Experto Universitario
Ciberseguridad Defensiva

tech universidad

tech universidad

Experto Universitario
Ciberseguridad Defensiva

- Modalidad: **No escolarizada (100% en línea)**
- Duración: **6 meses**
- Titulación: **TECH Universidad**
- Horario: **a tu ritmo**
- Exámenes: **online**

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

Índice

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 insustituibles 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 te 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 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 veremos podrán ser utilizados y aplicados también en un ambiente doméstico.

Como gran añadido al temario, el programa también ofrece al alumno lecciones extra en Ciberseguridad. Se trata de *Masterclasses* elaboradas por un docente de gran relevancia internacional, especialista en Inteligencia, Ciberseguridad y Tecnologías Disruptivas. Así, el profesional informático profundizará en los aspectos fundamentales de la Ciberseguridad Defensiva, como los antivirus, los firewalls o los detectores de intrusos (HIDS).

La seguridad 100% no existe, pero si conocemos los tipos de ataques a los que nos enfrentamos, los riesgos a los que estamos expuestos y disponemos de la información necesaria para hacerles frente, habremos dado un paso importante y añadido una capa más de seguridad a nuestra 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

¿Quieres especializarte en Ciberseguridad Defensiva? Lo conseguirás gracias a las Masterclasses diseñadas por un especialista en Inteligencia, Ciberseguridad y Tecnologías Disruptivas"

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 curso académico. Para ello, contará con la ayuda de un novedoso sistema de vídeo interactivo realizado 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 curso 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"

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

Profesores

Dña. Marcos Sbarbaro, Victoria Alicia

- Desarrolladora de Aplicaciones Móviles Android Nativas en B60. UK
- Analista Programadora para la Gestión, Coordinación y Documentación del Entorno Virtualizado de Alarmas de Seguridad
- Analista Programadora de Aplicaciones Java para cajeros automáticos
- Profesional del Desarrollo de Software para Aplicación de Validación de Firma y Gestión Documental
- Técnico de Sistemas para la Migración de Equipos y para la Gestión, Mantenimiento y Formación de Dispositivos Móviles PDA
- Ingeniero Técnico de Informática de Sistemas por la Universidad Oberta de Cataluña
- 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

- Consultor Sénior de Protección de Datos y Ciberseguridad en Altia
- Abogado / Asesor jurídico en Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- Asesor Jurídico / Pasante en Despacho Profesional: Óscar Padura
- Grado en Derecho por la Universidad Pública del País Vasco
- Máster en Delegado de Protección de Datos por EIS Innovative School
- Máster Universitario en Abogacía por la Universidad Pública del País Vasco
- Máster Especialista en Práctica Procesal Civil por la Universidad Internacional Isabel I de Castilla
- Docente en Máster en Protección de Datos Personales, Ciberseguridad y Derecho de las TIC

D. Catalá Barba, José Francisco

- Técnico Electrónico Experto en Ciberseguridad
- Desarrollador de Aplicaciones para Dispositivos Móviles
- Técnico Electrónico en Mando Intermedio en el Ministerio de la Defensa de España
- Técnico Electrónico en Factoría Ford Sita en Valencia

D. Jiménez Ramos, Álvaro

- Analista de Ciberseguridad
- Analista de Seguridad Sénior 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

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

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 red 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. Fai2ban

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. Arquitectura 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 dispositivos 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/Gateway
- 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 de estudio

TECH es la primera universidad en el mundo que combina la metodología de los ***case studies*** con el ***Relearning***, un sistema de aprendizaje 100% online basado en la reiteración dirigida.

Esta disruptiva estrategia pedagógica ha sido concebida para ofrecer a los profesionales la oportunidad de actualizar conocimientos y desarrollar competencias de un modo intensivo y riguroso. Un modelo de aprendizaje que coloca al estudiante en el centro del proceso académico y le otorga todo el protagonismo, adaptándose a sus necesidades y dejando de lado las metodologías más convencionales.

TECH te prepara para afrontar nuevos retos en entornos inciertos y lograr el éxito en tu carrera"

El alumno: la prioridad de todos los programas de TECH

En la metodología de estudios de TECH el alumno es el protagonista absoluto. Las herramientas pedagógicas de cada programa han sido seleccionadas teniendo en cuenta las demandas de tiempo, disponibilidad y rigor académico que, a día de hoy, no solo exigen los estudiantes sino los puestos más competitivos del mercado.

