el modelo más adecuado a la organización
- Identificar los marcos normativos de aplicación y las bases reguladoras de los mismos
- Analizar la estructura organizativa y funcional de un área de seguridad de la información (la oficina del CISO)
- Establecer un programa de auditorías que cubra las necesidades de autoevaluación de la organización en materia de ciberseguridad
- Desarrollar un programa de análisis y control de vulnerabilidades y un plan de respuesta a incidentes de ciberseguridad
- Determinar los elementos básicos de un Plan de Continuidad de Negocio (PCN) usando como base la guía de la ISO-22301
- Examinar los riesgos derivados de la no existencia de un Plan de Continuidad de Negocio (PCN)
- Analizar los criterios de éxito de un PCN y su integración dentro de una gestión de riesgos global de la compañía
- Concretar las fases de implantación de un Plan de Continuidad del Negocio



Objetivos específicos

Módulo 1. Arquitecturas y modelos de seguridad de la información

- Alinear el Plan Director de Seguridad con los objetivos estratégicos de la organización
- Establecer un marco continuo de gestión de riesgos como parte integral del Plan Director de Seguridad
- Determinar los indicadores adecuados para el seguimiento de la implantación del SGSI
- Establecer una estrategia de seguridad basada en políticas
- Analizar los objetivos y procedimientos asociados al plan de concienciación de empleados, proveedores y socios
- Identificar, dentro del marco normativo, las normativas, certificaciones y leyes de aplicación en cada organización
- Desarrollar los elementos fundamentales requeridos por la norma ISO 27001:2013
- Implantar un modelo de gestión de privacidad en línea con la regulación europea GDPR/ RGPD

Módulo 2. Gestión de la seguridad IT

- Identificar las diferentes estructuras que puede tener un área de seguridad de la información
- Desarrollar un modelo de seguridad basado en tres líneas de defensa
- Presentar los diferentes comités periódicos y extraordinarios en los que interviene el área de ciberseguridad
- Concretar las herramientas tecnológicas que dan soporte a las principales funciones del equipo de operaciones de seguridad (SOC)
- Evaluar las medidas de control de vulnerabilidades adecuadas a cada escenario
- Desarrollar el marco de trabajo de operaciones de seguridad basado en NIST CSF
- Concretar el alcance de los diferentes tipos de auditorías (*Red Team, Pentesting, Bug Bounty*, etc.)
- Proponer las actividades a realizar después de un incidente de seguridad
- Configurar un centro de mando de seguridad de la información que englobe a todos los actores relevantes (autoridades, clientes, proveedores, etc.)

Módulo 3. Plan de continuidad del negocio asociado a la seguridad

- Presentar los elementos clave de cada fase y Analizar las características del Plan de Continuidad de Negocio (PCN)
- Fundamentar la necesidad de un Plan de Continuidad para el Negocio
- Determinar los mapas de éxito y riesgo de cada fase del Plan de Continuidad de Negocio
- Concretar cómo se establece un Plan de Acción para la implantación
- Evaluar la completitud de un Plan de Continuidad del Negocio (PCN)
- Desarrollar el Plan de Implantación con éxito de un Plan de Continuidad para el Negocio

