Experto Universitario
Gestión de Incidentes de Seguridad Informática

tech universidad tecnológica

tech universidad tecnológica

Experto Universitario

Gestión de Incidentes de Seguridad Informática

- Modalidad: **online**
- Duración: **6 meses**
- Titulación: **TECH Universidad Tecnológica**
- Acreditación: **18 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: www.techtitute.com/informatica/experto-universitario/experto-gestion-incidentes-seguridad-informatica

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 empresas saben que están expuestas a un gran número de ciberataques, es por ello, que la implementación de políticas de seguridad es, hoy en día, indispensable para garantizar la protección de datos sensibles. En este escenario, los profesionales de la informática deben dar respuesta a los previsibles incidentes que sufra la entidad y adoptar medidas preventivas para evitar nuevos ataques. Este programa 100% online proporciona al alumnado todas las herramientas necesarias para abordar la seguridad informática. El equipo docente experto en este campo y la amplia biblioteca con recursos multimedia favorecerán el aprendizaje y la especialización de los profesionales en un campo que requiere de una alta cualificación.

Estarás preparado para hacer frente a cualquier incidente de Seguridad Informática que sufra una empresa. Matricúlate en este Experto Universitario"

La seguridad informática se hace cada vez más necesaria dado el gran volumen de datos sensibles que poseen las empresas e instituciones. No obstante, en muchas ocasiones malas prácticas por parte del personal o el desconocimiento en este campo tecnológico hacen que se produzcan fisuras e incidentes. Estos en ocasiones pueden generar pérdidas o afectar gravemente a la imagen de una entidad.

Este Experto Universitario aporta una enseñanza especializada que permite analizar y gestionar incidentes, desde la detección de los mismos a través de sistemas IDS/IPS y su posterior tratamiento en SIEM, hasta el proceso de notificado y escalado al departamento correspondiente. Todo un proceso que requiere de profesionales informáticos expertos y conocedores de herramientas útiles para la monitorización de sistemas de información.

Este programa con un enfoque eminentemente práctico pondrá en situación al alumnado ante un ataque *Ransomware*, para que perfeccione sus conocimientos en la adopción de medidas de actuación y protocolos de recuperación.

La modalidad 100% online de este programa permite a los profesionales de la informática acceder sin horarios fijos y desde cualquier dispositivo con acceso a internet, a un contenido multimedia de calidad desde el primer día. TECH facilita así el aprendizaje del alumnado, que desee compatibilizar su vida laboral y personal con una enseñanza al alcance de todos.

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

- El desarrollo de casos prácticos presentados por expertos en Seguridad Informática
- Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que está concebido recogen una información técnica 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

Domina a la perfección con este Experto Universitario, los programas de monitorización de redes como Nagios, Zabbix o Pandora y mantén vigilados los equipos”

Da un salto en tu carrera profesional. Especialízate y aporta respuestas a los fallos de seguridad informática de las empresas e instituciones. Inscríbete ya"

Profundiza en la normativa ISO 27035 y evita fallos de seguridad que atenten contra las empresas. Matricúlate en esta titulación.

Maneja a la perfección los protocolos y herramientas SNM con este Experto Universitario.

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.

