Experto Universitario
Ciberseguridad Defensiva



tech universidad tecnológica



tech universidad tecnológica

Experto Universitario
Ciberseguridad Defensiva

Modalidad: **Online**
Duración: **6 meses**
Titulación: **TECH Universidad Tecnológica**
Horas lectivas: **600 h.**
Acceso web: www.techtitute.com/informatica/experto-universitario/experto-ciberseguridad-defensiva

Índice

01
Presentación
pág. 4

02
Objetivos
pág. 8

03
Dirección de curso
pág. 12

04
Estructura y contenido
pág. 16

05
Metodología
pág. 22

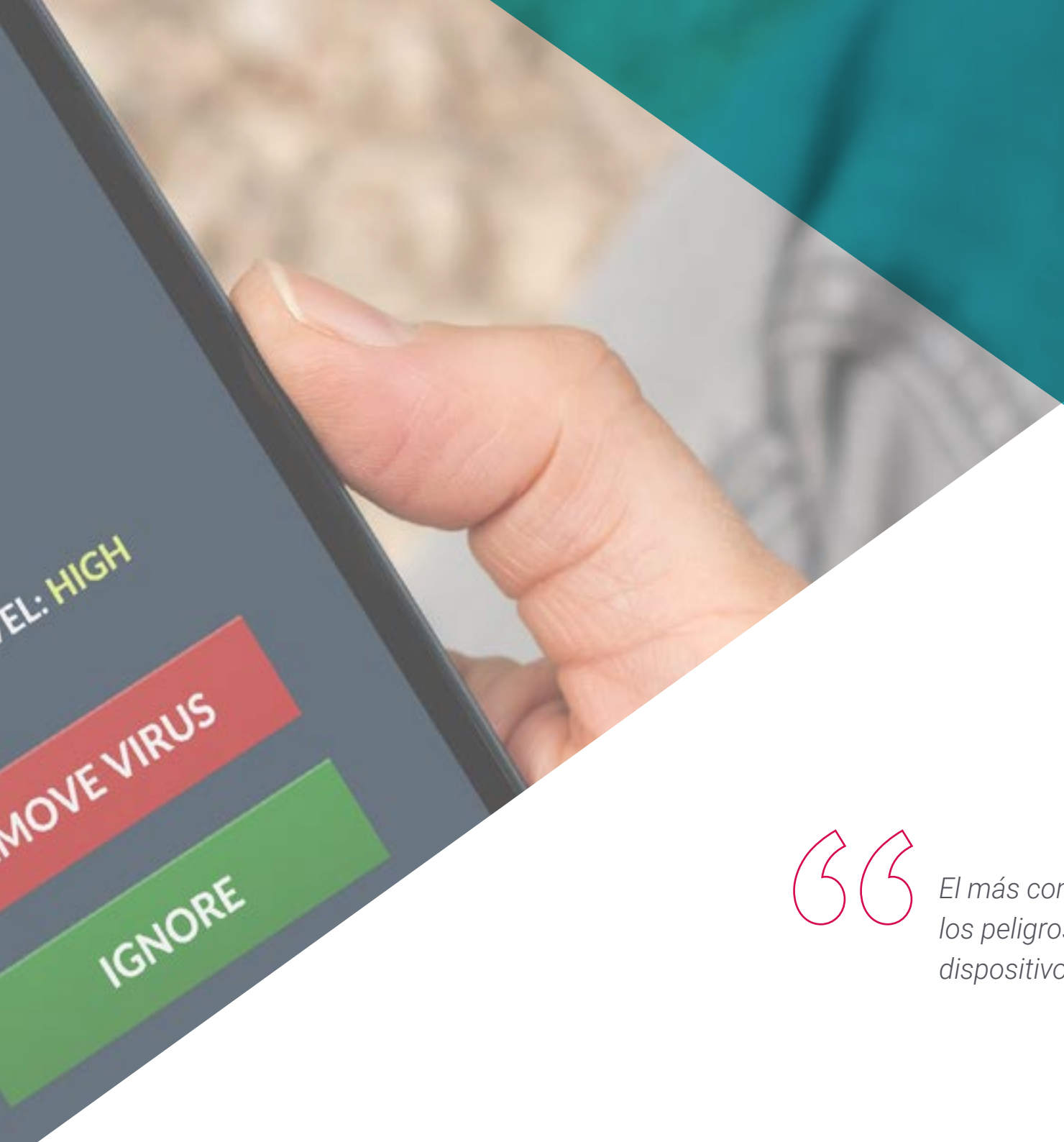
06
Titulación
pág. 30

01

Presentación

En el momento actual, en el que la vida cotidiana está directamente ligada al uso de dispositivos móviles, conocer las posibles formas de vulnerabilidad que acompañan a su uso es una necesidad imperiosa para los profesionales de las ramas tecnológicas. Con la sofisticación de los modelos se ha conseguido una capacidad de trabajo inusitada que los ha convertido en herramientas de alta sofisticación que acceden incluso, a datos sensibles personales y empresariales. Este programa estudiará profundamente todos los aspectos en los que los ciberataques pueden presentarse desarrollando las estrategias de ciberseguridad defensiva más innovadores y eficaces del momento. Un recorrido de alta capacitación que permitirá actuar como un especialista en este campo.





El más completo recorrido a través de los peligros y vulnerabilidades de los dispositivos móviles y su ciberprotección"

La seguridad doméstica y empresarial necesita ser estructurada por capas, es como una cadena y será tan fuerte como el eslabón más débil de la misma. Este Experto Universitario presenta las principales amenazas para los equipos de los usuarios y los servidores de forma que seamos capaces de tomar las medidas pertinentes y estar alertas ante cualquier situación.

Cuantas más nuevas funcionalidades existen y más comunicados estamos entre nosotros, más aumenta nuestra superficie de ataque. Es decir, crecen las posibilidades y vías que tienen los ciberdelincuentes para conseguir sus objetivos. Es por eso que los sistemas de defensa y monitorización de seguridad deben evolucionar también. Porque en un mundo donde cada vez se impone más el teletrabajo y servicios en *Cloud* no basta con un *firewall* perimetral tradicional. Por este motivo, en este Experto Universitario se va a tratar también la importancia de idear una defensa multicapa, también conocida como "*Defense in Depth*", que cubra todos los aspectos de una red corporativa donde algunos de los conceptos y sistemas que se verán podrán ser utilizados y aplicados también en un ambiente doméstico.