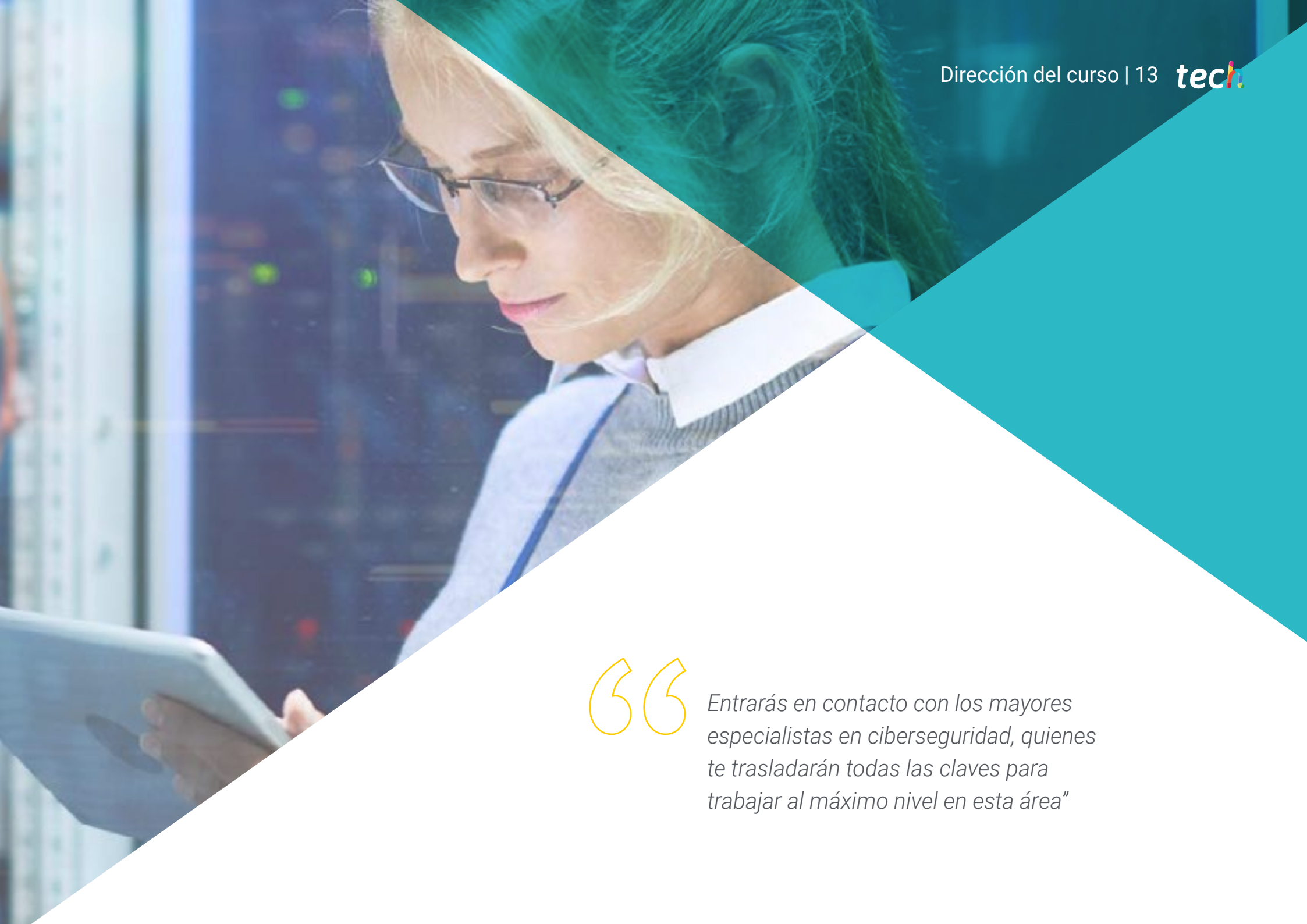
Serás el mayor especialista en seguridad aplicada a las tecnologías de información de tu entorno. No esperes más: matricúlate ya”

03

Dirección del curso

Tener a su disposición a los más grandes especialistas a nivel internacional en administración de la seguridad en el ámbito de las tecnologías de la información es una gran oportunidad para el profesional. Y justo eso es lo que ofrece este Experto Universitario, que dispone de un cuadro docente compuesto por prestigiosos ingenieros e informáticos que proporcionarán al alumno las técnicas y procedimientos más punteros para garantizar la adecuada seguridad interna de una empresa.





Entrarás en contacto con los mayores especialistas en ciberseguridad, quienes te trasladarán todas las claves para trabajar al máximo nivel en esta área”

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. Gozalo Fernández, Juan Luis

- Ingeniero Informático
- Profesor Asociado en DevOps y en Blockchain en UNIR
- Exdirector Blockchain DevOps en Alastria
- Director Desarrollo Aplicación Móvil Tinkerlink en Cronos Telecom
- Director Informática en Banco Santander
- Director Tecnología Gestión de Servicio IT en Barclays Bank España
- Licenciado en Ingeniería Superior Informática por la Universidad Nacional Educación a Distancia (UNED)

D. Embid Ruiz, Mario

- Abogado experto en Derecho TIC y protección de datos
- Responsable legal de Branddocs, SL, empresa tecnológica de soluciones de confianza
- Licenciatura en Derecho y Administración de Empresas por la Universidad Rey Juan Carlos
- Máster en Derecho de las Nuevas Tecnologías, Internet y Audiovisual por el Centro de Estudios Universitarios Villanueva y Cremades & Calvo Sotelo