02

Objetivos

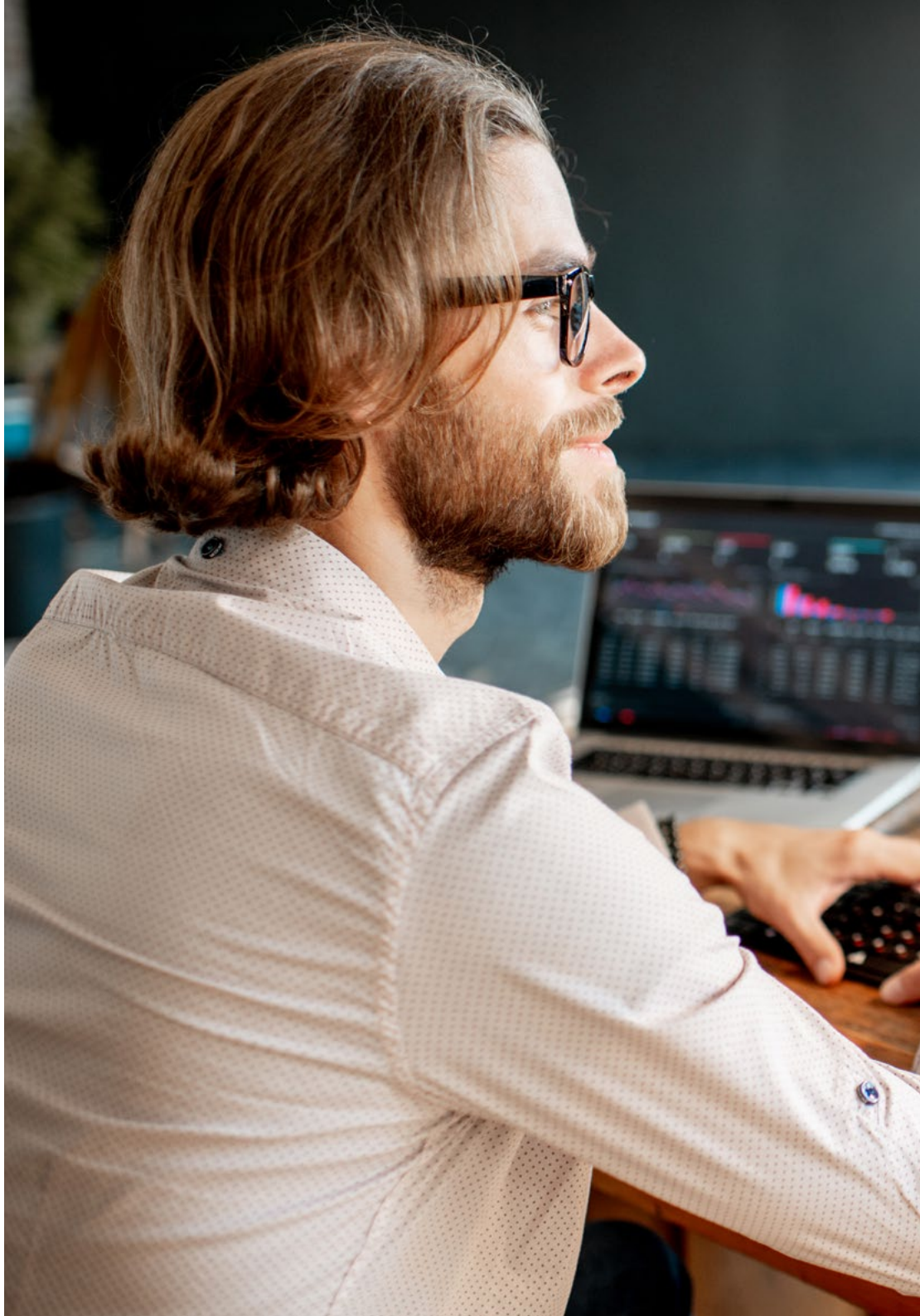
Durante los seis meses de duración de este Experto Universitario, los profesionales de la informática avanzarán en sus conocimientos en seguridad informática, que le llevarán durante el transcurso de la impartición de esta enseñanza a desarrollar medidas efectivas para garantizar las buenas prácticas en materia de seguridad en las empresas. Así serán capaces de realizar correctamente registros de auditoría en los sistemas y monitorizar las redes con las últimas herramientas tecnológicas. De esta forma, al finalizar el programa podrán poner en práctica un perfecto plan de políticas ante desastres de seguridad. Los videorresúmenes de cada tema y las lecturas complementarias facilitarán el alcance de dichas metas.

Desarrolla el mejor plan de seguridad informática y conviértete en el experto que las empresas necesitan para protegerse"

Objetivos generales

- Profundizar en los conceptos clave de la seguridad de la información
- Desarrollar las medidas necesarias para garantizar buenas prácticas en materia de seguridad de la información
- Desarrollar las diferentes metodologías para la realización de un análisis exhaustivo de amenazas
- Instalar y conocer las distintas herramientas utilizadas en el tratamiento y prevención de incidencias

La metodología pedagógica de TECH te permitirá alcanzar tus objetivos más ambiciosos incluso antes de lo que esperas"



Objetivos específicos

Módulo 1. Políticas de Gestión de Incidencias de Seguridad

- Desarrollar conocimiento especializado sobre cómo gestionar incidencias causadas por eventos de seguridad informática
- Determinar el funcionamiento de un equipo de tratamiento de incidencias en materia de seguridad
- Analizar las distintas fases de una gestión de eventos de seguridad informática
- Examinar los protocolos estandarizados para el tratamiento de incidencias de seguridad

Módulo 2. Herramientas de Monitorización en Políticas de Seguridad de los Sistemas de Información

- Desarrollar el concepto de monitorización e implementación de métricas
- Configurar los registros de auditoría en los sistemas y a monitorizar las redes
- Compilar las mejores herramientas de monitorización de sistemas existentes actualmente en el mercado

Módulo 3. Política de Recuperación práctica de Desastres de Seguridad

- Generar conocimiento especializado sobre el concepto de continuidad de la seguridad de la información
- Desarrollar un plan de continuidad de negocio
- Analizar un plan de continuidad TIC
- Diseñar un plan de recuperación de desastres

03

Dirección del curso

TECH proporciona al alumnado un aprendizaje de calidad y ajustado a las últimas novedades del sector, en este caso de la Seguridad Informática. En este Experto Universitario, el profesional de la informática accederá a un amplio conocimiento, gracias al saber de un equipo docente con amplia experiencia ciberseguridad y que actualmente se encuentra en activo en este campo. Por esta razón, el alumnado tendrá a su disposición una enseñanza que se aproxima a la realidad que viven los profesionales a diario ante ataques cibernéticos.