La seguridad 100% no existe, pero si se conocen los tipos de ataques a los que se enfrenta, los riesgos a los que se está expuesto y se dispone de la información necesaria para hacerles frente, se hablará dado un paso importante y añadido una capa más de seguridad a la información.

Este **Experto Universitario en Ciberseguridad Defensiva** 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

Comienza a actuar con el conocimiento más amplio en los tipos de riesgo existentes en la actualidad y los medios de defensa aplicables en cada caso"

Un recorrido completo que te permitirá conocer cuáles son y cómo funcionan las ciberamenazas actuales como base para desarrollar estrategias defensivas"

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

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 programa académico. Para ello, contará con la ayuda de un novedoso sistema de vídeos interactivos realizados por reconocidos expertos.



02

Objetivos

Realizar este Experto Universitario permite avanzar de manera exponencial en 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.





Una completa puesta al día en todos los aspectos que la Ciberseguridad Defensiva ha desarrollado en los últimos tiempos"

Objetivos generales

- Evaluar la seguridad de los equipos de los usuarios y los servidores
- Examinar las posibles amenazas en función del entorno de uso
- Analizar las soluciones para cada amenaza
- Desarrollar políticas de uso apropiadas
- Analizar el marco general, la importancia de la defensa multicapa y los sistemas de monitorización
- Examinar los sistemas de detección y prevención de las amenazas más importantes
- Desarrollar soluciones *firewall* en *Host Linux* y proveedores *Cloud*
- Evaluar nuevos sistemas de detección de amenazas, así como su evolución respecto a soluciones más tradicionales
- Generar soluciones inteligentes completas para automatizar comportamientos ante incidentes
- Analizar las principales plataformas móviles actuales, características y uso de las mismas
- Examinar las vulnerabilidades y amenazas existentes, así como los principales vectores de ataque
- Evaluar los riesgos asociados a las vulnerabilidades tanto fuera como dentro de la empresa
- Determinar herramientas y guías de buenas prácticas para conseguir la protección de los dispositivos móviles
- Analizar el IoT en distintos ámbitos en la actualidad
- Examinar la evolución y el impacto del IoT
- Determinar las partes de un proyecto IoT
- Identificar, analizar y evaluar riesgos de seguridad de las partes del proyecto IoT





