Experto Universitario

Implementación de Políticas de Seguridad Informática



tech universidad tecnológica



tech universidad tecnológica

Experto Universitario
Implementación de Políticas de Seguridad Informática

Modalidad: **Online**
Duración: **6 meses**
Titulación: **TECH Universidad Tecnológica**
Horas lectivas: **450 h.**
Acceso web: **www.techtitute.com/informatica/experto-universitario/experto-implementacion-politicas-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 ponen su foco en la seguridad de los equipos informáticos y de la nube para evitar el robo o pérdida de datos de gran valor, sin embargo, descuidan otros aspectos de seguridad igual de importantes en una empresa como, por ejemplo, es la protección del equipo físico y ambiental. En esta enseñanza 100% online, los profesionales de la informática profundizarán en el bastionado de sistemas con la implementación de métodos de seguridad avanzados para mantener un control de acceso y autorización a cada usuario. Todo ello, con un contenido de calidad basado en video resúmenes, lecturas específicas y casos prácticos que posibilitarán una especialización en un campo de la informática necesitado de profesionales con alta cualificación.





Profundiza en las principales tecnologías de identificación y autorización e implementa sistemas informáticos más seguros con este Experto Universitario"

Invertir en seguridad informática es esencial para las empresas e instituciones, sin embargo, muchas se orientan a los posibles ataques cibernéticos externos y se olvidan de desarrollar una política de seguridad física y ambiental correcta de control de acceso a los sistemas informáticos. En este Experto Universitario, el profesional de la informática profundizará en los principales aspectos a tener en cuenta para poner en práctica esta tarea, que no resulta nada fácil.

El programa, impartido por profesionales expertos en seguridad informática, se adentra en cómo chequear el estado de la seguridad de un sistema informático a través de los controles CIS, en analizar todos los sistemas biométricos de control de acceso que existen, su implementación y la gestión de riesgos. Además, aborda la implementación de criptografía en redes de comunicaciones con los protocolos actuales más utilizados, tanto simétricos como asimétricos.

Asimismo, la autenticación e identificación tendrán un espacio importante en esta titulación, donde los profesionales de la informática desarrollarán una PKI, conocerán su estructura y el uso de dicha infraestructura para proteger la red mediante el uso de Certificados Digitales.

Una excelente oportunidad que ofrece TECH para conseguir una especialización en un sector que requiere de profesionales con conocimientos actualizados y novedosos en el campo de la seguridad informática. El modelo de enseñanza 100% online permite compaginar el aprendizaje con otros ámbitos de la vida personal, ya que el alumnado tan solo necesitará de un dispositivo con conexión a internet para acceder a todo el contenido multimedia de calidad puesto a su alcance.

Este **Experto Universitario en Implementación de Políticas 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

Actualiza tus conocimientos en seguridad informática ante posibles incendios y terremotos. Inscríbete en este Experto Universitario"

Conoce las últimas novedades en huella dactilar, reconocimiento facial, de iris y retina como medidas de seguridad informática"

Profundiza en los protocolos seguros de comunicación y evita el robo de datos de gran valor. Matricúlate ahora.

Domina a la perfección la herramienta Secure Shell y evita filtraciones de información de las empresas.

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

Al concluir este Experto Universitario, los profesionales de la informática serán capaz de implementar políticas de seguridad en software y hardware o de examinar la biometría y sistemas biométricos. Además, el alumnado conseguirá aplicar diversas técnicas de cifrado en la red como TLS, VPN o SSH y controlar las mejores herramientas de monitorización de sistemas existentes actualmente en el mercado. El amplio abanico de recursos y los casos prácticos proporcionarán un aprendizaje muy cercano a la realidad que deberá afrontar en su ámbito laboral.





