Experto Universitario
Ciberseguridad Preventiva

tech universidad tecnológica

Experto Universitario
Ciberseguridad Preventiva

- Modalidad: **online**
- Duración: **3 meses**
- Titulación: **TECH Universidad Tecnológica**
- Acreditación: **18 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: www.techtitute.com/informatica/experto-universitario/experto-ciberseguridad-preventiva

Índice

01
Presentación
pág. 4

02
Objetivos
pág. 8

03
Dirección de curso
pág. 12

04
Estructura y contenido
pág. 18

05
Metodología
pág. 24

06
Titulación
pág. 32

01

Presentación

En el uso de dispositivos móviles se ponen en juego numerosos datos que los programas necesitan para realizar sus funciones. Este tipo de confianza que el usuario deposita en su tecnología de uso cotidiano supone la asunción de un riesgo elevado de vulneración de esta información a través de ciberataques. El desarrollo constante de nuevas formas de conseguir estos datos promueve que el desarrollo de sistemas preventivos deba ser contante, moviéndose con anticipación y dando respuestas rápidas y eficaces a cada nueva amenaza. El especialista que trabaja en este campo está obligado por ello, a una constante actualización que le permita mantener sus conocimientos totalmente al día, una tarea compleja por la velocidad de los cambios en el sector. Este programa es la respuesta más inmediata y de mayor calidad a las necesidades de capacitación en Ciberseguridad Preventiva del mercado docente online.

Avanza en tu capacidad en el entorno de la Ciberseguridad Preventiva con el programa más completo y actualizado en este campo"

En la actualidad ninguna empresa está exenta de sufrir un ciberataque y, por tanto, padecer las diferentes consecuencias que implica. Independientemente del tamaño de la misma, está expuesta a robos de información, chantajes, sabotajes, etc. Es necesario realizar un estudio de vulnerabilidades y determinar la superficie de ataque, por lo que cada vez más se van a realizar estudios periódicos de vulnerabilidades y riesgos. Cada empresa tendrá que ver si cumple con las normas y legislación del país conde está ubicada y ser consciente de los daños ocasionados tanto monetarios como otros daños inmateriales, por ejemplo, su reputación.

Este programa supone un estudio de la actualidad en Ciberinteligencia y Ciberseguridad. Aborda aspectos fundamentales como el Ciclo de inteligencia, fuentes de inteligencia, ingeniería social, metodología OSINT, HUMINT, Anonimización, análisis de riesgos, metodologías existentes (OWASP, OWISAM, OSSTM, PTES) y normativas vigentes en materia de ciberseguridad. Además, examina los organismos internacionales más relevantes en materia de Ciberseguridad, exponiendo su ámbito de actuación y su postura frente a diferentes problemas.

Todos los Desarrolladores se enfrentan al reto de realizar Código de Aplicaciones de Calidad y Seguridad, dado que, en el ecosistema actual de aplicaciones, cualquier vulnerabilidad del código o del sistema va a provocar pérdidas, exposición y robos de datos, así como otros problemas causados por Ciberataques. Es obligación del Desarrollador conocer bien los diferentes entornos y fases por las que va a pasar su código y asegurarse de que funciona, en cualquiera de ellos, de la manera más eficiente y segura.

Además, TECH pondrá a disposición del alumnado *Masterclasses* exclusivas, las cuales complementarán el temario de la mano de un profesional de relevancia internacional. Este docente, especialista en Inteligencia, Ciberseguridad y Tecnologías Disruptivas, acompañará al egresado a la hora de profundizar en la Ciberseguridad Preventiva, pasando por las técnicas y herramientas más útiles en inteligencia.

Este **Experto Universitario en Ciberseguridad Preventiva** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos
- 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.

"Desarrolla todo tu potencial gracias a las Masterclasses en Ciberseguridad, impartidas por un especialista de gran prestigio internacional en este campo"

Con un planteamiento totalmente centrado en la práctica, este Experto Universitario impulsará tu capacidad hasta el nivel de un especialista"

Aprende a desarrollar códigos de aplicaciones de seguridad planteando estrategias que disminuyan la vulnerabilidad.

Un proceso de alta capacitación creado para ser asumible y flexible, con la metodología más interesante de la docencia online.

El programa incluye, en su cuadro docente, a profesionales del sector que vierten en esta capacitación la experiencia de su trabajo, además de reconocidos especialistas de sociedades de referencia y universidades de prestigio.

Su contenido multimedia, elaborado con la última tecnología educativa, permitirá al profesional un aprendizaje situado y contextual, es decir, un entorno simulado que proporcionará una capacitación inmersiva programada para entrenarse ante situaciones reales.

El diseño de este programa se centra en el Aprendizaje Basado en Problemas, mediante el cual el profesional deberá tratar de resolver las distintas situaciones de práctica profesional que se le planteen a lo largo del curso académico. Para ello, contará con la ayuda de un novedoso sistema de vídeo interactivo realizado por reconocidos expertos.