Objetivos específicos

Módulo 1. Seguridad en Host

- Concretar las políticas de *backup* de los datos de personales y profesionales
- Valorar las diferentes herramientas para dar soluciones a problemas específicos de seguridad
- Establecer mecanismos para tener un sistema actualizado
- Analizar el equipo para detectar intrusos
- Determinar las reglas de acceso al sistema
- Examinar y clasificar los correos para evitar fraudes
- Generar listas de software permitido

Módulo 2. Seguridad en Red (Perimetral)

- Analizar las arquitecturas actuales de red para identificar el perímetro que debemos proteger
- Desarrollar las configuraciones concretas de *firewall* y en *Linux* para mitigar los ataques más comunes
- Compilar las soluciones más usadas como *Snort* y *Suricata*, así como su configuración
- Examinar las diferentes capas adicionales que proporcionan los *firewalls* de nueva generación y funcionalidades de red en entornos *Cloud*
- Determinar las herramientas para la protección de la red y demostrar por qué son fundamentales para una defensa multicapa

Módulo 3. Seguridad en *Smartphones*

- Examinar los distintos vectores de ataque para evitar convertirse en un blanco fácil
- Determinar los principales ataques y tipos de *Malware* a los que se exponen los usuarios de dispositivos móviles
- Analizar los dispositivos más actuales para establecer una mayor seguridad en la configuración
- Concretar los pasos principales para realizar una prueba de penetración tanto en plataformas iOS como en plataformas android
- Desarrollar conocimiento especializado sobre las diferentes herramientas de protección y seguridad
- Establecer buenas prácticas en programación orientadas a dispositivos móviles

Módulo 4. Seguridad en IoT

- Analizar las principales arquitecturas de IoT
- Examinar las tecnologías de conectividad
- Desarrollar los protocolos de aplicación principales
- Concretar los diferentes tipos de dispositivos existentes
- Evaluar los niveles de riesgo y vulnerabilidades conocidas
- Desarrollar políticas de uso seguras
- Establecer las condiciones de uso apropiadas para estos dispositivos

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.





La visión directa de una profesión en constante movimiento, a través de profesionales expertos que te darán la visión más realista de este trabajo"

Dirección



Dña. Fernández Sapena, Sonia

- Formadora de Seguridad Informática y Hacking Ético. Centro de Referencia Nacional de Getafe en Informática y Telecomunicaciones. Madrid
- Instructora certificada E-Council. Madrid
- 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). Universidad de las Islas Baleares
- Ingeniera en Informática. Universidad de Alcalá de Henares. Madrid
- Máster en DevOps: Docker and Kubernetes. Cas-Training. Madrid
- Microsoft Azure Security Techonologies. E-Council. Madrid

Profesores

D. Catalá Barba, José Francisco

- Mando intermedio en el MINISDEF. Distintos cometidos y responsabilidades dentro del GOE III, tales como administración y gestión de incidencias de la red interna, realización de programas a medida para diferentes áreas, cursos de formación a los usuarios de la red y al personal del grupo en general
- Técnico electrónico en Factoría Ford sita en Almusafes, Valencia, programaciónde robots, PLC,s, reparación y mantenimiento
- Técnico Electrónico
- Desarrollador de aplicaciones para dispositivos móviles

D. Jiménez Ramos, Álvaro

- Analista de seguridad Senior en The Workshop
- Analista de ciberseguridad L1 en Axians
- Analista de ciberseguridad L2 en Axians
- Analista de ciberseguridad en SACYR S.A.
- Grado en Ingeniería Telemática por la Universidad Politécnica de Madrid
- Máster de Ciberseguridad y Hacking Ético por CICE
- Curso Superior de Ciberseguridad por Deusto Formación

Dña. Marcos Sbarbaro, Victoria Alicia

- Desarrolladora de Aplicaciones Móviles Android Nativas en B60. UK
- Analista Programadora para la gestión, coordinación y documentación de entorno virtualizado de alarmas de seguridad en cliente
- Analista Programadora de aplicaciones Java para cajeros automáticos en cliente
- Profesional del Desarrollo de Software para aplicación de validación de firma y gestión documental en cliente
- Técnico de Sistemas para la migración de equipos y para la gestión, mantenimiento y formación de dispositivos móviles PDAs en cliente
- Ingeniería Técnica de Informática de Sistemas. Universitat Oberta de Catalunya
- Máster en Seguridad Informática y Hacking Ético Oficial de EC- Council y CompTIA por la Escuela Profesional de Nuevas Tecnologías CICE