Expertos en seguridad en empresas públicas y privadas te darán las claves para que impulses tu carrera profesional en este campo”

Dirección

Dña. Fernández Sapena, Sonia

- Formadora de Seguridad Informática y Hacking Ético en el Centro de Referencia Nacional de Getafe en Informática y Telecomunicaciones de Madrid
- Instructora certificada E-Council
- Formadora en las siguientes certificaciones: EXIN Ethical Hacking Foundation y EXIN Cyber & IT Security Foundation. Madrid
- Formadora acreditada experta por la CAM de los siguientes certificados de profesionalidad: Seguridad Informática (IFCT0190), Gestión de Redes de Voz y datos (IFCM0310), Administración de Redes departamentales (IFCT0410), Gestión de Alarmas en redes de telecomunicaciones (IFCM0410), Operador de Redes de voz y datos (IFCM0110), y Administración de servicios de internet (IFCT0509)
- Colaboradora externa CSO/SSA (Chief Security Officer/Senior Security Architect) en la Universidad de las Islas Baleares
- Ingeniera en Informática por la Universidad de Alcalá de Henares de Madrid
- Máster en DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Profesores

D. Oropesiano Carrizosa, Francisco

- Ingeniero informático
- Técnico en Microinformática, Redes y Seguridad en Cas-Training
- Desarrollador de servicios web, CMS, e-Commerce, UI y UX en Fersa Reparaciones
- Gestor de servicios web, contenidos, correo y DNS en Oropesia Web & Network
- Diseñador gráfico y de aplicaciones web en Xarxa Sakai Projectes
- Diplomado en Informática de Sistemas por la Universidad de Alcalá de Henares
- Master en DevOps: Docker and Kubernetes por Cyber Business Center
- Técnico de Redes y Seguridad Informática por la Universidad de las Islas Baleares
- Experto en Diseño Gráfico por la Universidad Politécnica de Madrid

D. Ortega López, Florencio

- Consultor de seguridad (Gestión de Identidades) en SIA Group
- Consultor de TIC y Seguridad como profesional independiente
- Profesor formador en sector TI
- Graduado en Ingeniería Técnica Industrial por la Universidad de Alcalá de Henares
- Máster para el Profesorado por la UNIR
- MBA en Gestión y Dirección de Empresas por IDE-CESEM
- Máster en Dirección y Gestión de Tecnología de la Información por IDE-CESEM
- Certified Information Security Management (CISM) por la ISACA

04

Estructura y contenido

El plan de estudios de este Experto Universitario ha sido planificado para abordar en sus tres módulos los puntos clave para la gestión de incidentes de seguridad informática. De esta forma, el alumnado se adentrará en las políticas de gestión, los sistemas de detección y prevención de instrucciones, para profundizar a lo largo de este programa en las herramientas, protocolos y auditorías en materia de seguridad. Asimismo, la recuperación práctica de desastres de seguridad tendrá un papel importante en esta titulación. Los casos prácticos y el sistema *Relearning*, basado en la reiteración de contenidos, harán que el alumnado cimente de forma más sencilla y rápida, todo el conocimiento de esta titulación.

El amplio abanico de recursos multimedia enriquece este temario confeccionado por expertos en el campo de la seguridad informática"

Módulo 1. Políticas de Gestión de Incidencias de Seguridad

1.1. Políticas de gestión de incidencias de seguridad de la información y mejoras
- 1.1.1. Gestión de incidencias
- 1.1.2. Responsabilidades y procedimientos
- 1.1.3. Notificación de eventos

1.2. Sistemas de detección y prevención de intrusiones (IDS/IPS)
- 1.2.1. Datos de funcionamiento del sistema
- 1.2.2. Tipos de sistemas de detección de intrusos
- 1.2.3. Criterios para la ubicación de los IDS/IPS