D. Rodrigo Estébanez, Juan Manuel

- Fundador de ISMET TECH S.L
- Grado en Ingeniería por la Universidad de Valladolid
- Master Sistemas de Gestión Integrados por CFE-CEU
- ISO 27001 Lead Auditor (IMQ)
- ISO 27001 Lead Implementor (IMQ)
- NATO Standards HPS (OTAN)

04

Estructura y contenido

El temario de este Experto Universitario en Administración de la Seguridad en Tecnologías de la Información ha sido estructurado en 3 módulos que se desarrollarán a lo largo de 450 horas de aprendizaje. En ese periodo, el profesional ahondará en aspectos relevantes de este sector como los análisis forenses, los modelos de seguridad de la información, el marco normativo aplicable en esta área o la configuración de reglas de seguridad de red, entre muchas otras cuestiones.





Tendrás a tu disposición el temario más completo, presentado a través de unos recursos didácticos a los que podrás acceder las 24 horas del día"

Módulo 1. Arquitecturas y modelos de seguridad de la información

1.1. Arquitectura de seguridad de la información
- 1.1.1. SGSI / PDS
- 1.1.2. Alineación estratégica
- 1.1.3. Gestión del riesgo
- 1.1.4. Medición del desempeño

1.2. Modelos de seguridad de la información
- 1.2.1. Basados en políticas de seguridad
- 1.2.2. Basados en herramientas de protección
- 1.2.3. Basados en equipos de trabajo

1.3. Modelo de seguridad. Componentes clave
- 1.3.1. Identificación de riesgos
- 1.3.2. Definición de controles
- 1.3.3. Evaluación continua de niveles de riesgo
- 1.3.4. Plan de concienciación de empleados, proveedores, socios, etc.

1.4. Proceso de gestión de riesgos
- 1.4.1. Identificación de activos
- 1.4.2. Identificación de amenazas
- 1.4.3. Evaluación de riesgos
- 1.4.4. Priorización de controles
- 1.4.5. Reevaluación y riesgo residual

1.5. Procesos de negocio y seguridad de la información
- 1.5.1. Procesos de negocio
- 1.5.2. Evaluación de riesgos basados en parámetros de negocio
- 1.5.3. Análisis de impacto al negocio
- 1.5.4. Las operaciones de negocio y la seguridad de la información

1.6. Proceso de mejora continua
- 1.6.1. El ciclo de Deming
  - 1.6.1.1. Planificar
  - 1.6.1.2. Hacer
  - 1.6.1.3. Verificar
  - 1.6.1.4. Actuar

1.7. Arquitecturas de seguridad
- 1.7.1. Selección y homogeneización de tecnologías
- 1.7.2. Gestión de identidades. Autenticación
- 1.7.3. Gestión de accesos. Autorización
- 1.7.4. Seguridad de infraestructura de red
- 1.7.5. Tecnologías y soluciones de cifrado
- 1.7.6. Seguridad de Equipos Terminales (EDR)

1.8. El marco normativo
- 1.8.1. Normativas sectoriales
- 1.8.2. Certificaciones
- 1.8.3. Legislaciones

1.9. La norma ISO 27001
- 1.9.1. Implementación
- 1.9.2. Certificación
- 1.9.3. Auditorías y tests de intrusión
- 1.9.4. Gestión continua del riesgo
- 1.9.5. Clasificación de la información

1.10. Legislación sobre privacidad. RGPD (GDPR)
- 1.10.1. Alcance del Reglamento General de Protección de Datos (RGPD)
- 1.10.2. Datos personales
- 1.10.3. Roles en el tratamiento de datos personales
- 1.10.4. Derechos ARCO
- 1.10.5. El DPO. Funciones

Módulo 2. Gestión de la seguridad IT

2.1. Gestión de la seguridad
- 2.1.1. Operaciones de seguridad
- 2.1.2. Aspecto legal y regulatorio
- 2.1.3. Habilitación del negocio
- 2.1.4. Gestión de riesgos
- 2.1.5. Gestión de identidades y accesos

2.2. Estructura del área de seguridad. La Oficina del CISO
- 2.2.1. Estructura organizativa. Posición del CISO en la estructura
- 2.2.2. Las líneas de defensa
- 2.2.3. Organigrama de la oficina del CISO
- 2.2.4. Gestión presupuestaria

2.3. Gobierno de seguridad
- 2.3.1. Comité de seguridad
- 2.3.2. Comité de seguimiento de riesgos
- 2.3.3. Comité de auditoría
- 2.3.4. Comité de crisis