D. Peralta Alonso, Jon

- Abogado / DPO Altia Consultores S.A
- Docente en Máster en Protección de Datos Personales, Ciberseguridad y Derecho de las TIC. Universidad Pública del País Vasco (UPV-EHU)
- Abogado / Asesor jurídico. Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Asesor jurídico / Pasante. Despacho de profesional: Oscar Padura
- Grado en Derecho. Universidad Pública del País Vasco
- Máster en Delegado de Protección de Datos. EIS Innovative School
- Máster Universitario en Abogacía. Universidad Pública del País Vasco
- Máster Especialista en Práctica Procesal Civil. Universidad Internacional Isabel I de Castilla

04

Estructura y contenido

El temario de este programa recorre todos y cada uno de los campos de conocimiento que el profesional que interviene en ciberseguridad debe conocer en el ámbito de la acción defensiva. 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.





Todos los aspectos que el análisis y la intervención en ciberseguridad defensiva requiere, desarrollados de forma estructurada en un planteamiento de estudio centrado en la eficiencia"

Módulo 1. Seguridad en *Host*

1.1. Copias de seguridad
- 1.1.1. Estrategias para las copias de seguridad
- 1.1.2. Herramientas para Windows
- 1.1.3. Herramientas para Linux
- 1.1.4. Herramientas para MacOS

1.2. Antivirus de usuario
- 1.2.1. Tipos de antivirus
- 1.2.2. Antivirus para Windows
- 1.2.3. Antivirus para Linux
- 1.2.4. Antivirus para MacOS
- 1.2.5. Antivirus para smartphones

1.3. Detectores de intrusos - HIDS
- 1.3.1. Métodos de detección de intrusos
- 1.3.2. Sagan
- 1.3.3. Aide
- 1.3.4. *Rkhunter*

1.4. *Firewall* local
- 1.4.1. *Firewalls* para Windows
- 1.4.2. *Firewalls* para Linux
- 1.4.3. *Firewalls* para MacOS

1.5. Gestores de contraseñas
- 1.5.1. Password
- 1.5.2. *LastPass*
- 1.5.3. *KeePass*
- 1.5.4. *Sticky Password*
- 1.5.5. RoboForm

1.6. Detectores de *Phishing*
- 1.6.1. Detección del *phishing* de forma manual
- 1.6.2. Herramientas *antiphishing*

1.7. *Spyware*
- 1.7.1. Mecanismos de evitación
- 1.7.2. Herramientas *antispyware*

1.8. Rastreadores
- 1.8.1. Medidas para proteger el sistema
- 1.8.2. Herramientas anti-rastreadores

1.9. *EDR- End point Detection and Response*
- 1.9.1. Comportamiento del sistema EDR
- 1.9.2. Diferencias entre EDR y antivirus
- 1.9.3. El futuro de los sistemas EDR

1.10. Control sobre la instalación de software
- 1.10.1. Repositorios y tiendas de software
- 1.10.2. Listas de software permitido o prohibido
- 1.10.3. Criterios de actualizaciones
- 1.10.4. Privilegios para instalar software

Módulo 2. Seguridad En Red (Perimetral)

2.1. Sistemas de detección y prevención de amenazas
- 2.1.1. Marco general de los incidentes de seguridad
- 2.1.2. Sistemas de defensa actuales: *defense in depth* y SOC
- 2.1.3. Arquitecturas de redes actuales
- 2.1.4. Tipos de herramientas para la detección y prevención de incidentes
  - 2.1.4.1. Sistemas basados en red
  - 2.1.4.2. Sistemas basados en *host*
  - 2.1.4.3. Sistemas centralizados
- 2.1.5. Comunicación y detección de instancias/*Hosts*, contenedores y *serverless*