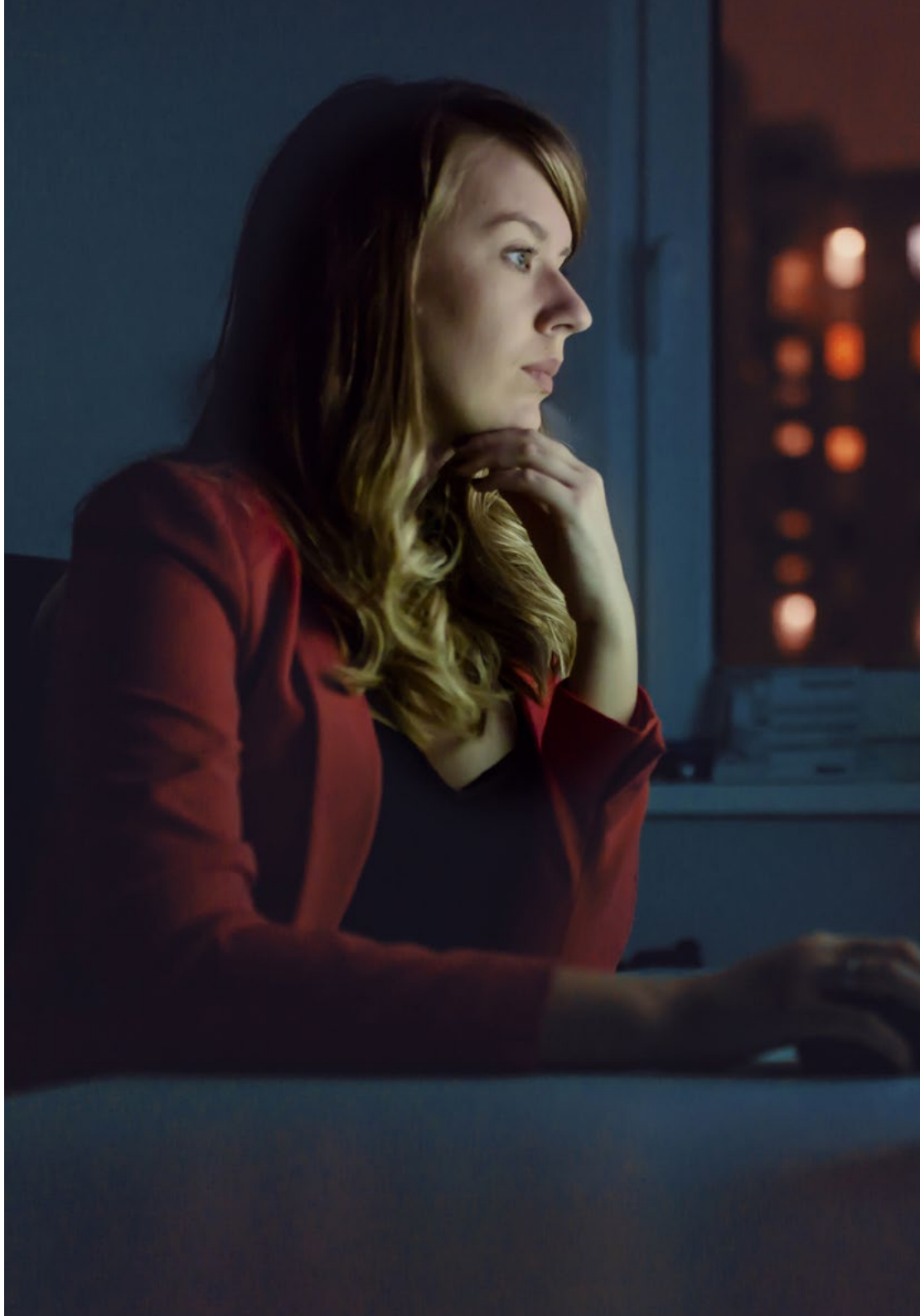
1.3. Respuesta ante incidentes de seguridad
- 1.3.1. Procedimiento de recolección de información
- 1.3.2. Proceso de verificación de intrusión
- 1.3.3. Organismos CERT

1.4. Proceso de notificación y gestión de intentos de intrusión
- 1.4.1. Responsabilidades en el proceso de notificación
- 1.4.2. Clasificación de los incidentes
- 1.4.3. Proceso de resolución y recuperación

1.5. Análisis forense como política de seguridad
- 1.5.1. Evidencias volátiles y no volátiles
- 1.5.2. Análisis y recogida de evidencias electrónicas
  - 1.5.2.1. Análisis de evidencias electrónicas
  - 1.5.2.2. Recogida de evidencias electrónicas

1.6. Herramientas de sistemas de detección y prevención de intrusiones (IDS/IPS)
- 1.6.1. Snort
- 1.6.2. Suricata
- 1.6.3. SolarWinds