02

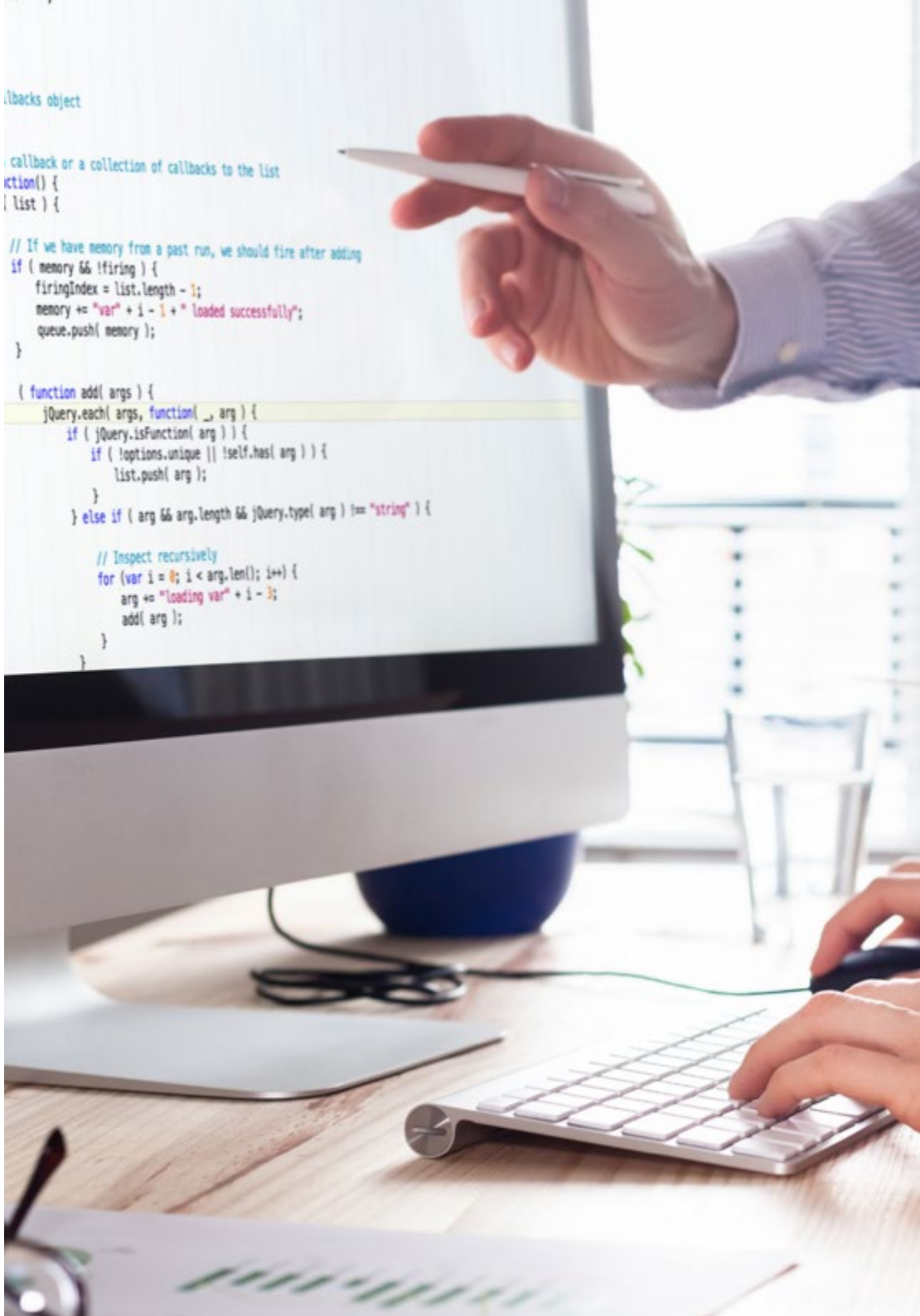
Objetivos

Este Experto Universitario impulsará de forma espectacular la capacidad de intervención en este campo. Con objetivos realistas y de alto interés, este proceso de estudio se ha configurado para llevar al alumnado, de forma progresiva a la adquisición de los conocimientos teóricos y prácticos necesarios para intervenir con calidad desarrollando, además, competencias transversales que permitirán afrontar situaciones complejas elaborando respuestas ajustadas y precisas.

Conoce y aplica las metodologías más interesantes en Ciberseguridad Preventiva y comienza a desarrollar aplicaciones con los sistemas de prevención más eficaces del momento"

Objetivos generales

- Analizar el rol del analista en ciberseguridad
- Profundizar en la ingeniería social y sus métodos
- Examinar las metodologías OSINT, HUMINT, OWASP, PTEC. OSSTM, OWISAM
- Realizar un análisis de riesgo y conocer las métricas de riesgo
- Determinar el adecuado uso de anonimato y uso de redes como TOR, I2P y *Freenet*
- Compilar las normativas vigentes en materia de ciberseguridad
- Generar conocimiento especializado para realizar una auditoría de seguridad
- Analizar los diferentes sistemas existentes
- Evaluar la información obtenida y desarrollar mecanismos de prevención y *hacking*
- Establecer prioridades en el estudio y resolución de las vulnerabilidades
- Demostrar que un sistema es vulnerable, atacarlo con fines preventivos y solventar dichos problemas
- Determinar las directrices que debe seguir un buen desarrollador para cumplir con la seguridad necesaria
- Establecer una metodología apropiada para el desarrollador y para el entorno de producción
- Concretar las pruebas que hay que realizar al software desarrollado