2.2. *Firewall*
- 2.2.1. Tipos de *Firewalls*
- 2.2.2. Ataques y mitigación
- 2.2.3. *Firewalls* comunes en *kernel* Linux
  - 2.2.3.1. UFW
  - 2.2.3.2. Nftables e iptables
  - 2.2.3.3. *Firewalld*
- 2.2.4. Sistemas de detección basados en *logs* del sistema
  - 2.2.4.1. TCP *wrappers*
  - 2.2.4.2. *BlockHosts* y *DenyHosts*
  - 2.2.4.3. Fail2Ban

2.3. Sistemas de detección y prevención de intrusiones (IDS/IPS)
- 2.3.1. Ataques sobre IDS/IPS
- 2.3.2. Sistemas de IDS/IPS
  - 2.3.2.1. *Snort*
  - 2.3.2.2. Suricata

2.4. *Firewalls* de siguiente generación (NGFW)
- 2.4.1. Diferencias entre NGFW y *Firewall* tradicional
- 2.4.2. Capacidades principales
- 2.4.3. Soluciones comerciales
- 2.4.4. *Firewalls* para servicios de *Cloud*
  - 2.4.4.1. Arquirtectura Cloud VPC
  - 2.4.4.2. *Cloud* ACLs
  - 2.4.4.3. *Security Group*

2.5. *Proxy*
- 2.5.1. Tipos de *Proxy*
- 2.5.2. Uso de *Proxy*. Ventajas e inconvenientes

2.6. Motores de antivirus
- 2.6.1. Contexto general del *Malware* e IOCs
- 2.6.2. Problemas de los motores de antivirus

2.7. Sistemas de protección de correo
- 2.7.1. Antispam
  - 2.7.1.1. Listas blancas y negras
  - 2.7.1.2. Filtros bayesianos
- 2.7.2. *Mail Gateway* (MGW)

2.8. SIEM.
- 2.8.1. Componentes y arquitectura
- 2.8.2. Reglas de correlación y casos de uso
- 2.8.3. Retos actuales de los sistemas SIEM

2.9. SOAR
- 2.9.1. SOAR y SIEM: enemigos o aliados
- 2.9.2. El futuro de los sistemas SOAR

2.10. Otros Sistemas basados en red
- 2.10.1. WAF
- 2.10.2. NAC
- 2.10.3. *HoneyPots* y *HoneyNets*
- 2.10.4. CASB

Módulo 3. Seguridad en Smartphones

3.1. El mundo del dispositivo móvil
- 3.1.1. Tipos de plataformas móviles
- 3.1.2. Dispositivos IOS
- 3.1.3. Dispositivos android

3.2. Gestión de la seguridad móvil
- 3.2.1. Proyecto de Seguridad móvil OWASP
  - 3.2.1.1. Top 10 vulnerabilidades
- 3.2.2. Comunicaciones, redes y modos de conexión

3.3. El Dispositivo Móvil en el entorno Empresarial
- 3.3.1. Riesgos
- 3.3.2. Políticas de seguridad
- 3.3.3. Monitorización de dispositivos
- 3.3.4. Gestión de dispositivos móviles (MDM)

3.4. Privacidad del Usuario y seguridad de los datos
- 3.4.1. Estados de la información
- 3.4.2. Protección y confidencialidad de los datos
  - 3.4.2.1. Permisos
  - 3.4.2.2. Encriptación
- 3.4.3. Almacenamiento seguro de los datos
  - 3.4.3.1. Almacenamiento seguro en iOS
  - 3.4.3.2. Almacenamiento seguro en android
- 3.4.4. Buenas prácticas en el desarrollo de aplicaciones

3.5. Vulnerabilidades y vectores de ataque
- 3.5.1. Vulnerabilidades
- 3.5.2. Vectores de ataque
  - 3.5.2.1. *Malware*
  - 3.5.2.2. Exfiltración de datos
  - 3.5.2.3. Manipulación de los datos

3.6. Principales amenazas
- 3.6.1. Usuario no forzado
- 3.6.2. *Malware*
  - 3.6.2.1. Tipos de *Malware*
- 3.6.3. Ingeniería social
- 3.6.4. Fuga de datos
- 3.6.5. Robo de información
- 3.6.6. Redes WiFi no seguras
- 3.6.7. Software desactualizado
- 3.6.8. Aplicaciones maliciosas
- 3.6.9. Contraseñas poco seguras
- 3.6.10. Configuración débil o inexistente de seguridad
- 3.6.11. Acceso físico
- 3.6.12. Pérdida o robo del dispositivo
- 3.6.13. Suplantación de identidad (Integridad)
- 3.6.14. Criptografía débil o rota
- 3.6.15. Denegación de servicio (DoS)