2.4. Gobierno de seguridad. Funciones
- 2.4.1. Políticas y normas
- 2.4.2. Plan director de seguridad
- 2.4.3. Cuadros de mando
- 2.4.4. Concienciación y formación
- 2.4.5. Seguridad en la cadena de suministro

2.5. Operaciones de seguridad
- 2.5.1. Gestión de identidades y accesos
- 2.5.2. Configuración de reglas de seguridad de red. Firewalls
- 2.5.3. Gestión de plataformas IDS/IPS
- 2.5.4. Análisis de vulnerabilidades

2.6. Marco de trabajo de ciberseguridad. NIST CSF
- 2.6.1. Metodología NIST
  - 2.6.1.1. Identificar
  - 2.6.1.2. Proteger
  - 2.6.1.3. Detectar
  - 2.6.1.4. Responder
  - 2.6.1.5. Recuperar

2.7. Centro de Operaciones de Seguridad (SOC). Funciones
- 2.7.1. Protección. *Red Team, pentesting, threat intelligence*
- 2.7.2. Detección. SIEM, *user behavior analytics, fraud prevention*
- 2.7.3. Respuesta

2.8. Auditorías de seguridad
- 2.8.1. Test de intrusión
- 2.8.2. Ejercicios de *Red Team*
- 2.8.3. Auditorías de código fuente. Desarrollo seguro
- 2.8.4. Seguridad de componentes (*software supply chain*)
- 2.8.5. Análisis forense

2.9. Respuesta a incidentes
- 2.9.1. Preparación
- 2.9.2. Detección, análisis y notificación
- 2.9.3. Contención, erradicación y recuperación
- 2.9.4. Actividad post incidente
  - 2.9.4.1. Retención de evidencias
  - 2.9.4.2. Análisis forense
  - 2.9.4.3. Gestión de brechas
- 2.9.5. Guías oficiales de gestión de ciberincidentes

2.10. Gestión de vulnerabilidades
- 2.10.1. Análisis de vulnerabilidades
- 2.10.2. Valoración de vulnerabilidad
- 2.10.3. Bastionado de sistemas
- 2.10.4. Vulnerabilidades de día 0. *Zero-day*

Módulo 3. Plan de continuidad del negocio asociado a la seguridad

3.1. Plan de Continuidad de Negocio
- 3.1.1. Los planes de Continuidad de Negocio (PCN)
- 3.1.2. Plan de Continuidad de Negocio (PCN). Aspectos clave
- 3.1.3. Plan de Continuidad de Negocio (PCN) para la valoración de la empresa