Logra una especialización en el campo de la seguridad informática gracias a este Experto Universitario. Inscríbete ya"

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



Objetivos específicos

Módulo 1. Implementación práctica de políticas de seguridad en software y hardware

- Determinar qué es la autenticación e identificación
- Analizar los distintos métodos de autenticación que existen y su implementación práctica
- Implementar la política de control de accesos correcta al software y sistemas
- Establecer las principales tecnologías de identificación actuales
- Generar conocimiento especializado sobre las distintas metodologías que existen para el bastionado de sistemas

Módulo 2. Implementación de políticas de seguridad física y ambiental en la empresa

- Analizar el término de área segura y perímetro seguro
- Examinar la biometría y sistemas biométricos
- Implementar políticas de seguridad correctas en materia de seguridad física
- Desarrollar la normativa vigente acerca de áreas seguras de sistemas informáticos

Módulo 3. Políticas de comunicaciones seguras en la empresa

- Hacer segura una red de comunicaciones mediante la división de la misma
- Analizar los distintos algoritmos de cifrado utilizados en redes de comunicaciones
- Implementar diversas técnicas de cifrado en la red como TLS, VPN o SSH

Módulo 4. 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 monitorizar las redes
- Compilar las mejores herramientas de monitorización de sistemas existentes actualmente en el mercado

Este programa te proporcionará las herramientas necesarias para examinar la biometría y los sistemas biométricos en una empresa"

03

Dirección del curso

Este Experto Universitario cuenta con un profesorado con experiencia en gestión web y seguridad en redes y sistemas de servicios. Su amplio conocimiento en esta área de la informática ha sido clave para su elección. De esta forma, el alumnado cuenta con la garantía de ser guiado, durante los seis meses de esta enseñanza, por docentes que poseen la enseñanza académica necesaria y la práctica diaria en la aplicación de herramientas, sistemas y protocolos de seguridad en empresas. Todo ello, con el objetivo final de proporcionar un aprendizaje de calidad, que le permita al profesional de la informática avanzar en esta área.





Un equipo docente con amplia experiencia en Seguridad Informática será tu garantía de éxito en este aprendizaje"

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

Dña. López García, Rosa María

- Especialista en Información de Gestión
- Profesora de Linux Professional Institute
- Colaboradora en Academia Hacker Incibe
- Capitana de Talento en Ciberseguridad en Teamciberhack
- Administrativa y gestora contable y financiera en Integra2Transportes
- Auxiliar administrativo en recursos de compras en el Centro de Educación Cardenal Marcelo Espínola
- Técnico Superior en Ciberseguridad y hacking Ético
- Miembro de Ciberpatrulla

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

04

Estructura y contenido

El profesorado de este Experto Universitario ha elaborado un temario que integra todo el conocimiento sobre la implementación práctica de políticas de seguridad en software y hardware, dedicando uno de sus módulos a abordar en profundidad los sistemas biométricos y la protección frente a factores ambientales como incendios o terremotos. Además, este plan de estudio presta especial atención a las herramientas de monitorización de sistemas y los algoritmos criptográficos. El sistema *Relearning*, basado en la reiteración de contenido, y los casos eminentemente prácticos permitirán al alumnado adquirir un aprendizaje sólido y de forma sencilla.





Adapta la carga lectiva de esta enseñanza a tus necesidades. Accede al contenido a cualquier hora y desde cualquier lugar. Haz clic y matricúlate"

Módulo 1. Implementación práctica de políticas de seguridad en software y hardware

1.1. Implementación práctica de políticas de seguridad en software y hardware
- 1.1.1. Implementación de identificación y autorización
- 1.1.2. Implementación de técnicas de identificación
- 1.1.3. Medidas técnicas de autorización

1.2. Tecnologías de identificación y autorización
- 1.2.1. Identificador y OTP
- 1.2.2. *Token* USB o tarjeta inteligente PKI
- 1.2.3. La llave "Confidencial Defensa"
- 1.2.4. El RFID Activo

1.3. Políticas de seguridad en el acceso a software y sistemas
- 1.3.1. Implementación de políticas de control de accesos
- 1.3.2. Implementación de políticas de acceso a comunicaciones
- 1.3.3. Tipos de herramientas de seguridad para control de acceso

1.4. Gestión de acceso a usuarios
- 1.4.1. Gestión de los derechos de acceso
- 1.4.2. Segregación de roles y funciones de acceso
- 1.4.3. Implementación derechos de acceso en sistemas

1.5. Control de acceso a sistemas y aplicaciones
- 1.5.1. Norma del mínimo acceso
- 1.5.2. Tecnologías seguras de inicios de sesión
- 1.5.3. Políticas de seguridad en contraseñas

