Maestría Oficial Universitaria
Seguridad Informática

Nº de RVOE: 20230354

RVOE
EDUCACIÓN SUPERIOR

tech
universidad

tech universidad

Nº de RVOE: 20230354

Maestría Oficial Universitaria
Seguridad Informática

Idioma: **Español**
Modalidad: **100% online**
Duración: **20 meses**
Fecha de vigencia RVOE: **13/02/2023**
Acceso web: www.techtitute.com/mx/informatica/maestria-universitaria/maestria-universitaria-seguridad-informatica

Índice

01

Presentación del programa

La Seguridad Informática es esencial en la era digital actual, dada la creciente dependencia de los sistemas informáticos y la masificación de Internet. Además, ante el considerable aumento de ciberataques y amenazas complejas, cada vez más organizaciones demandan la incorporación de expertos capaces de diseñar e implementar soluciones robustas para garantizar la protección de datos confidenciales. Para aprovechar estas oportunidades laborales, los expertos necesitan obtener una ventaja competitiva que los diferencie del resto de candidatos. Con esta idea en mente, TECH lanza un innovador programa universitario que brindará al alumnado las últimas tendencias en Ciberseguridad. A su vez, se imparte en una cómoda modalidad 100% online que se adapta a los horarios de los profesionales.

Este es el momento, te estábamos esperando

Con esta Maestría Oficial Universitaria completamente online, dominarás las técnicas de Seguridad Informática más modernas para prevenir una variedad de ciberataques"

De acuerdo con un reciente informe elaborado por la Organización Internacional de Normalización, el 45% de las empresas a escala global sufren incidentes relacionados con la Ciberseguridad. Este hecho pone de manifiesto la creciente vulnerabilidad de los sistemas digitales. Por eso, es fundamental que los informáticos manejen las medidas de seguridad más avanzadas para prevenir riesgos potenciales como el *ransomware*, *phishing* o ataques de denegación de servicio. Solamente así, los expertos podrán fortalecer la infraestructura tecnológica de las instituciones y minimizar el impacto de amenazas digitales.

En este contexto, TECH presenta una revolucionaria Maestría Oficial Universitaria en Seguridad Informática. Así, el plan de estudios ahondará en cuestiones que abarcan desde la implementación de capas de seguridad o metodologías de evaluación de sistemas hasta la realización de auditorías sobre el funcionamiento de la protección de datos. En esta misma línea, los materiales didácticos brindarán a los alumnos múltiples estrategias para manejar técnicas de encriptación, seguridad en redes y protección en entornos de nube. De esta forma, los egresados adquirirán competencias avanzadas para evaluar, identificar y mitigar riesgos de seguridad, aplicando soluciones efectivas para la protección de informaciones sensibles.

Por otra parte, en cuanto a la metodología de la titulación, TECH ofrece un entorno académico totalmente online, adaptado a las necesidades de los profesionales ocupados que quieren avanzar en sus carreras. Además, emplea su disruptivo método del *Relearning*, basado en la repetición de conceptos clave para fijar conocimientos de forma progresiva y natural. En esta misma línea, lo único que necesitarán los egresados es tener a su alcance un dispositivo electrónico con conexión a internet para acceder al Campus Virtual. En esta plataforma encontrarán una biblioteca llena de recursos multimedia de apoyo como lecturas especializadas, vídeos explicativos, infografías o resúmenes interactivos.

Dispondrás de una comprensión integral sobre las regulaciones vigentes en materia de Protección de Datos, lo que garantizará que mantengas altos estándares éticos durante el ejercicio de tu labor”

02

¿Por qué estudiar en TECH?

TECH es la mayor Universidad digital del mundo. Con un impresionante catálogo de más de 14.000 programas universitarios, disponibles en 11 idiomas, se posiciona como líder en empleabilidad, con una tasa de inserción laboral del 99%. Además, cuenta con un enorme claustro de más de 6.000 profesores de máximo prestigio internacional.