Objetivos específicos

Módulo 1. Ciberinteligencia y ciberseguridad

- Desarrollar las metodologías usadas en materia de ciberseguridad
- Examinar el ciclo de inteligencia y establecer su aplicación en la ciberinteligencia
- Determinar el papel del analista de inteligencia y los obstáculos de actividad evacuativa
- Analizar las metodologías OSINT, OWISAM, OSSTM, PTES, OWASP
- Establecer las herramientas más comunes para la producción de inteligencia
- Llevar a cabo un análisis de riesgos y conocer las métricas usadas
- Concretar las opciones de anonimato y el uso de redes como TOR, I2P, *FreeNet*
- Detallar las Normativas vigentes en ciberseguridad

Módulo 2. *Hacking* ético

- Examinar los métodos de IOSINT
- Recopilar la información disponible en medios públicos
- Escanear redes para obtener información de modo activo
- Desarrollar laboratorios de pruebas
- Analizar las herramientas para el desempeño del *pentesting*
- Catalogar y evaluar las diferentes vulnerabilidades de los sistemas
- Concretar las diferentes metodologías de *hacking*

Módulo 3. Desarrollo seguro

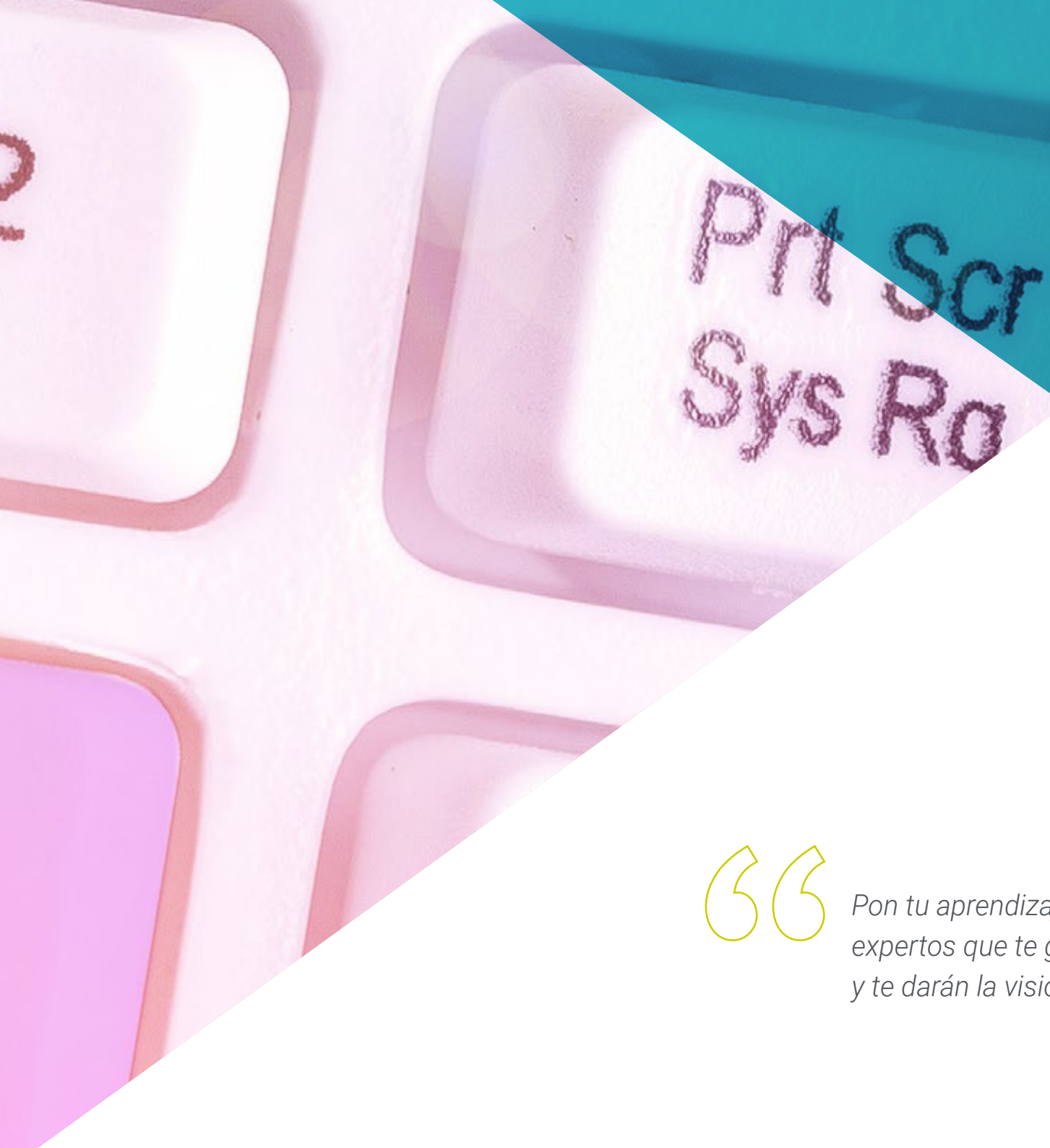
- Establecer los requisitos necesarios para el correcto funcionamiento de una aplicación de forma segura
- Examinar los archivos de *Logs* para entender los mensajes de error
- Analizar los diferentes eventos y decidir qué mostrar al usuario y qué guardar en los *logs*
- Generar un código sanitizado, fácilmente verificable y de calidad
- Evaluar la documentación adecuada para cada fase del desarrollo
- Concretar el comportamiento del servidor para optimizar el sistema
- Desarrollar código modular, reusable y mantenible