3.7. Principales ataques
- 3.7.1. Ataques de *phishing*
- 3.7.2. Ataques relacionados con los modos de comunicación
- 3.7.3. Ataques de *Smishing*
- 3.7.4. Ataques de *Criptojacking*
- 3.7.5. *Man in The Middle*

3.8. *Hacking*
- 3.8.1. *Rooting* y *Jailbreaking*
- 3.8.2. Anatomía de un ataque móvil
  - 3.8.2.1. Propagación de la amenaza
  - 3.8.2.2. Instalación de *Malware* en el dispositivo
  - 3.8.2.3. Persistencia
  - 3.8.2.4. Ejecución del *payload* y extracción de la información
- 3.8.3. Hacking en dispositivos IOS: mecanismos y herramientas
- 3.8.4. Hacking en dispositivos android: mecanismos y herramientas

3.9. Pruebas de penetración
- 3.9.1. IOS *Pentesting*
- 3.9.2. Android *Pentesting*
- 3.9.3. Herramientas

3.10. Protección y seguridad
- 3.10.1. Configuración de seguridad
  - 3.10.1.1. En dispositivos iOS
  - 3.10.1.2. En dispositvos android
- 3.10.2. Medidas de seguridad
- 3.10.3. Herramientas de protección

Módulo 4. Seguridad en IoT

4.1. Dispositivos
- 4.1.1. Tipos de dispositivos
- 4.1.2. Arquitecturas estandarizadas
  - 4.1.2.1. OneM2M
  - 4.1.2.2. IoTWF
- 4.1.3. Protocolos de aplicación
- 4.1.4. Tecnologías de conectividad

4.2. Dispositivos IoT. Áreas de aplicación
- 4.2.1. SmartHome
- 4.2.2. SmartCity
- 4.2.3. Transportes
- 4.2.4. *Wearables*
- 4.2.5. Sector salud
- 4.2.6. IIoT

4.3. Protocolos de comunicación
- 4.3.1. MQTT
- 4.3.2. LWM2M
- 4.3.3. OMA-DM
- 4.3.4. TR-069

4.4. SmartHome
- 4.4.1. Domótica
- 4.4.2. Redes
- 4.4.3. Electrodomésticos
- 4.4.4. Vigilancia y seguridad



4.5. SmartCity
- 4.5.1. Iluminación
- 4.5.2. Meteorología
- 4.5.3. Seguridad

4.6. Transportes
- 4.6.1. Localización
- 4.6.2. Realización de pagos y obtención de servicios
- 4.6.3. Conectividad

4.7. Wearables
- 4.7.1. Ropa inteligente
- 4.7.2. Joyas inteligentes
- 4.7.3. Relojes inteligentes

4.8. Sector Salud
- 4.8.1. Monitorización de ejercicio/ritmo cardiaco
- 4.8.2. Monitorización de pacientes y personas mayores
- 4.8.3. Implantables
- 4.8.4. Robots quirúrgicos

4.9. Conectividad
- 4.9.1. WiFi
- 4.9.2. Bluetooth
- 4.9.3. Conectividad incorporada

4.10. Securización
- 4.10.1. Redes dedicadas
- 4.10.2. Gestor de contraseñas
- 4.10.3. Uso de protocolos cifrados
- 4.10.4. Consejos de uso

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.