Te damos +

Estudia en la mayor universidad digital del mundo y asegura tu éxito profesional. El futuro empieza en TECH”

La mejor universidad online del mundo según FORBES

La prestigiosa revista Forbes, especializada en negocios y finanzas, ha destacado a TECH como «la mejor universidad online del mundo». Así lo han hecho constar recientemente en un artículo de su edición digital en el que se hacen eco del caso de éxito de esta institución, «gracias a la oferta académica que ofrece, la selección de su personal docente, y un método de aprendizaje innovador orientado a formar a los profesionales del futuro».

El mejor claustro docente top internacional

El claustro docente de TECH está integrado por más de 6.000 profesores de máximo prestigio internacional. Catedráticos, investigadores y altos ejecutivos de multinacionales, entre los cuales se destacan Isaiah Covington, entrenador de rendimiento de los Boston Celtics; Magda Romanska, investigadora principal de MetaLAB de Harvard; Ignacio Wistumba, presidente del departamento de patología molecular traslacional del MD Anderson Cancer Center; o D.W Pine, director creativo de la revista TIME, entre otros.

La mayor universidad digital del mundo

TECH es la mayor universidad digital del mundo. Somos la mayor institución educativa, con el mejor y más amplio catálogo educativo digital, cien por cien online y abarcando la gran mayoría de áreas de conocimiento. Ofrecemos el mayor número de titulaciones propias, titulaciones oficiales de posgrado y de grado universitario del mundo. En total, más de 14.000 títulos universitarios, en once idiomas distintos, que nos convierten en la mayor institución educativa del mundo.

Los planes de estudio más completos del panorama universitario

TECH ofrece los planes de estudio más completos del panorama universitario, con temarios que abarcan conceptos fundamentales y, al mismo tiempo, los principales avances científicos en sus áreas científicas específicas. Asimismo, estos programas son actualizados continuamente para garantizar al alumnado la vanguardia académica y las competencias profesionales más demandadas. De esta forma, los títulos de la universidad proporcionan a sus egresados una significativa ventaja para impulsar sus carreras hacia el éxito.

Un método de aprendizaje único

TECH es la primera universidad que emplea el *Relearning* en todas sus titulaciones. Se trata de la mejor metodología de aprendizaje online, acreditada con certificaciones internacionales de calidad docente, dispuestas por agencias educativas de prestigio. Además, este disruptivo modelo académico se complementa con el "Método del Caso", configurando así una estrategia de docencia online única. También en ella se implementan recursos didácticos innovadores entre los que destacan vídeos en detalle, infografías y resúmenes interactivos.

La universidad online oficial de la NBA

TECH es la universidad online oficial de la NBA. Gracias a un acuerdo con la mayor liga de baloncesto, ofrece a sus alumnos programas universitarios exclusivos, así como una gran variedad de recursos educativos centrados en el negocio de la liga y otras áreas de la industria del deporte. Cada programa tiene un currículo de diseño único y cuenta con oradores invitados de excepción: profesionales con una distinguida trayectoria deportiva que ofrecerán su experiencia en los temas más relevantes.

Líderes en empleabilidad

TECH ha conseguido convertirse en la universidad líder en empleabilidad. El 99% de sus alumnos obtienen trabajo en el campo académico que ha estudiado, antes de completar un año luego de finalizar cualquiera de los programas de la universidad. Una cifra similar consigue mejorar su carrera profesional de forma inmediata. Todo ello gracias a una metodología de estudio que basa su eficacia en la adquisición de competencias prácticas, totalmente necesarias para el desarrollo profesional.

Google Partner Premier

El gigante tecnológico norteamericano ha otorgado a TECH la insignia Google Partner Premier. Este galardón, solo al alcance del 3% de las empresas del mundo, pone en valor la experiencia eficaz, flexible y adaptada que esta universidad proporciona al alumno. El reconocimiento no solo acredita el máximo rigor, rendimiento e inversión en las infraestructuras digitales de TECH, sino que también sitúa a esta universidad como una de las compañías tecnológicas más punteras del mundo.

La universidad mejor valorada por sus alumnos

La web de valoraciones Trustpilot ha posicionado a TECH como la universidad mejor valorada del mundo por sus alumnos. Este portal de reseñas, el más fiable y prestigioso porque verifica y valida la autenticidad de cada opinión publicada, ha concedido a TECH su calificación más alta, 4,9 sobre 5, atendiendo a más de 1.000 reseñas recibidas. Unas cifras que sitúan a TECH como la referencia universitaria absoluta a nivel internacional.