1.7. Herramientas centralizadoras de eventos
- 1.7.1. SIM
- 1.7.2. SEM
- 1.7.3. SIEM



1.8. Guía de seguridad CCN-STIC 817
- 1.8.1. Gestión de ciberincidentes
- 1.8.2. Métricas e indicadores

1.9. NIST SP800-61
- 1.9.1. Capacidad de respuesta antes incidentes de seguridad informática
- 1.9.2. Manejo de un incidente
- 1.9.3. Coordinación e información compartida

1.10. Norma ISO 27035
- 1.10.1. Norma ISO 27035. Principios de la gestión de incidentes
- 1.10.2. Guías para la elaboración de un plan para la gestión de incidentes
- 1.10.3. Guías de operaciones en la respuesta a incidentes

Módulo 2. Herramientas de Monitorización en Políticas de Seguridad de los Sistemas de Información

2.1. Políticas de monitorización de sistemas de la información
- 2.1.1. Monitorización de sistemas
- 2.1.2. Métricas
- 2.1.3. Tipos de métricas

2.2. Auditoría y registro en sistemas
- 2.2.1. Auditoría y registro en sistemas
- 2.2.2. Auditoría y registro en Windows
- 2.2.3. Auditoría y registro en Linux

2.3. Protocolo SNMP. *Simple Network Management Protocol*
- 2.3.1. Protocolo SNMP
- 2.3.2. Funcionamiento de SNMP
- 2.3.3. Herramientas SNMP

2.4. Monitorización de redes
- 2.4.1. La monitorización de red en sistemas de control
- 2.4.2. Herramientas de monitorización para sistemas de control

2.5. Nagios. Sistema de monitorización de redes
- 2.5.1. Nagios
- 2.5.2. Funcionamiento de Nagios
- 2.5.3. Instalación de Nagios

2.6. Zabbix. Sistema de monitorización de redes
- 2.6.1. Zabbix
- 2.6.2. Funcionamiento de Zabbix
- 2.6.3. Instalación de Zabbix

2.7. Cacti. Sistema de monitorización de redes
- 2.7.1. Cacti
- 2.7.2. Funcionamiento de Cacti
- 2.7.3. Instalación de Cacti

2.8. Pandora. Sistema de monitorización de redes
- 2.8.1. Pandora
- 2.8.2. Funcionamiento de Pandora
- 2.8.3. Instalación de Pandora

2.9. SolarWinds. Sistema de monitorización de redes
- 2.9.1. SolarWinds
- 2.9.2. Funcionamiento de SolarWinds
- 2.9.3. Instalación de SolarWinds

2.10. Normativa sobre monitorización
- 2.10.1. Controles CIS sobre auditoria y registro
- 2.10.2. NIST 800-123 (EE. UU)

Módulo 3. Política de Recuperación práctica de Desastres de Seguridad

3.1. DRP. Plan de Recuperación de Desastres
- 3.1.1. Objetivo de un DRP
- 3.1.2. Beneficios de un DRP
- 3.1.3. Consecuencias de ausencia de un DRP y no actualizado

3.2. Guía para definir un DRP (Plan de Recuperación de Desastres)
- 3.2.1. Alcance y objetivos
- 3.2.2. Diseño de la estrategia de recuperación
- 3.2.3. Asignación de roles y responsabilidades
- 3.2.4. Realización de un Inventario de hardware, software y servicios
- 3.2.5. Tolerancia para tiempo de inactividad y pérdida de datos
- 3.2.6. Establecimiento de los tipos específicos de DRP's que se requieren
- 3.2.7. Realización de un plan de formación, concienciación y comunicación

3.3. Alcance y objetivos de un DRP (Plan de Recuperación de Desastres)
- 3.3.1. Garantía de respuesta
- 3.3.2. Componentes tecnológicos
- 3.3.3. Alcance de la política de continuidad