Con el modelo educativo asincrónico de TECH, es el alumno quien elige el tiempo que destina al estudio, cómo decide establecer sus rutinas y todo ello desde la comodidad del dispositivo electrónico de su preferencia. El alumno no tendrá que asistir a clases en vivo, a las que muchas veces no podrá acudir. Las actividades de aprendizaje las realizará cuando le venga bien. Siempre podrá decidir cuándo y desde dónde estudiar.

"En TECH NO tendrás clases en directo (a las que luego nunca puedes asistir)"

Los planes de estudios más exhaustivos a nivel internacional

TECH se caracteriza por ofrecer los itinerarios académicos más completos del entorno universitario. Esta exhaustividad se logra a través de la creación de temarios que no solo abarcan los conocimientos esenciales, sino también las innovaciones más recientes en cada área.

Al estar en constante actualización, estos programas permiten que los estudiantes se mantengan al día con los cambios del mercado y adquieran las habilidades más valoradas por los empleadores. De esta manera, quienes finalizan sus estudios en TECH reciben una preparación integral que les proporciona una ventaja competitiva notable para avanzar en sus carreras.

Y además, podrán hacerlo desde cualquier dispositivo, pc, tableta o smartphone.

El modelo de TECH es asincrónico, de modo que te permite estudiar con tu pc, tableta o tu smartphone donde quieras, cuando quieras y durante el tiempo que quieras”

Case studies o Método del caso

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de negocios del mundo. Desarrollado en 1912 para que los estudiantes de Derecho no solo aprendiesen las leyes a base de contenidos teóricos, su función era también presentarles situaciones complejas reales. Así, podían tomar decisiones y emitir juicios de valor fundamentados sobre cómo resolverlas. En 1924 se estableció como método estándar de enseñanza en Harvard.

Con este modelo de enseñanza es el propio alumno quien va construyendo su competencia profesional a través de estrategias como el *Learning by doing* o el *Design Thinking*, utilizadas por otras instituciones de renombre como Yale o Stanford.

Este método, orientado a la acción, será aplicado a lo largo de todo el itinerario académico que el alumno emprenda junto a TECH. De ese modo se enfrentará a múltiples situaciones reales y deberá integrar conocimientos, investigar, argumentar y defender sus ideas y decisiones. Todo ello con la premisa de responder al cuestionamiento de cómo actuaría al posicionarse frente a eventos específicos de complejidad en su labor cotidiana.

Método *Relearning*

En TECH los *case studies* son potenciados con el mejor método de enseñanza 100% online: el *Relearning*.

Este método rompe con las técnicas tradicionales de enseñanza para poner al alumno en el centro de la ecuación, proveyéndole del mejor contenido en diferentes formatos. De esta forma, consigue repasar y reiterar los conceptos clave de cada materia y aprender a aplicarlos en un entorno real.

En esta misma línea, y de acuerdo a múltiples investigaciones científicas, la reiteración es la mejor manera de aprender. Por eso, TECH ofrece entre 8 y 16 repeticiones de cada concepto clave dentro de una misma lección, presentada de una manera diferente, con el objetivo de asegurar que el conocimiento sea completamente afianzado durante el proceso de estudio.

El Relearning te permitirá aprender con menos esfuerzo y más rendimiento, implicándote más en tu especialización, desarrollando el espíritu crítico, la defensa de argumentos y el contraste de opiniones: una ecuación directa al éxito.

Un Campus Virtual 100% online con los mejores recursos didácticos

Para aplicar su metodología de forma eficaz, TECH se centra en proveer a los egresados de materiales didácticos en diferentes formatos: textos, vídeos interactivos, ilustraciones y mapas de conocimiento, entre otros. Todos ellos, diseñados por profesores cualificados que centran el trabajo en combinar casos reales con la resolución de situaciones complejas mediante simulación, el estudio de contextos aplicados a cada carrera profesional y el aprendizaje basado en la reiteración, a través de audios, presentaciones, animaciones, imágenes, etc.

Y es que las últimas evidencias científicas en el ámbito de las Neurociencias apuntan a la importancia de tener en cuenta el lugar y el contexto donde se accede a los contenidos antes de iniciar un nuevo aprendizaje. Poder ajustar esas variables de una manera personalizada favorece que las personas puedan recordar y almacenar en el hipocampo los conocimientos para retenerlos a largo plazo. Se trata de un modelo denominado *Neurocognitive context-dependent e-learning* que es aplicado de manera consciente en esta titulación universitaria.

Por otro lado, también en aras de favorecer al máximo el contacto mentor-alumno, se proporciona un amplio abanico de posibilidades de comunicación, tanto en tiempo real como en diferido (mensajería interna, foros de discusión, servicio de atención telefónica, email de contacto con secretaría técnica, chat y videoconferencia).