03

Plan de estudios

El plan de estudios de esta Maestría Oficial Universitaria en Seguridad Informática está diseñado para ofrecer una especialización holística en Ciberseguridad. A lo largo del programa, los alumnos dominarán herramientas avanzadas para proteger sistemas y datos, gestionar riesgos cibernéticos y prevenir amenazas. En este sentido, los materiales didácticos ofrecerán a los alumnos las claves para implementar técnicas sofisticadas de cifrado, análisis forense y seguridad en entornos *cloud*. De esta forma, los profesionales adquirirán habilidades estratégicas para abordar con éxito los retos más complejos en el panorama digital actual.

Un temario completo y bien desarrollado

Ahondarás en la identificación, clasificación y mitigación de riesgos, incluyendo vulnerabilidades como malware”

Gracias a su modalidad 100% online, esta titulación universitaria permite a los profesionales estudiar de manera flexible y a su propio ritmo, combinando teoría con ejercicios prácticos, recursos interactivos, vídeos, clases magistrales y material complementario que refuerzan el proceso educativo. De este modo, el plan de estudios proporciona al alumnado las herramientas necesarias para convertirse en expertos en Seguridad Informática, listos para enfrentar los retos y desafíos de un sector en constante evolución.

Accederás a un sistema de aprendizaje basado en la reiteración natural de conceptos fundamentales, lo que te permitirá incrementar tus conocimientos de manera progresiva. ¡Olvídate de invertir largas horas al estudio!"

Dónde, cuándo y cómo se imparte

Esta Maestría Oficial Universitaria se ofrece 100% online, por lo que el alumno podrá cursarlo desde cualquier sitio, haciendo uso de una computadora, una tableta o simplemente mediante su *smartphone*. Además, podrá acceder a los contenidos de manera offline, bastando con descargarse los contenidos de los temas elegidos en el dispositivo y abordarlos sin necesidad de estar conectado a Internet. Una modalidad de estudio autodirigida y asincrónica que pone al estudiante en el centro del proceso académico, gracias a un formato metodológico ideado para que pueda aprovechar al máximo su tiempo y optimizar el aprendizaje.

En esta Maestría con RVOE, el alumnado dispondrá de 10 asignaturas que podrá abordar y analizar a lo largo de 20 meses de estudio.

Asignatura 1	Inteligencia y Seguridad Informática
Asignatura 2	Seguridad en el alojamiento
Asignatura 3	Seguridad en red perimetral
Asignatura 4	Seguridad en Teléfonos Inteligentes
Asignatura 5	Seguridad en Internet de las Cosas
Asignatura 6	Hackeo Ético
Asignatura 7	Ingeniería Inversa
Asignatura 8	Desarrollo seguro
Asignatura 9	Análisis Forense
Asignatura 10	Retos actuales y futuros en Seguridad Informática

Los contenidos académicos de este programa abarcan también los siguientes temas y subtemas:

Asignatura 1. Inteligencia y Seguridad Informática

1.1. Inteligencia Informática
- 1.1.1. Inteligencia informática
  - 1.1.1.1. La Inteligencia
    - 1.1.1.1.1. Ciclo de Inteligencia
  - 1.1.1.2. Inteligencia y seguridad informática
- 1.1.2. El Analista de Inteligencia
  - 1.1.2.1. El rol del Analista de Inteligencia
  - 1.1.2.2. Los sesgos del Analista de Inteligencia en la actividad evaluativa

1.2. Seguridad informática
- 1.2.1. Las Capas de Seguridad
- 1.2.2. Identificación de las amenazas informática
  - 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. Inteligencia de fuentes abiertas (OSINT)
- 1.3.2. Inteligencia de las redes sociales (SOCMINT)
- 1.3.3. Plataforma HUMIT
- 1.3.4. Distribuciones de Linux y herramientas.
- 1.3.5. Metodología de evaluación de seguridad inalámbrica abierta (OWISAM)
- 1.3.6. Proyecto de seguridad de aplicaciones web abiertas (OWASP)
- 1.3.7. Procedimientos de trabajo seguro (PETS)
- 1.3.8. Manual de la Metodología Abierta de Testeo de Seguridad (OSSTM)