1.6. Tecnologías de sistemas de identificación
- 1.6.1. Directorio activo
- 1.6.2. OTP
- 1.6.3. PAP, CHAP
- 1.6.4. KERBEROS, DIAMETER, NTLM

1.7. Controles CIS para bastionado de sistemas
- 1.7.1. Controles CIS básicos
- 1.7.2. Controles CIS fundamentales
- 1.7.3. Controles CIS organizacionales

1.8. Seguridad en la operativa
- 1.8.1. Protección contra código malicioso
- 1.8.2. Copias de seguridad
- 1.8.3. Registro de actividad y supervisión

1.9. Gestión de las vulnerabilidades técnicas
- 1.9.1. Vulnerabilidades técnicas
- 1.9.2. Gestión de vulnerabilidades técnicas
- 1.9.3. Restricciones en la instalación de software

1.10. Implementación de prácticas de políticas de seguridad
- 1.10.1. Implementación de prácticas de políticas de seguridad
- 1.10.2. Vulnerabilidades lógicas
- 1.10.3. Implementación de políticas de defensa

Módulo 2. Implementación de políticas de seguridad física y ambiental en la empresa

2.1. Áreas seguras
- 2.1.1. Perímetro de seguridad física
- 2.1.2. Trabajo en áreas seguras
- 2.1.3. Seguridad de oficinas, despachos y recursos

2.2. Controles físicos de entrada
- 2.2.1. Controles físicos de entrada
- 2.2.2. Políticas de control de acceso físico
- 2.2.3. Sistemas de control físico de entrada

2.3. Vulnerabilidades de accesos físicos
- 2.3.1. Vulnerabilidades de accesos físicos
- 2.3.2. Principales vulnerabilidades físicas
- 2.3.3. Implementación de medidas de salvaguardas

2.4. Sistemas biométricos fisiológicos
- 2.4.1. Huella dactilar
- 2.4.2. Reconocimiento facial
- 2.4.3. Reconocimiento de iris y retina
- 2.4.4. Otros sistemas biométricos fisiológicos

2.5. Sistemas biométricos de comportamiento
- 2.5.1. Reconocimiento de firma
- 2.5.2. Reconocimiento de escritor
- 2.5.3. Reconocimiento de voz
- 2.5.4. Otros sistemas biométricos de comportamientos

2.6. Gestión de riesgos en biometría
- 2.6.1. Gestión de riesgos en biometría
- 2.6.2. Implementación de sistemas biométricos
- 2.6.3. Vulnerabilidades de los sistemas biométricos

2.7. Implementación de políticas en *Hosts*
- 2.7.1. Instalación de suministro y seguridad de cableado
- 2.7.2. Emplazamiento de los equipos
- 2.7.3. Salida de los equipos fuera de las dependencias
- 2.7.4. Equipo informático desatendido y política de puesto despejado

2.8. Protección ambiental
- 2.8.1. Sistemas de protección ante incendios
- 2.8.2. Sistemas de protección ante seísmos
- 2.8.3. Sistemas de protección antiterremotos

2.9. Seguridad en centro de procesamiento de datos
- 2.9.1. Puertas de seguridad
- 2.9.2. Sistemas de videovigilancia (CCTV)
- 2.9.3. Control de seguridad

2.10. Normativa internacional de la seguridad física
- 2.10.1. IEC 62443-2-1 (europea)
- 2.10.2. NERC CIP-005-5 (EE. UU)
- 2.10.3. NERC CIP-014-2 (EE. UU)

Módulo 3. Políticas de comunicaciones seguras en la empresa

3.1. Gestión de la seguridad en las redes
- 3.1.1. Control y monitorización de red
- 3.1.2. Segregación de redes
- 3.1.3. Sistemas de seguridad en redes

3.2. Protocolos seguros de comunicación
- 3.2.1. Modelo TCP/IP
- 3.2.2. Protocolo IPSEC
- 3.2.3. Protocolo TLS

3.3. Protocolo TLS 1.3
- 3.3.1. Fases de un proceso TLS 1.3
- 3.3.2. Protocolo Handshake
- 3.3.3. Protocolo de registro
- 3.3.4. Diferencias con TLS 1.2