"Aprenderás a optimizar sistemas aplicando requisitos que propicien la mayor seguridad y usabilidad de las aplicaciones"

03

Dirección del curso

Los docentes que imparten este programa han sido seleccionados por su excepcional competencia en este campo. Combinan la experiencia técnica y práctica con la docente, ofreciendo al alumnado un apoyo de primer nivel en la consecución de sus metas. A través de ellos, el programa ofrece la visión más directa e inmediata de las características reales de la intervención en este campo consiguiendo una visión contextual del máximo interés.



Pon tu aprendizaje en manos de profesionales expertos que te guiarán en cada fase del estudio y te darán la visión más realista de este trabajo"

Director Invitado Internacional

El Doctor Frederic Lemieux es reconocido a nivel internacional como experto innovador y líder inspirador en los campos de la **Inteligencia**, **Seguridad Nacional**, **Seguridad Interna**, **Ciberseguridad** y **Tecnologías Disruptivas**. Y es que su constante dedicación y relevantes aportaciones en Investigación y Educación, le posicionan como una figura clave en la **promoción de la seguridad** y el **entendimiento de las tecnologías emergentes** en la actualidad. Durante su trayectoria profesional, ha conceptualizado y dirigido programas académicos de vanguardia en diversas instituciones de renombre, como la **Universidad de Montreal**, la **Universidad George Washington** y la **Universidad de Georgetown.**

A lo largo de su extenso bagaje, ha publicado múltiples libros de gran relevancia, todos ellos relacionados con la **inteligencia criminal**, la **labor policial**, las **amenazas cibernéticas** y la **seguridad internacional**. Asimismo, ha contribuido de manera significativa al campo de la **Ciberseguridad** con la publicación de numerosos artículos en revistas académicas, las cuales examinan el control del crimen durante desastres importantes, la lucha contra el terrorismo, las agencias de inteligencia y la cooperación policial. Además, ha sido panelista y ponente principal en diversas conferencias nacionales e internacionales, consolidándose como un referente en el ámbito académico y profesional.

El Doctor Lemieux ha desempeñado roles editoriales y evaluativos en diferentes organizaciones académicas, privadas y gubernamentales, reflejando su influencia y compromiso con la excelencia en su campo de especialización. De esta forma, su prestigiosa carrera académica lo ha llevado a desempeñarse como Profesor de Prácticas y Director de Facultad de los programas MPS en **Inteligencia Aplicada**, **Gestión de Riesgos en Ciberseguridad**, **Gestión Tecnológica** y **Gestión de Tecnologías de la Información** en la **Universidad de Georgetown.**

Dr. Lemieux, Frederic

- Director del Máster en Cybersecurity Risk Management en Georgetown, Washington, Estados Unidos
- Director del Máster en Technology Management en la Universidad de Georgetown
- Director del Máster en Applied Intelligence en la Universidad de Georgetown
- Profesor de Prácticas en la Universidad de Georgetown
- Doctor en Criminología por la School of Criminology en la Universidad de Montreal
- Licenciado en Sociología y Minor Degree en Psicología por la Universidad de Laval
- Miembro de: New Program Roundtable Committee, Universidad de Georgetown

"Gracias a TECH podrás aprender con los mejores profesionales del mundo"

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

SHARE
HTML
JUST MAKE THE BEST THINGS!
CREATIVE
LAYOUT
CONTENT

04

Estructura y contenido

Este programa te llevará a través del estudio de todos y cada uno de los campos de conocimiento que el profesional que interviene en ciberseguridad debe conocer en el ámbito de la acción preventiva. Para ello se ha estructurado con vistas a la adquisición eficiente de conocimientos sumatorios, que propicien la penetración de los aprendizajes y consoliden lo estudiado dotando al alumnado de capacidad de intervención de la manera más rápida posible. Un recorrido de alta intensidad y enorme calidad creado para capacitar a los mejores del sector.