Asimismo, este completísimo Campus Virtual permitirá que el alumnado de TECH organice sus horarios de estudio de acuerdo con su disponibilidad personal o sus obligaciones laborales. De esa manera tendrá un control global de los contenidos académicos y sus herramientas didácticas, puestas en función de su acelerada actualización profesional.

> *La modalidad de estudios online de este programa te permitirá organizar tu tiempo y tu ritmo de aprendizaje, adaptándolo a tus horarios"*

La eficacia del método se justifica con cuatro logros fundamentales:

1. Los alumnos que siguen este método no solo consiguen la asimilación de conceptos, sino un desarrollo de su capacidad mental, mediante ejercicios de evaluación de situaciones reales y aplicación de conocimientos.
2. El aprendizaje se concreta de una manera sólida en capacidades prácticas que permiten al alumno una mejor integración en el mundo real.
3. Se consigue una asimilación más sencilla y eficiente de las ideas y conceptos, gracias al planteamiento de situaciones que han surgido de la realidad.
4. La sensación de eficiencia del esfuerzo invertido se convierte en un estímulo muy importante para el alumnado, que se traduce en un interés mayor en los aprendizajes y un incremento del tiempo dedicado a trabajar en el curso.

La metodología universitaria mejor valorada por sus alumnos

Los resultados de este innovador modelo académico son constatables en los niveles de satisfacción global de los egresados de TECH.

La valoración de los estudiantes sobre la calidad docente, calidad de los materiales, estructura del curso y sus objetivos es excelente. No en valde, la institución se convirtió en la universidad mejor valorada por sus alumnos en la plataforma de reseñas Trustpilot, obteniendo un 4,9 de 5.

Accede a los contenidos de estudio desde cualquier dispositivo con conexión a Internet (ordenador, tablet, smartphone) gracias a que TECH está al día de la vanguardia tecnológica y pedagógica.

Podrás aprender con las ventajas del acceso a entornos simulados de aprendizaje y el planteamiento de aprendizaje por observación, esto es, Learning from an expert.

Así, en este programa estarán disponibles los mejores materiales educativos, preparados a conciencia:

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 que creará nuestra manera de trabajo online, con las técnicas más novedosas que nos permiten ofrecerte una gran calidad, en cada una de las piezas que pondremos a tu servicio.

Prácticas de habilidades y competencias

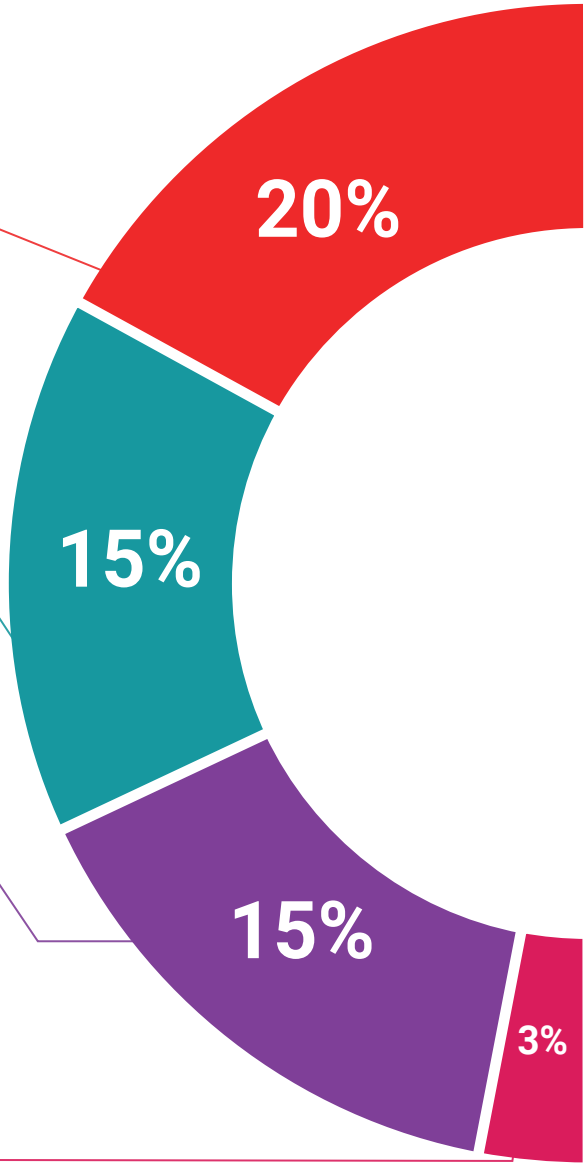
Realizarás actividades de desarrollo de competencias y habilidades específicas en cada área temática. Prácticas y dinámicas para adquirir y desarrollar las destrezas y habilidades que un especialista precisa desarrollar en el marco de la globalización que vivimos.