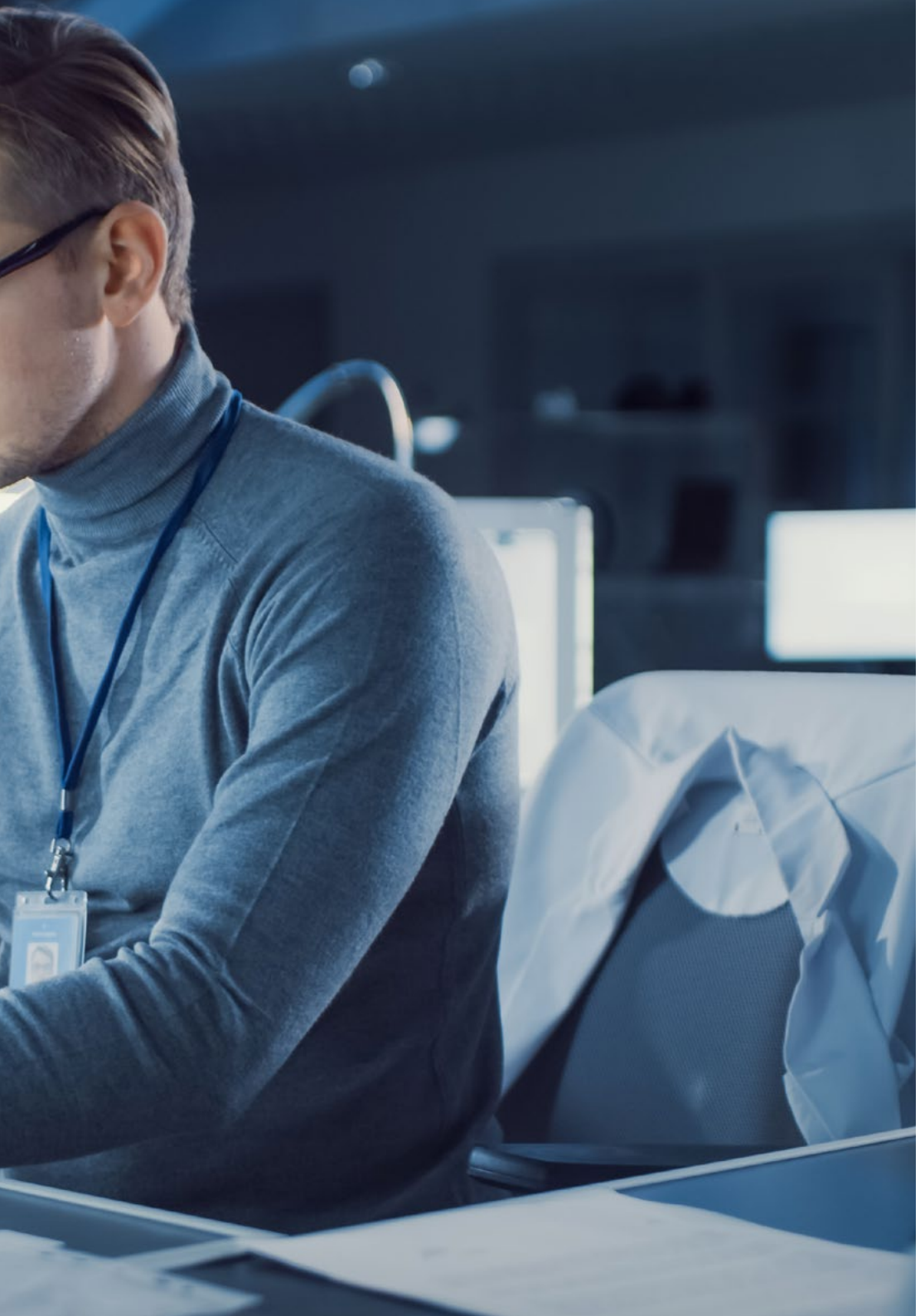
3.4. Diseño de la estrategia de un DRP (Plan de Recuperación de Desastre)
- 3.4.1. Estrategia de Recuperación de Desastre
- 3.4.2. Presupuesto
- 3.4.3. Recursos Humanos y Físicos
- 3.4.4. Posiciones gerenciales en riesgo
- 3.4.5. Tecnología
- 3.4.6. Datos

3.5. Continuidad de los procesos de la información
- 3.5.1. Planificación de la continuidad
- 3.5.2. Implantación de la continuidad
- 3.5.3. Verificación evaluación de la continuidad

3.6. Alcance de un BCP (Plan de Continuidad Empresarial)
- 3.6.1. Determinación de los procesos de mayor criticidad
- 3.6.2. Enfoque por activo
- 3.6.3. Enfoque por proceso

3.7. Implementación de los procesos garantizados de negocio
- 3.7.1. Actividades prioritarias (AP)
- 3.7.2. Tiempos de recuperación ideales (TRI)
- 3.7.3. Estrategias de supervivencia

3.8. Análisis de la organización
- 3.8.1. Obtención de información
- 3.8.2. Análisis de impacto sobre negocio (BIA)
- 3.8.3. Análisis de riesgos en la organización



3.9. Respuesta a la contingencia
- 3.9.1. Plan de crisis
- 3.9.2. Planes operativos de recuperación de entornos
- 3.9.3. Procedimientos técnicos de trabajo o de incidentes

3.10. Norma Internacional ISO 27031 BCP
- 3.10.1. Objetivos
- 3.10.2. Términos y definiciones
- 3.10.3. Operación

El sistema Relearning y la modalidad 100% online serán tus aliados para que logres un aprendizaje de gran utilidad en tu campo profesional"