El análisis y la intervención en Ciberseguridad Preventiva desarrollado de forma estructurada en un planteamiento de estudio centrado en la eficiencia"

Módulo 1. Ciberinteligencia y Ciberseguridad

1.1. Ciberinteligencia
- 1.1.1. Ciberinteligencia
  - 1.1.1.1. La inteligencia
    - 1.1.1.1.1. Ciclo de inteligencia
  - 1.1.1.2. Ciberinteligencia
  - 1.1.1.3. Los sesgos del analista de inteligencia en la actividad evaluativa
- 1.1.2. El analista de inteligencia
  - 1.1.2.1. El rol del analista de inteligencia
  - 1.1.2.2. Ciberinteligencia

1.2. Ciberseguridad
- 1.2.1. Las capas de seguridad
- 1.2.2. Identificación de las ciberamenazas
  - 1.2.2.1. Amenazas externas
  - 1.2.2.2. Amenazas internas
- 1.2.3. Acciones adversas
  - 1.2.3.1. Ingeniería social
  - 1.2.3.2. Métodos comúnmente usados

1.3. Técnicas y herramientas de inteligencias
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. HUMIT
- 1.3.4. Distribuciones de *Linux* y herramientas
- 1.3.5. OWISAM
- 1.3.6. OWISAP
- 1.3.7. PTES
- 1.3.8. OSSTMM

1.4. Metodologías de evaluación
- 1.4.1. El análisis de inteligencia
- 1.4.2. Técnicas de organización de la información adquirida
- 1.4.3. Fiabilidad y credibilidad de las fuentes de información
- 1.4.4. Metodologías de análisis
- 1.4.5. Presentación de los resultados de la inteligencia

1.5. Auditorías y documentación
- 1.5.1. La auditoría en seguridad informática
- 1.5.2. Documentación y permisos para auditoría
- 1.5.3. Tipos de auditoría
- 1.5.4. Entregables
  - 1.5.4.1. Informe técnico
  - 1.5.4.2. Informe ejecutivo

1.6. Anonimato en la red
- 1.6.1. Uso de anonimato
- 1.6.2. Técnicas de anonimato (*Proxy*, VPN)
- 1.6.3. Redes TOR, *Freenet* e IP2

1.7. Amenazas y tipos de seguridad
- 1.7.1. Tipos de amenazas
- 1.7.2. Seguridad física
- 1.7.3. Seguridad en redes
- 1.7.4. Seguridad lógica
- 1.7.5. Seguridad en aplicaciones web
- 1.7.6. Seguridad en dispositivos móviles

1.8. Normativa y *compliance*
- 1.8.1. RGPD
- 1.8.2. La estrategia nacional de ciberseguridad 2019
- 1.8.3. Familia ISO 27000
- 1.8.4. Marco de ciberseguridad NIST
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. Normativas *cloud*
- 1.8.8. SOX
- 1.8.9. PCI

1.9. Análisis de riesgos y métricas
- 1.9.1. Alcance de riesgos
- 1.9.2. Los activos
- 1.9.3. Las amenazas

1.9.4. las vulnerabilidades
1.9.5. Evaluación del riesgo
1.9.6. Tratamiento del riesgo
1.10. Organismos importantes en materia de ciberseguridad
1.10.1. NIST
1.10.2. ENISA
1.10.3. INCIBE
1.10.4. OEA
1.10.5. UNASUR - PROSUR

Módulo 2. Hacking Ético

2.1. Entorno de trabajo
2.1.1. Distribuciones *Linux*
2.1.1.1. *Kali Linux - Offensive Security*
2.1.1.2. *Parrot* OS
2.1.1.3. *Ubuntu*
2.1.2. Sistemas de virtualización
2.1.3. *Sandbox*
2.1.4. Despliegue de laboratorios
2.2. Metodologías
2.2.1. OSSTMM
2.2.2. OWASP
2.2.3. NIST
2.2.4. PTES
2.2.5. ISSAF
2.3. *Footprinting*
2.3.1. Inteligencia de fuentes abiertas (OSINT)
2.3.2. Búsqueda de brechas y vulnerabilidades de datos
2.3.3. Uso de herramientas pasivas
2.4. Escaneo de redes
2.4.1. Herramientas de escaneo
2.4.1.1. *Nmap*
2.4.1.2. *Hping3*
2.4.1.3. Otras herramientas de escaneo
2.4.2. Técnicas de escaneo
2.4.3. Técnicas de evasión de *firewall* e IDS
2.4.4. *Banner Grabbing*
2.4.5. Diagramas de red
2.5. Enumeración
2.5.1. Enumeración SMTP
2.5.2. Enumeración DNS
2.5.3. Enumeración de NetBIOS y Samba
2.5.4. Enumeración de LDAP
2.5.5. Enumeración de SNMP
2.5.6. Otras técnicas de enumeración
2.6. Análisis de vulnerabilidades
2.6.1. Soluciones de análisis de vulnerabilidades
2.6.1.1. *Qualys*
2.6.1.2. *Nessus*
2.6.1.3. CFI *LanGuard*
2.6.2. Sistemas de puntuación de vulnerabilidades
2.6.2.1. CVSS
2.6.2.2. CVE
2.6.2.3. NVD
2.7. Ataques a redes inalámbrica
2.7.1. Metodología de *hacking* en redes inalámbricas
2.7.1.1. WiFi *Discovery*
2.7.1.2. Análisis de tráfico
2.7.1.3. Ataques del *aircrack*
2.7.1.3.1. Ataques WEP
2.7.1.3.2. Ataques WPA/WPA2
2.7.1.4. Ataques de *Evil Twin*
2.7.1.5. Ataques a WPS
2.7.1.6. *Jamming*
2.7.2. Herramientas para la seguridad inalámbrica