3.4. Algoritmos criptográficos
- 3.4.1. Algoritmos criptográficos usados en comunicaciones
- 3.4.2. *Cipher-suites*
- 3.4.3. Algoritmos criptográficos permitidos para TLS 1.3

3.5. Funciones *Digest*
- 3.5.1. Funciones *Digest*
- 3.5.2. MD6
- 3.5.3. SHA

3.6. PKI. Infraestructura de clave pública
- 3.6.1. PKI y sus entidades
- 3.6.2. Certificado digital
- 3.6.3. Tipos de certificados digital

3.7. Comunicaciones de túnel y transporte
- 3.7.1. Comunicaciones túnel
- 3.7.2. Comunicaciones transporte
- 3.7.3. Implementación túnel cifrado

3.8. SSH. *Secure Shell*
- 3.8.1. SSH. Cápsula segura
- 3.8.2. Funcionamiento de SSH
- 3.8.3. Herramientas SSH

3.9. Auditoría de sistemas criptográficos
- 3.9.1. Auditoría de sistemas criptográficos
- 3.9.2. Pruebas de integridad
- 3.9.3. Testeo sistema criptográfico

3.10. Sistemas criptográficos
- 3.10.1. Sistemas criptográficos
- 3.10.2. Vulnerabilidades sistemas criptográficos
- 3.10.3. Salvaguardas en criptografía

Módulo 4. Herramientas de monitorización en políticas de seguridad de los sistemas de información

4.1. Políticas de monitorización de sistemas de la información
- 4.1.1. Monitorización de sistemas
- 4.1.2. Métricas
- 4.1.3. Tipos de métricas

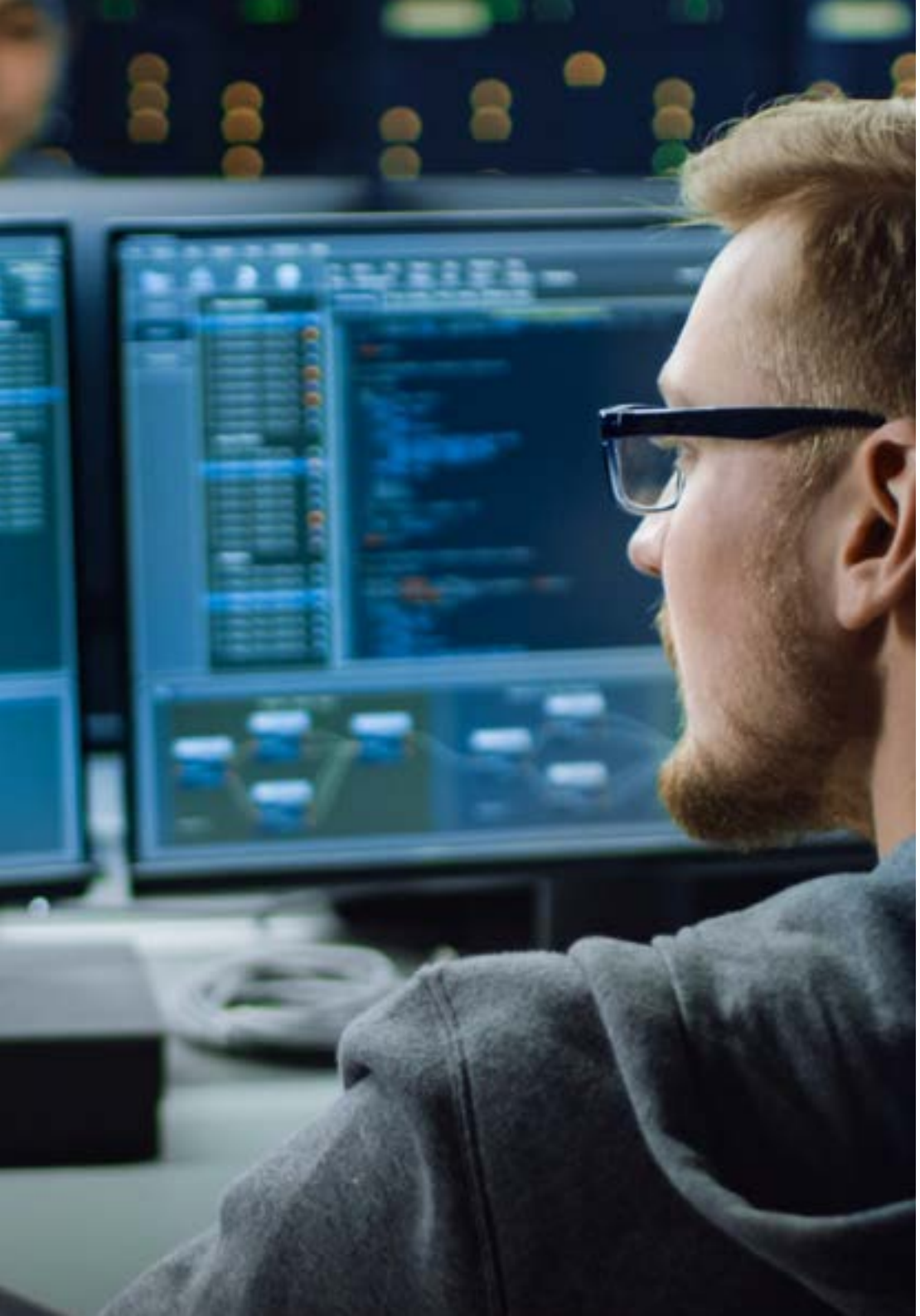
4.2. Auditoría y registro en sistemas
- 4.2.1. Auditoría y registro en sistemas
- 4.2.2. Auditoría y registro en Windows
- 4.2.3. Auditoría y registro en Linux