06

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

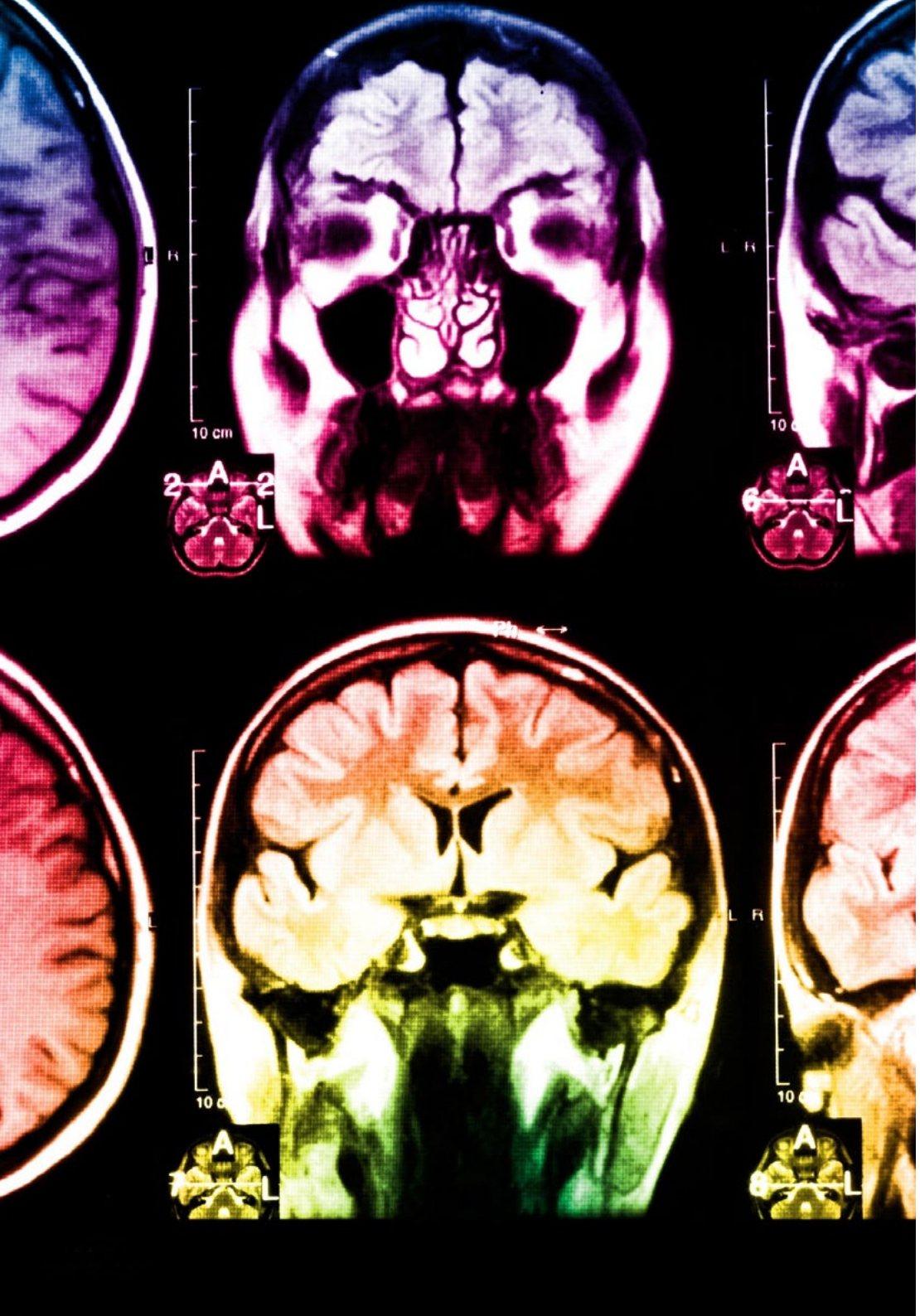
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

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.