2.8. Hackeo de servidores webs
- 2.8.1. *Cross Site Scripting*
- 2.8.2. CSRF
- 2.8.3. *Session Hijacking*
- 2.8.4. SQL *injection*

2.9. Explotación de vulnerabilidades
- 2.9.1. Uso de *exploits* conocidos
- 2.9.2. Uso de *metasploit*
- 2.9.3. Uso de *malware*
  - 2.9.3.1. Definición y alcance
  - 2.9.3.2. Generación de *malware*
  - 2.9.3.3. Bypass de soluciones antivirus

2.10. Persistencia
- 2.10.1. Instalación de *rootkits*
- 2.10.2. Uso de ncat
- 2.10.3. Uso de tareas programadas para *backdoors*
- 2.10.4. Creación de usuarios
- 2.10.5. Detección de HIDS

Módulo 3. Desarrollo Seguro

3.1. Desarrollo seguro
- 3.1.1. Calidad, funcionalidad y seguridad
- 3.1.2. Confidencialidad, integridad y disponibilidad
- 3.1.3. Ciclo de vida del desarrollo de software

3.2. Fase de Requerimientos
- 3.2.1. Control de la autenticación
- 3.2.2. Control de roles y privilegios
- 3.2.3. Requerimientos orientados al riesgo
- 3.2.4. Aprobación de privilegios

3.3. Fases de Análisis y Diseño
- 3.3.1. Acceso a componentes y administración del sistema
- 3.3.2. Pistas de auditoría
- 3.3.3. Gestión de sesiones

3.3.4. Datos históricos
3.3.5. Manejo apropiado de errores
3.3.6. Separación de funciones
3.4. Fase de Implementación y Codificación
3.4.1. Aseguramiento del ambiente de desarrollo
3.4.2. Elaboración de la documentación técnica
3.4.3. Codificación segura
3.4.4. Seguridad en las comunicaciones
3.5. Buenas prácticas de Codificación Segura
3.5.1. Validación de datos de entrada
3.5.2. Codificación de los datos de salida
3.5.3. Estilo de programación
3.5.4. Manejo de registro de cambios
3.5.5. Prácticas criptográficas
3.5.6. Gestión de errores y *logs*
3.5.7. Gestión de archivos
3.5.8. Gestión de memoria
3.5.9. Estandarización y reutilización de funciones de seguridad
3.6. Preparación del servidor y *Hardening*
3.6.1. Gestión de usuarios, grupos y roles en el servidor
3.6.2. Instalación de software
3.6.3. *Hardening* del servidor
3.6.4. Configuración robusta del entorno de la aplicación
3.7. Preparación de la BBDD y *Hardening*
3.7.1. Optimización del motor de BBDD
3.7.2. Creación del usuario propio para la aplicación
3.7.3. Asignación de los privilegios precisos para el usuario
3.7.4. *Hardening* de la BBDD
3.8. Fase de pruebas
3.8.1. Control de calidad en controles de seguridad
3.8.2. Inspección del código por fases
3.8.3. Comprobación de la gestión de las configuraciones
3.8.4. Pruebas de caja negra
3.9. Preparación del Paso a producción
3.9.1. Realizar el control de cambios
3.9.2. Realizar procedimiento de paso a producción
3.9.3. Realizar procedimiento de *rollback*
3.9.4. Pruebas en fase de preproducción
3.10. Fase de mantenimiento
3.10.1. Aseguramiento basado en riesgos
3.10.2. Pruebas de mantenimiento de seguridad de caja blanca
3.10.3. Pruebas de mantenimiento de seguridad de caja negra

"Una experiencia de capacitación única, clave y decisiva para impulsar tu desarrollo 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