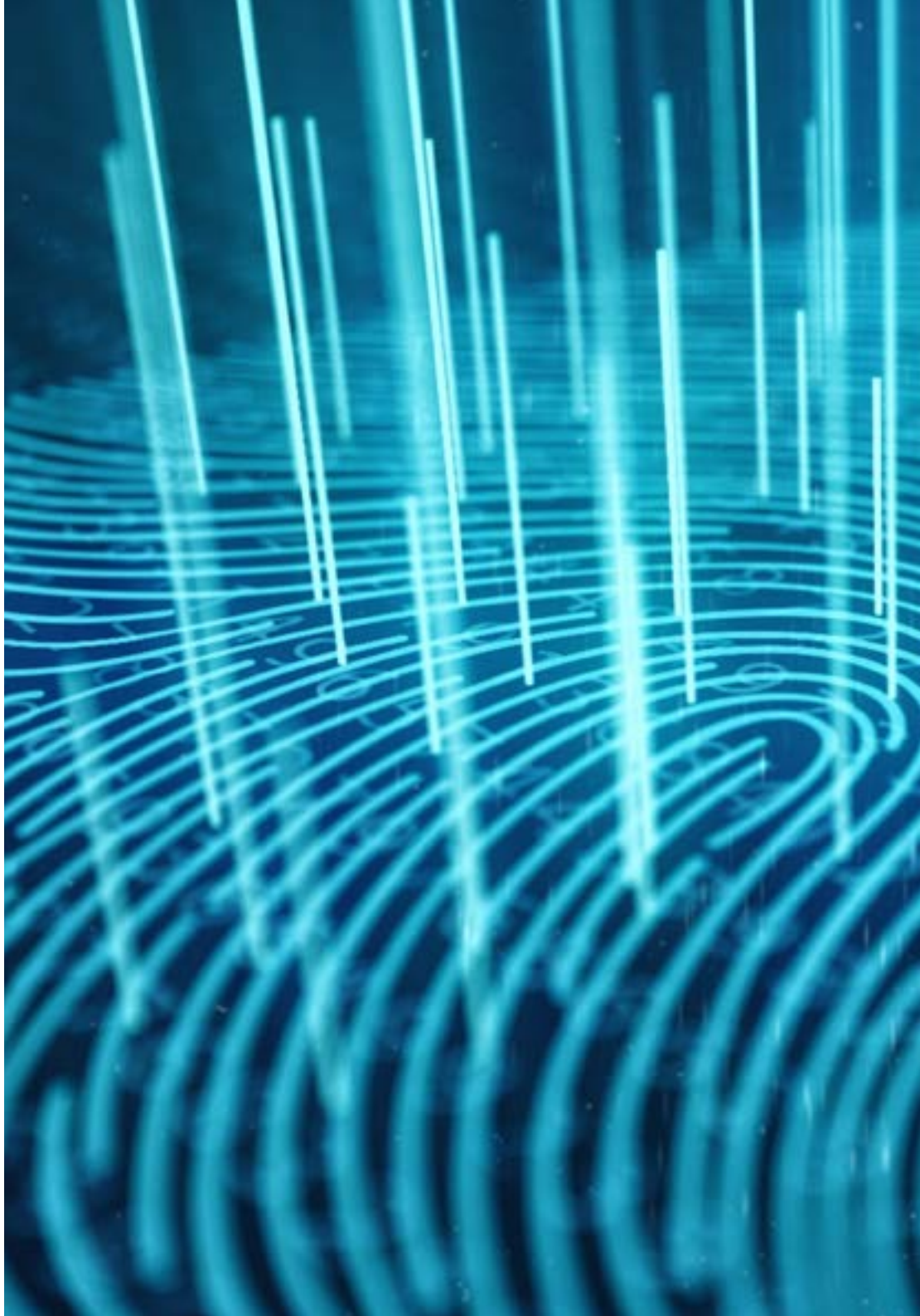
3.2. Métricas en un plan de Continuidad de Negocio (PCN)
- 3.2.1. *Recovery Time Objective* (RTO) y *Recovery Point Objective* (RPO)
- 3.2.2. Tiempo Máximo Tolerable (MTD)
- 3.2.3. Niveles Mínimos de Recuperación (ROL)
- 3.2.4. Punto de Recuperación Objetivo (RPO)

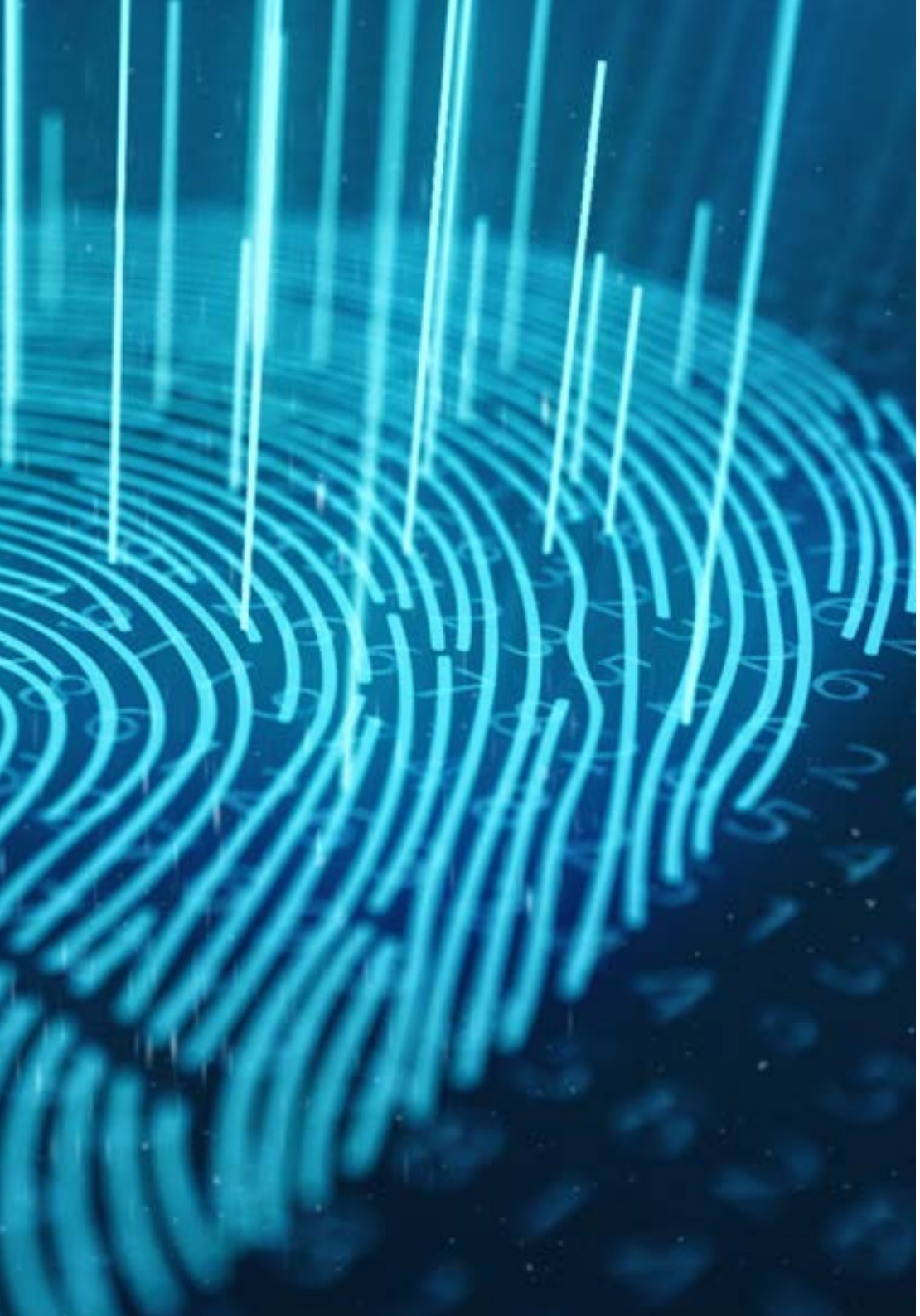
3.3. Proyectos de continuidad. Tipología
- 3.3.1. Plan de Continuidad de Negocio (PCN)
- 3.3.2. Plan de continuidad de TIC (PCTIC)
- 3.3.3. Plan de recuperación ante desastres (PRD)