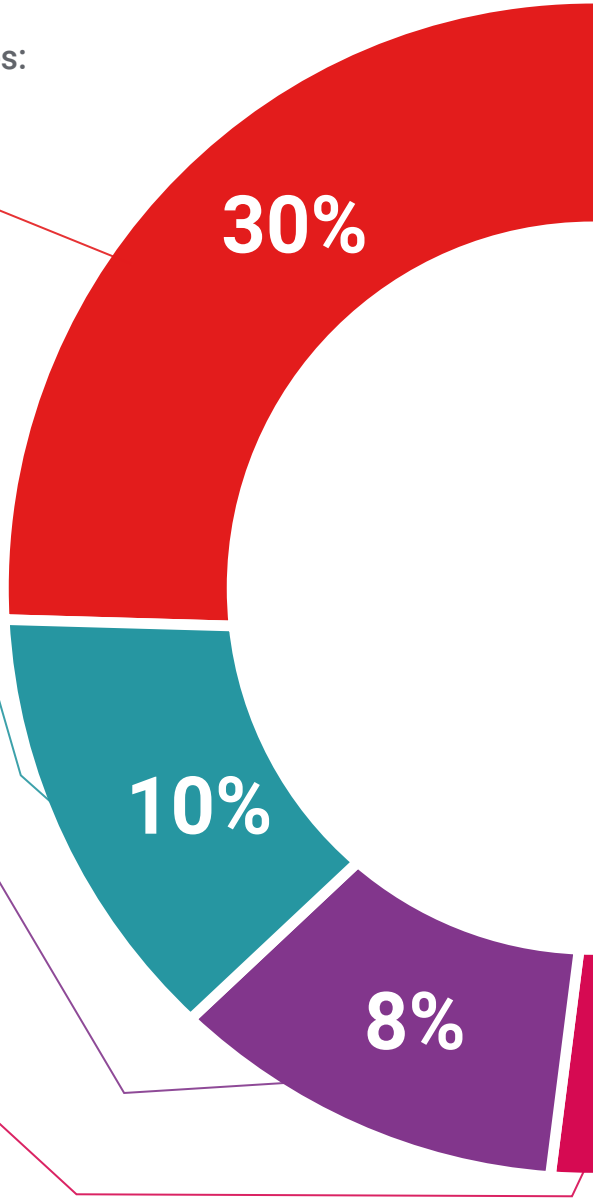
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

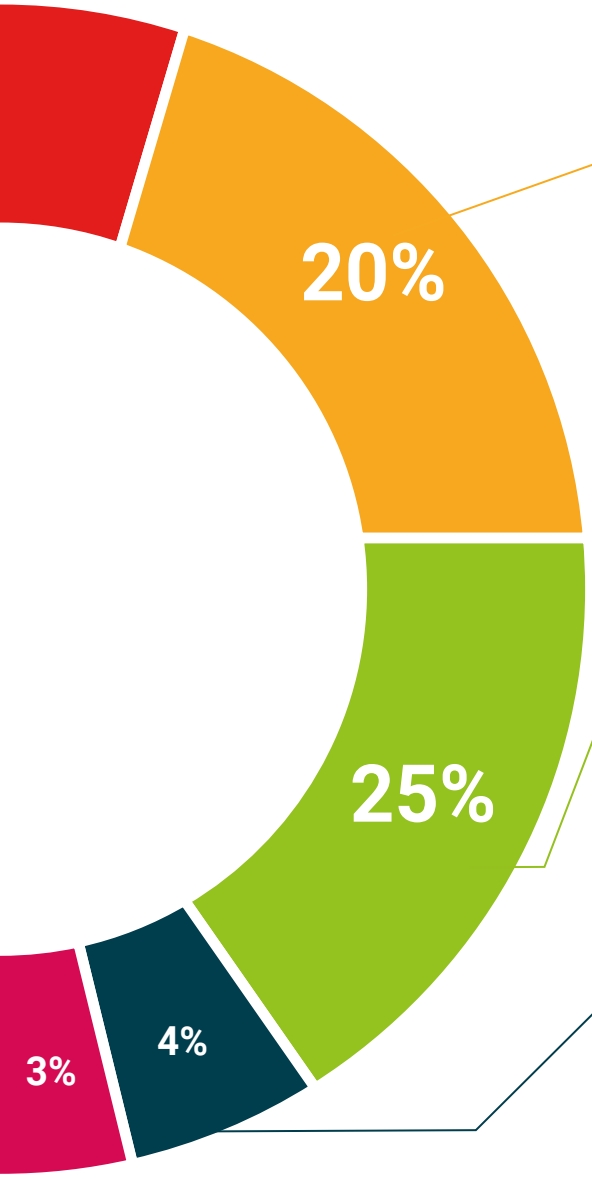
Prácticas de habilidades y competencias

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 Gestión de Incidentes de Seguridad Informática 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 Gestión de Incidentes de Seguridad Informática** 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 Gestión de Incidentes de Seguridad Informática**

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

Gestión de Incidentes de Seguridad Informática

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

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
Gestión de Incidentes de Seguridad Informática

- Modalidad: **online**
- Duración: **6 meses**
- Titulación: **TECH Universidad Tecnológica**
- Acreditación: **18 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Experto Universitario
Gestión de Incidentes de Seguridad Informática

tech universidad tecnológica