4.3. Protocolo SNMP. *Simple Network Management Protocol*
- 4.3.1. Protocolo SNMP
- 4.3.2. Funcionamiento de SNMP
- 4.3.3. Herramientas SNMP

4.4. Monitorización de redes
- 4.4.1. Monitorización de redes
- 4.4.2. La monitorización de red en sistemas de control
- 4.4.3. Herramientas de monitorización para sistemas de control

4.5. Nagios. Sistema de monitorización de redes
- 4.5.1. Nagios
- 4.5.2. Funcionamiento de Nagios
- 4.5.3. Instalación de Nagios

4.6. Zabbix. Sistema de monitorización de redes
- 4.6.1. Zabbix
- 4.6.2. Funcionamiento de Zabbix
- 4.6.3. Instalación de Zabbix



4.7. Cacti. Sistema de monitorización de redes
- 4.7.1. Cacti
- 4.7.2. Funcionamiento de Cacti
- 4.7.3. Instalación de Cacti

4.8. Pandora. Sistema de monitorización de redes
- 4.8.1. Pandora
- 4.8.2. Funcionamiento de Pandora
- 4.8.3. Instalación de Pandora

4.9. SolarWinds. Sistema de monitorización de redes
- 4.9.1. SolarWinds
- 4.9.2. Funcionamiento de SolarWinds
- 4.9.3. Instalación de SolarWinds

4.10. Normativa sobre monitorización
- 4.10.1. Normativa sobre monitorización
- 4.10.2. Controles CIS sobre auditoría y registro
- 4.10.3. NIST 800-123 (EE. UU)

Los resúmenes interactivos y los casos prácticos elaborados por el equipo docente te aportarán el contenido necesario para avanzar en tu carrera profesional"

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.