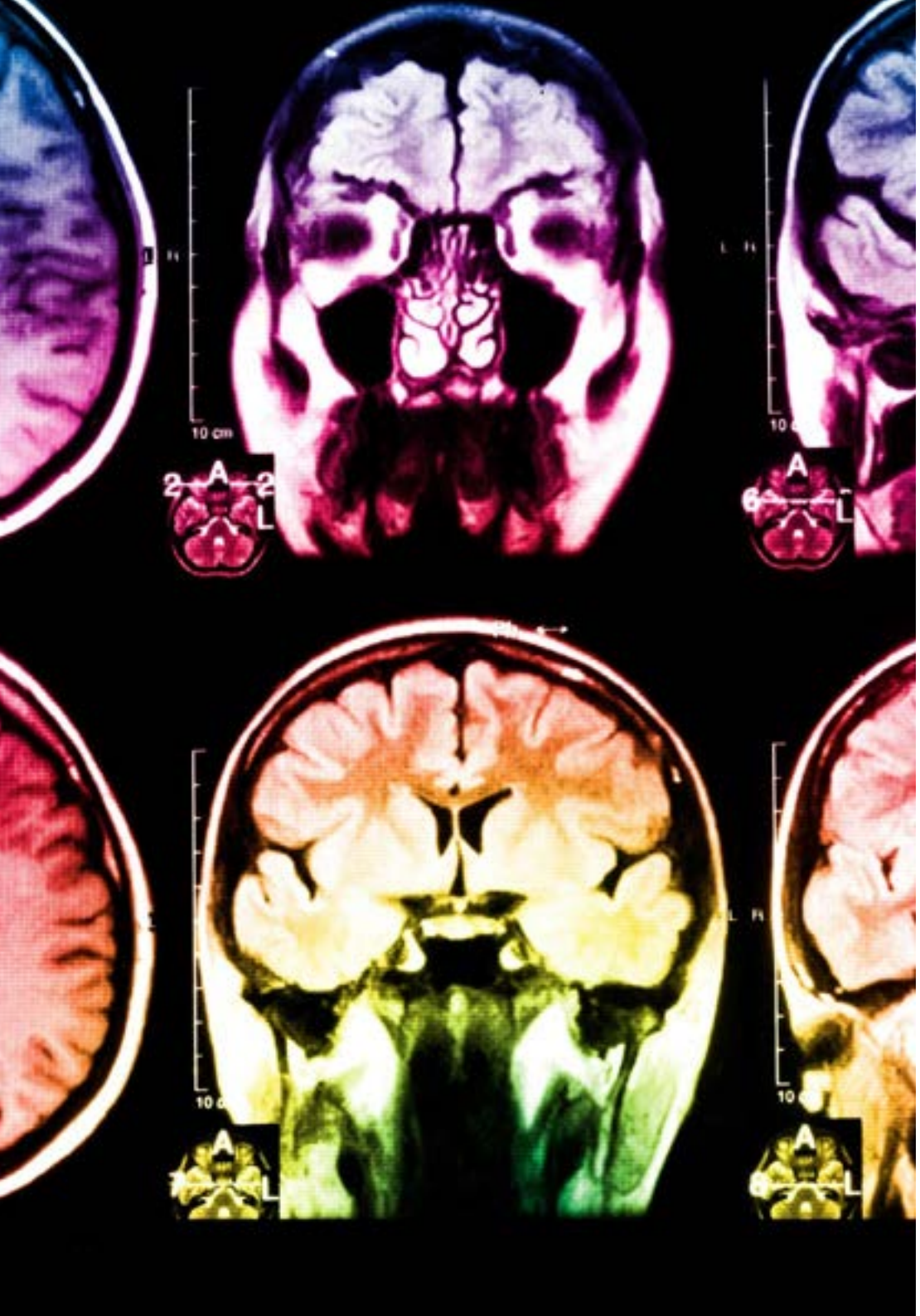
Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el Relearning.

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.