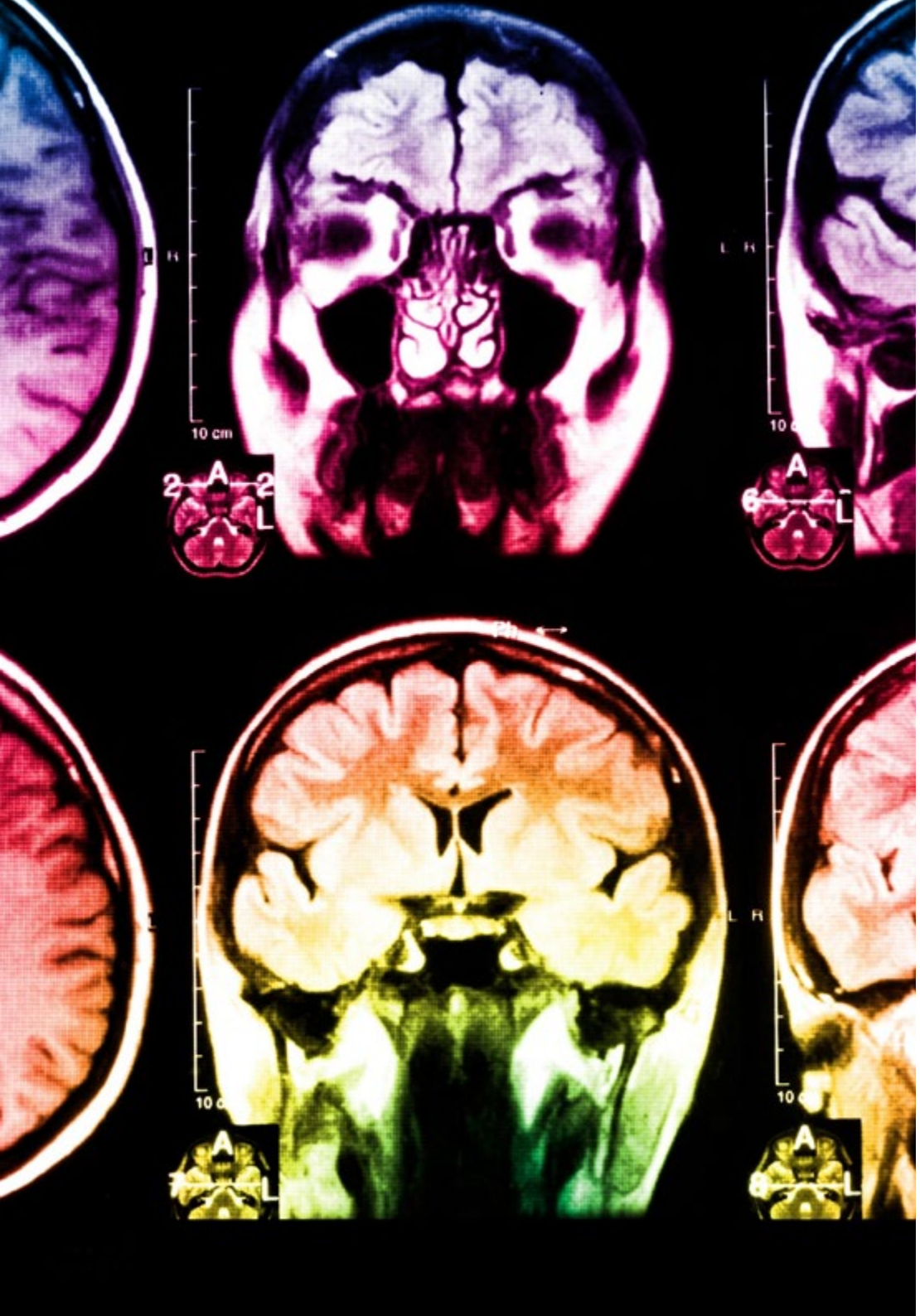
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

Potenciamos el Estudio de Caso con el mejor método de enseñanza 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.

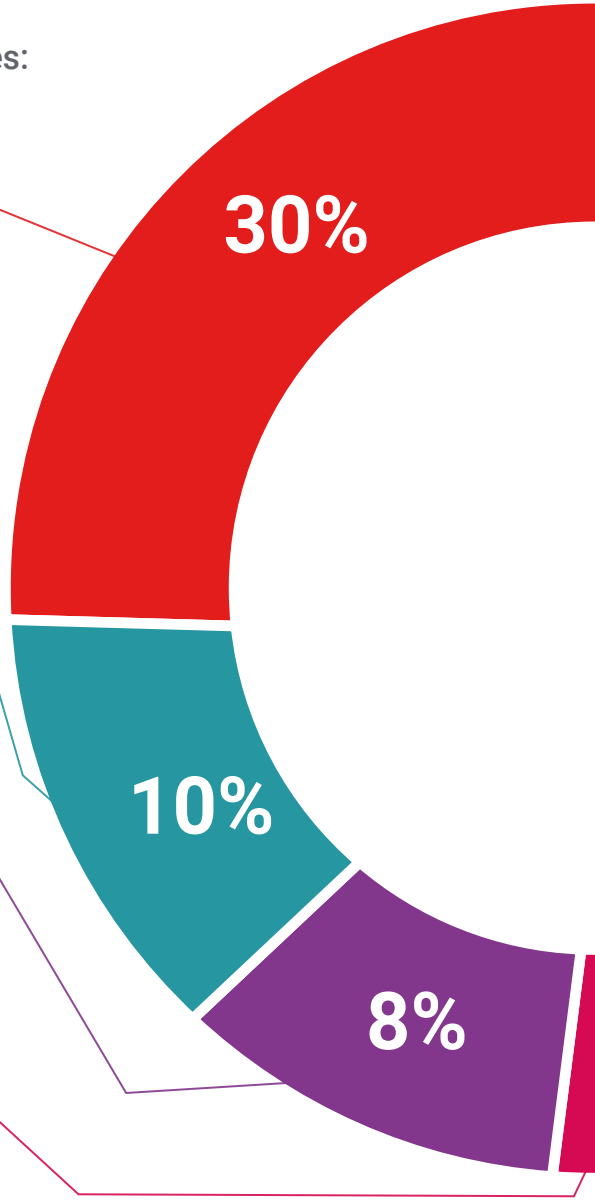
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