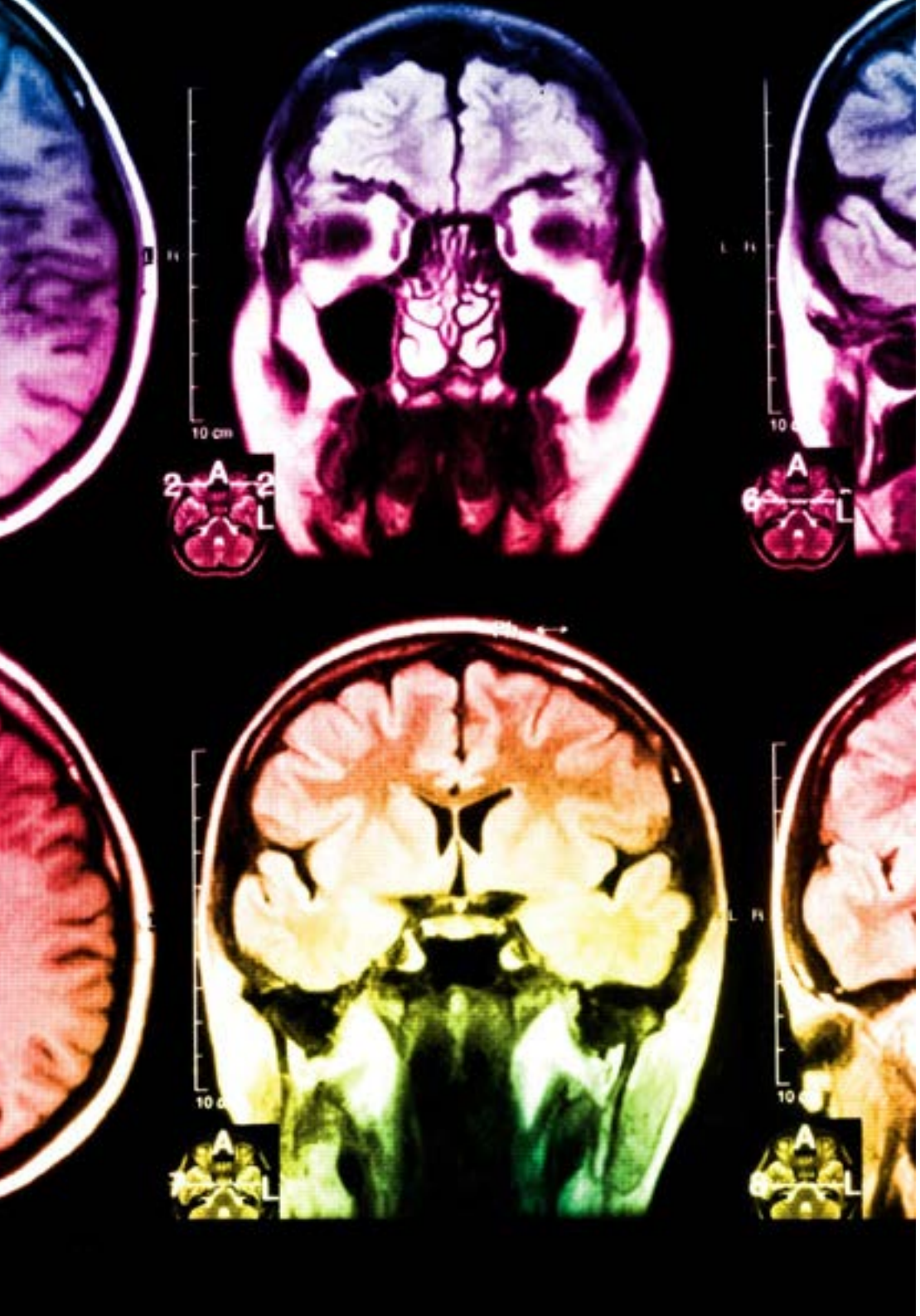
Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el Relearning.

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.