3.4. Gestión de riesgos asociada al PCN
- 3.4.1. Análisis de impacto sobre el negocio
- 3.4.2. Beneficios de la implantación de un PCN
- 3.4.3. Mentalidad basada en riesgos

3.5. Ciclo de vida de un plan de Continuidad de Negocio
- 3.5.1. Fase 1: análisis de la organización
- 3.5.2. Fase 2: determinación de la estrategia de continuidad
- 3.5.3. Fase 3: respuesta a la contingencia
- 3.5.4. Fase 4: prueba, mantenimiento y revisión

3.6. Fase del análisis de la organización de un PCN
- 3.6.1. Identificación de procesos en el alcance del PCN
- 3.6.2. Identificación de áreas críticas del negocio
- 3.6.3. Identificación de dependencias entre áreas y procesos
- 3.6.4. Determinación del MTD adecuado
- 3.6.5. Entregables. Creación de un plan





3.7. Fase de determinación de la estrategia de continuidad en un PCN
  3.7.1. Roles en la fase de determinación de la estrategia
  3.7.2. Tareas de la fase de determinación de la estrategia
  3.7.3. Entregables
3.8. Fase de respuesta a la contingencia en un PCN
  3.8.1. Roles en la fase de respuesta
  3.8.2. Tareas en esta fase
  3.8.3. Entregables
3.9. Fase de pruebas, mantenimiento y revisión de un PCN
  3.9.1. Roles en la fase de pruebas, mantenimiento y revisión
  3.9.2. Tareas en la fase de pruebas, mantenimiento y revisión
  3.9.3. Entregables
3.10. Normas ISO asociadas a los planes de Continuidad de Negocio (PCN)
  3.10.1. ISO 22301:2019
  3.10.2. ISO 22313:2020
  3.10.3. Otras normas ISO e internacionales relacionadas

Este programa te permitirá ahondar en cuestiones como la identificación de dependencias entre áreas y procesos, aspecto fundamental para establecer una correcta 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 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.