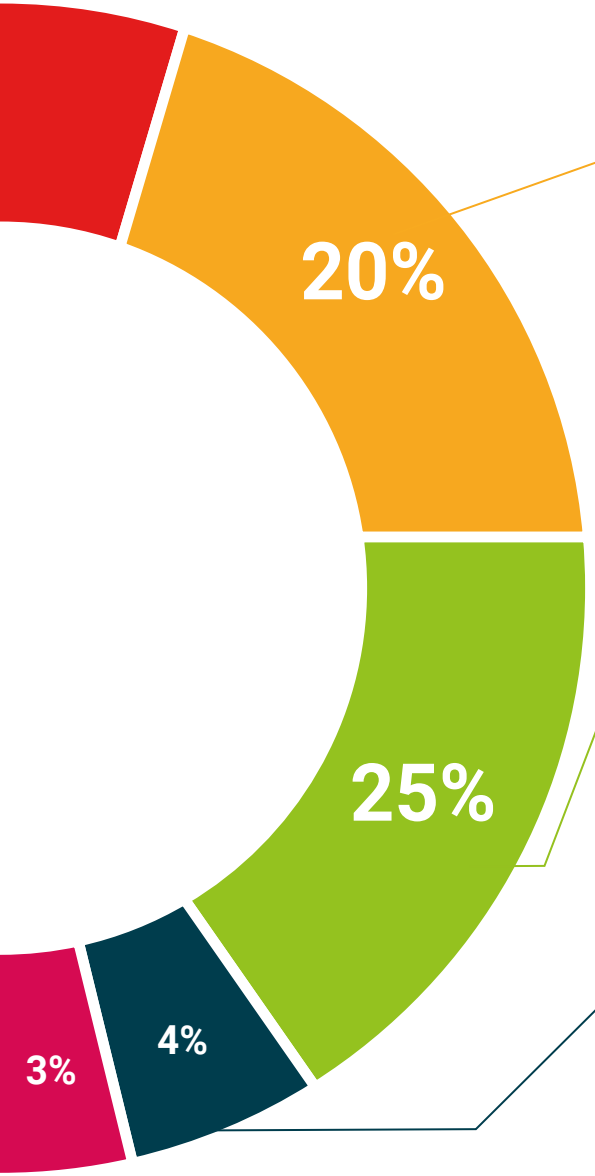
Prácticas de habilidades y competencias

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

Este programa en Ciberseguridad Preventiva 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 programa te permitirá obtener el título de **Experto Universitario en Ciberseguridad Preventiva** emitido por TECH Universidad Tecnológica.

TECH Universidad Tecnológica, es una Universidad española oficial, que forma parte del Espacio Europeo de Educación Superior (EEES). Con un enfoque centrado en la excelencia académica y la calidad universitaria a través de la tecnología.

Este título propio contribuye de forma relevante al desarrollo de la educación continua y actualización del profesional, garantizándole la adquisición de las competencias en su área de conocimiento y aportándole un alto valor curricular universitario a su formación. Es 100% válido en todas las Oposiciones, Carrera Profesional y Bolsas de Trabajo de cualquier Comunidad Autónoma española.

Además, el riguroso sistema de garantía de calidad de TECH asegura que cada título otorgado cumpla con los más altos estándares académicos, brindándole al egresado la confianza y la credibilidad que necesita para destacarse en su carrera profesional.

Título: **Experto Universitario en Ciberseguridad Preventiva**

Modalidad: **online**

Duración: **3 meses**

Acreditación: **18 ECTS**

tech universidad tecnológica

D/Dña _____, con documento de identificación _____ ha superado con éxito y obtenido el título de:

Experto Universitario en Ciberseguridad Preventiva

Se trata de un título propio de 450 horas de duración equivalente a 18 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH es una universidad Oficial Española legalmente reconocida mediante la Ley 1/2024, del 16 de abril, de la Comunidad Autónoma de Canarias, publicada en el Boletín Oficial del Estado (BOE) núm. 181, de 27 de julio de 2024 (pág. 96.369) e integrada en el Registro de Universidades, Centros y Títulos (RUCT) del Ministerio de Ciencia, Innovación y Universidades con el código 104.

En San Cristóbal de la Laguna, a 28 de febrero de 2024

Dr. Pedro Navarro Illana
Rector

código único TECH: AFWOR23S techtitute.com/titulos

*Apostilla de La Haya. En caso de que el alumno solicite que su título en papel recabe la Apostilla de La Haya, TECH EDUCATION realizará las gestiones oportunas para su obtención, con un coste adicional.

tech universidad tecnológica

Experto Universitario
Ciberseguridad Preventiva

- Modalidad: **online**
- Duración: **3 meses**
- Titulación: **TECH Universidad Tecnológica**
- Acreditación: **18 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Experto Universitario

Ciberseguridad Preventiva

tech universidad tecnológica