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 Auditoria 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
- 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
- 1.8.1. Reglamento General de Protección de Datos (RGPD)
- 1.8.2. La estrategia nacional de ciberseguridad 2019
- 1.8.3. Familia ISO 27000
- 1.8.4. Marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST)
- 1.8.5. Ley PIC
- 1.8.6. ISO 27032
- 1.8.7. Normativas Cloud
- 1.8.8. Sarbanes-Oxley (SOX)
- 1.8.9. Normas PCI DSS

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 seguridad informática
- 1.10.1. Instituto Nacional de Estándares y Tecnología (NIST)
- 1.10.2. Agencia Europea de Seguridad de las Redes y la Información (ENISA)
- 1.10.3. Operador Económico Autorizado (OEA)
- 1.10.4. Unión de Naciones Suramericanas (UNASUR)

Asignatura 2. Seguridad en el alojamiento

2.1. Copias de seguridad
- 2.1.1. Estrategias para las copias de seguridad
- 2.1.2. Herramientas para Windows
- 2.1.3. Herramientas para Linux
- 2.1.4. Herramientas para MacOS

2.2. Antivirus de usuario
- 2.2.1. Tipos de antivirus
- 2.2.2. Antivirus para Windows
- 2.2.3. Antivirus para Linux
- 2.2.4. Antivirus para MacOS
- 2.2.5. Antivirus para teléfonos inteligentes

2.3. Detectores de intrusos
- 2.3.1. Métodos de detección de intrusos
- 2.3.2. Esquema de seguridad Sagan
- 2.3.3. Esquema de seguridad Aide
- 2.3.4. Esquema de seguridad Rkhunter

2.4. Cortafuegos local
- 2.4.1. Cortafuegos para Windows
- 2.4.2. Cortafuegos para Linux
- 2.4.3. Cortafuegos para MacOS

2.5. Gestores de contraseñas
- 2.5.1. Password
- 2.5.2. LastPass
- 2.5.3. KeePass
- 2.5.4. StickyPassword
- 2.5.5. RoboForm

2.6. Detectores de Phishing
- 2.6.1. Detección del phishing de forma manual
- 2.6.2. Herramientas antiphishing

2.7. Programas espía
- 2.7.1. Mecanismos de Evitación
- 2.7.2. Herramientas anti espionaje

2.8. Rastreadores
- 2.8.1. Medidas para proteger el sistema
- 2.8.2. Herramientas anti-rastreadores

2.9. Detección y respuesta de endpoints (EDR)
- 2.9.1. Comportamiento del Sistema EDR
- 2.9.2. Diferencias entre EDR y Antivirus
- 2.9.3. El futuro de los sistemas EDR

2.10. Control sobre la instalación de software
- 2.10.1. Repositorios y tiendas de software
- 2.10.2. Listas de software permitido o prohibido
- 2.10.3. Criterios de actualizaciones
- 2.10.4. Privilegios para instalar software

Asignatura 3. Seguridad en red perimetral

3.1. Sistemas de detección y prevención de amenazas
- 3.1.1. Marco general de los incidentes de seguridad
- 3.1.2. Sistemas de Defensa Actuales
- 3.1.3. Arquitecturas de red Actuales
- 3.1.4. Tipos de herramientas para la detección y prevención de incidentes
  - 3.1.4.1. Sistemas basados en Red
  - 3.1.4.2. Sistemas basados en Alojamiento
  - 3.1.4.3. Sistemas centralizados
- 3.1.5. Comunicación y detección de instancias/alojamiento, contenedores y computación sin servidor

3.2. Corta fuegos
- 3.2.1. Tipos
- 3.2.2. Ataques y mitigación
- 3.2.3. Firewalls comunes en Kernel Linux
- 3.2.4. Sistemas de detección basados en registros del sistema