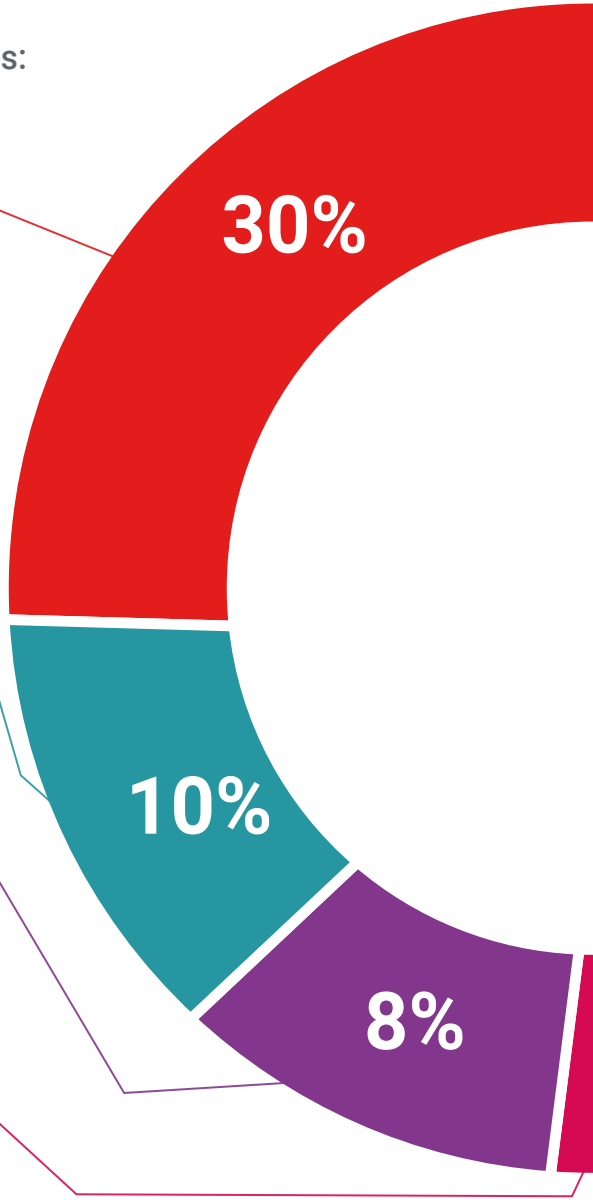
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

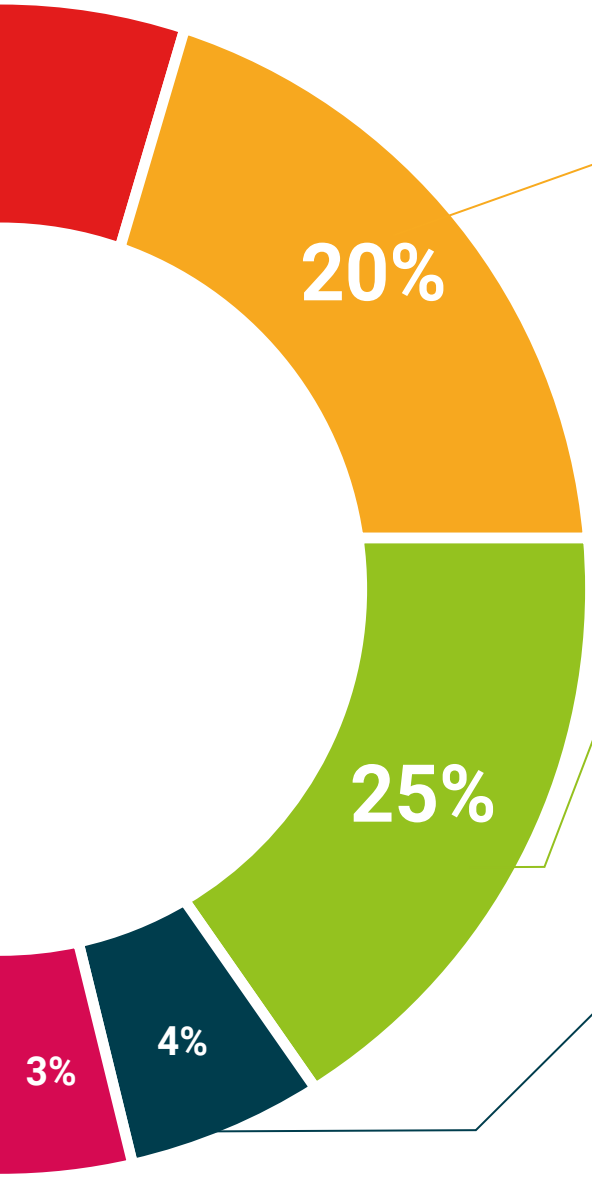
Prácticas de habilidades y competencias

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 Implementación de Políticas 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 Implementación de Políticas 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 Implementación de Políticas 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

Implementación de Políticas 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
Implementación de Políticas de Seguridad Informática

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

Experto Universitario

Implementación de Políticas de Seguridad Informática



tech universidad tecnológica