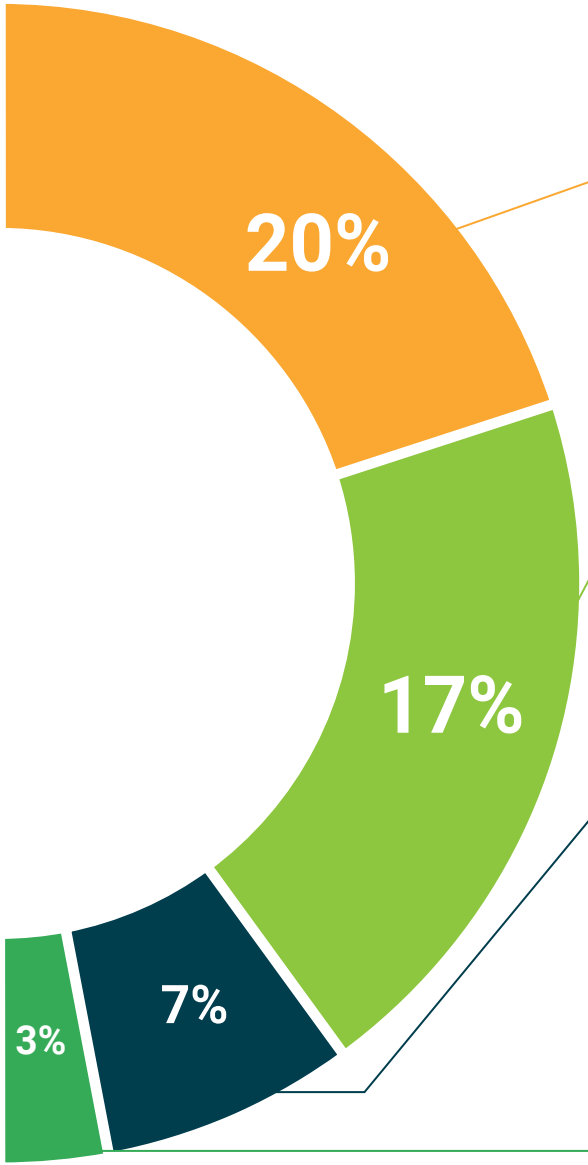
Resúmenes interactivos

Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.
Este sistema exclusivo educativo para la presentación de contenidos multimedia fue premiado por Microsoft como "Caso de éxito en Europa".

Lecturas complementarias

Artículos recientes, documentos de consenso, guías internacionales... En nuestra biblioteca virtual tendrás acceso a todo lo que necesitas para completar tu capacitación.





Case Studies

Completarás una selección de los mejores *case studies* de la materia. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.

Testing & Retesting

Evaluamos y reevaluamos periódicamente tu conocimiento a lo largo del programa. Lo hacemos sobre 3 de los 4 niveles de la Pirámide de Miller.

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 nuestras futuras decisiones difíciles.

Guías rápidas de actuación

TECH ofrece los contenidos más relevantes del curso en forma de fichas o guías rápidas de actuación. Una manera sintética, práctica y eficaz de ayudar al estudiante a progresar en su aprendizaje.

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.

Supera con éxito este programa y recibe tu titulación universitaria sin desplazamientos ni farragosos trámites"

Este **Experto Universitario en Ciberseguridad Defensiva** 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.**

Este título expedido por **TECH Universidad** 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**

Modalidad: **No escolarizada (100% en línea)**

Duración: **6 meses**


tech universidad

C. _____, con documento de identificación _____ ha superado con éxito y obtenido el título 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.

En Ciudad de México, a 31 de mayo de 2024

Mtro. Gerardo Daniel Orozco Martínez
Rector

código único TECH: AFWDR23S 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 Universidad realizará las gestiones oportunas para su obtención, con un coste adicional.

tech universidad

Experto Universitario
Ciberseguridad Defensiva

- Modalidad: **No escolarizada (100% en línea)**
- Duración: **6 meses**
- Titulación: **TECH Universidad**
- Horario: **a tu ritmo**
- Exámenes: **online**

Experto Universitario
Ciberseguridad Defensiva

tech universidad