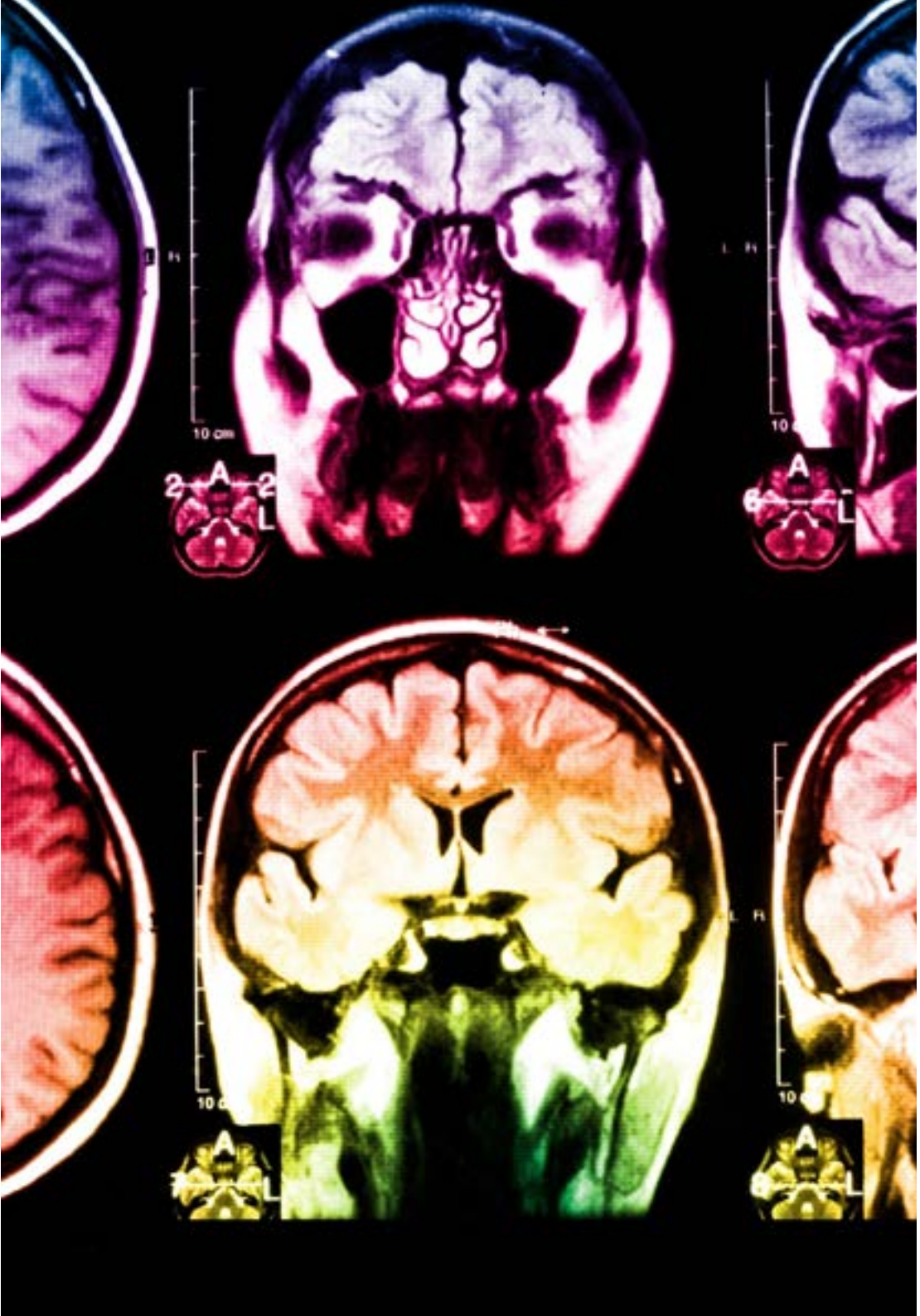
Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el Relearning.

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.