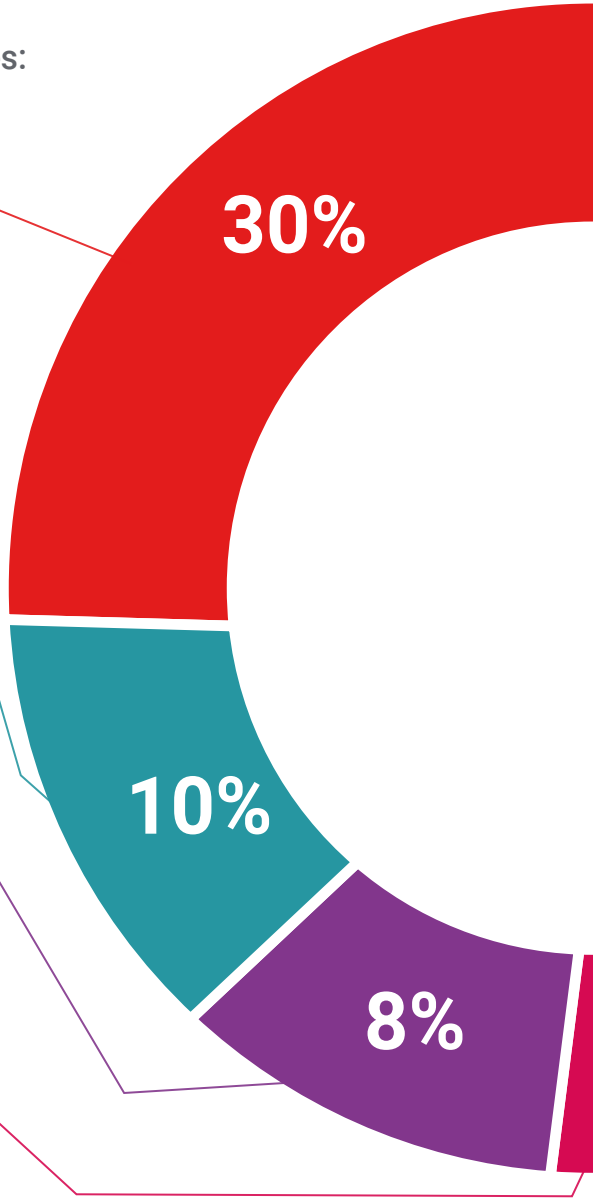
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

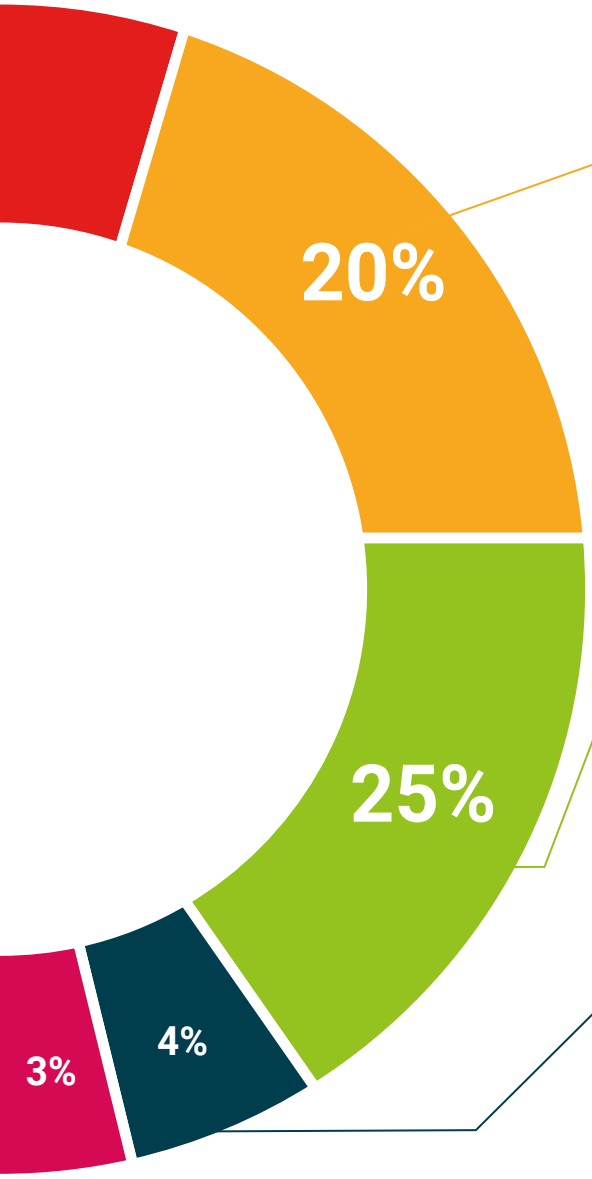
Prácticas de habilidades y competencias

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 Ciberseguridad Defensiva 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 Ciberseguridad Defensiva** contiene el programa educativo 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 Ciberseguridad Defensiva**

N.º Horas Oficiales: **600 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

Ciberseguridad Defensiva

Se trata de un título propio de esta Universidad con una duración de 600 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
Ciberseguridad Defensiva

Modalidad: **Online**
Duración: **6 meses**
Titulación: **TECH Universidad Tecnológica**
Horas lectivas: **600 h.**

Experto Universitario
Ciberseguridad Defensiva



tech universidad tecnológica