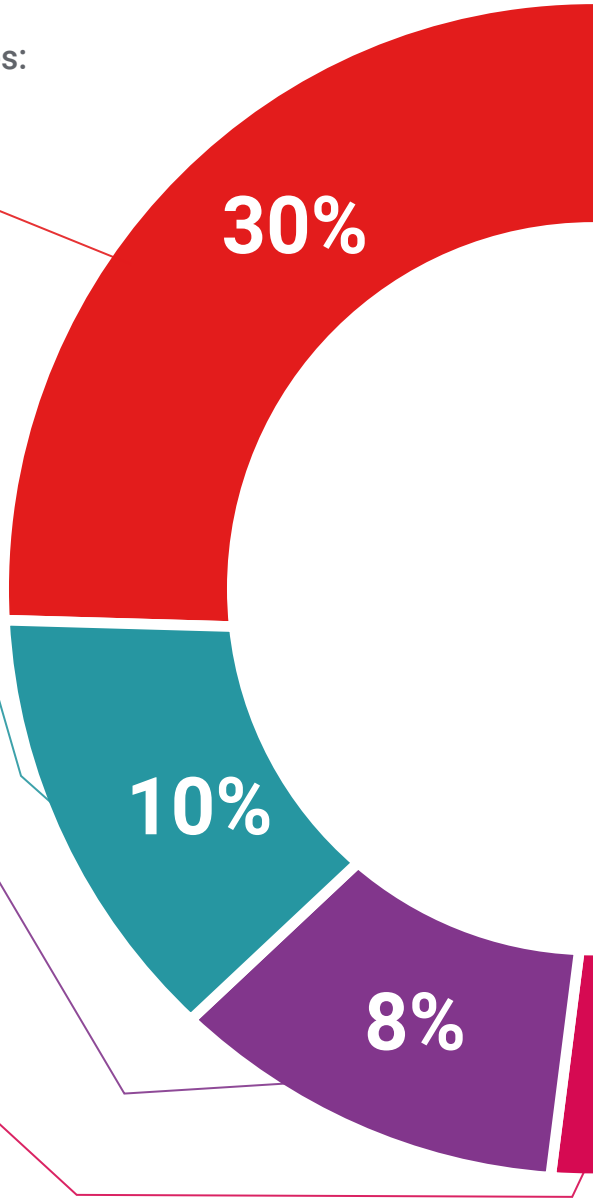
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

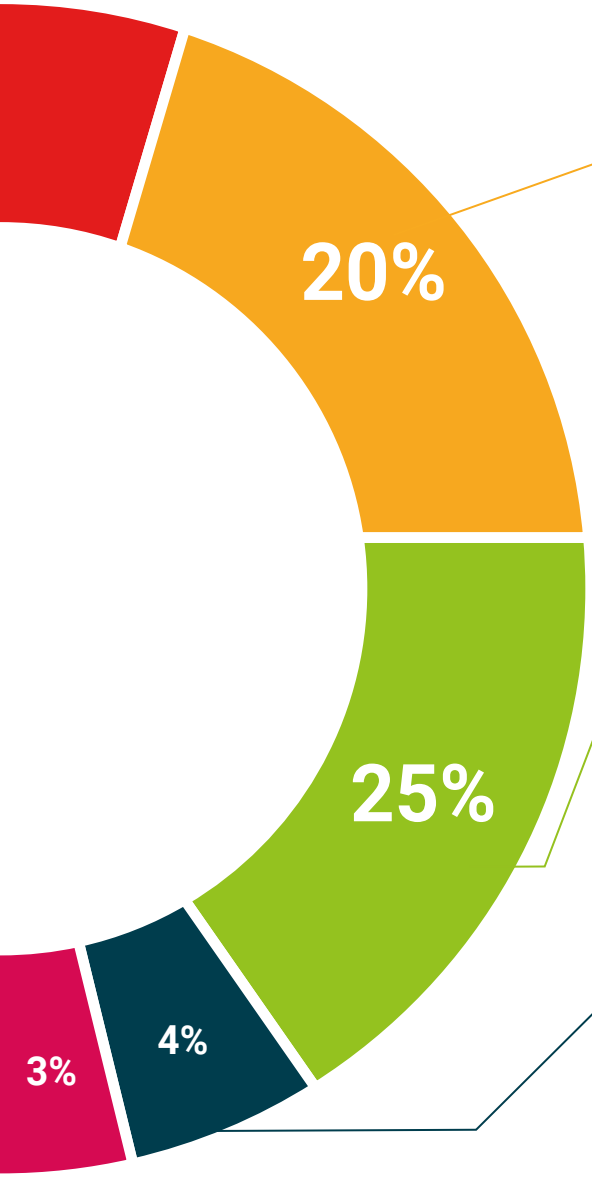
Prácticas de habilidades y competencias

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 Administración de la Seguridad en Tecnologías de la Información 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 Administración de la Seguridad en Tecnologías de la Información** 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 Administración de la Seguridad en Tecnologías de la Información**

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

Administración de la Seguridad en Tecnologías de la Información

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

Administración de la Seguridad en Tecnologías de la Información

Modalidad: **Online**

Duración: **6 meses**

Titulación: **TECH Universidad Tecnológica**

Horas lectivas: **450 h.**

Experto Universitario

Administración de la Seguridad en Tecnologías de la Información



tech universidad tecnológica