3.3. Sistemas de Detección y Prevención de Intrusiones (IDS/IPS)
- 3.3.1. Ataques sobre IDS/IPS
- 3.3.2. Sistemas de IDS/IPS
  - 3.3.2.1. Sistema Snort
  - 3.3.2.2. Sistema Suricata

3.4. Corta fuegos de Siguiente Generación (NGFW)
- 3.4.1. Diferencias entre NGFW y Firewall tradicional
- 3.4.2. Capacidades principales
- 3.4.3. Soluciones comerciales
- 3.4.4. Firewalls para servicios de Cloud
- 3.4.5. Arquitectura Cloud VPC
  - 3.4.5.1. Cloud ACLs
  - 3.4.5.2. Security Group

3.5. Servidor Proxy
- 3.5.1. Tipos de Proxy
- 3.5.2. Uso de Proxy. Ventajas e inconvenientes

3.6. Motores de Antivirus
- 3.6.1. Contexto general del programas maliciosos e incidentes de seguridad
- 3.6.2. Problemas de los motores de Antivirus

3.7. Sistemas de Protección de Correo
- 3.7.1. Antispam
  - 3.7.1.1. Listas blancas y negras
  - 3.7.1.2. Filtros bayesianos
- 3.7.2. Dispositivo Mail Gateway (MGW)

3.8. Sistema de Gestión de Eventos e Información de Seguridad (SIEM)
- 3.8.1. Componentes y Arquitectura
- 3.8.2. Reglas de correlación y casos de uso
- 3.8.3. Retos actuales de los sistemas SIEM

3.9. Automatización y respuesta de la orquestación de seguridad (SOAR)
- 3.9.1. SOAR y SIEM: Enemigos o aliados
- 3.9.2. El futuro de los sistemas SOAR

3.10. Otros Sistemas basados en Red
- 3.10.1. Corta fuegos de aplicaciones (WAF)
- 3.10.2. Control de acceso a la red (NAC)
- 3.10.3. Herramientas HoneyPots y HoneyNets
- 3.10.4. agente de seguridad de acceso a la nube (CASB)

Asignatura 4. Seguridad en Teléfonos Inteligentes

4.1. El mundo del Dispositivo Móvil
- 4.1.1. Tipos de Plataformas móviles
- 4.1.2. Dispositivos iOS
- 4.1.3. Dispositivos Android

4.2. Gestión de la Seguridad Móvil
- 4.2.1. Proyecto de Seguridad Móvil (OWASP)

4.2.1.1. Las 10 vulnerabilidades más frecuentes
- 4.2.2. Comunicaciones, Redes y Modos de Conexión

4.3. El Dispositivo Móvil en el entorno Empresarial
- 4.3.1. Riesgos 3.2. Políticas de Seguridad
- 4.3.3. Monitorización de Dispositivos
- 4.3.4. Gestión de Dispositivos Móviles (MDM)

4.4. Privacidad del Usuario y Seguridad de los Datos
- 4.4.1. Estados de la Información
- 4.4.2. Protección y Confidencialidad de los Datos
  - 4.4.2.1. Permisos
  - 4.4.2.2. Encriptación
- 4.4.3. Almacenamiento Seguro de los Datos
  - 4.4.3.1. Almacenamiento Seguro en iOS
  - 4.4.3.2. Almacenamiento Seguro en Android
- 4.4.4. Buenas prácticas en el Desarrollo de Aplicaciones

4.5. Vulnerabilidades y Vectores de Ataque
- 4.5.1. Vulnerabilidades
- 4.5.2. Vectores de ataque
  - 4.5.2.1. Software malicioso
  - 4.5.2.2. Exfiltración de datos
  - 4.5.2.3. Manipulación de los datos

4.6. Principales Amenazas
- 4.6.1. Usuario no forzado
- 4.6.2. Software malicioso
  - 4.6.2.1. Tipos
- 4.6.3. Ingeniería Social
- 4.6.4. Fuga de Datos
- 4.6.5. Robo de información
- 4.6.6. Redes Wi-Fi no seguras
- 4.6.7. Software desactualizado
- 4.6.8. Aplicaciones Maliciosas
- 4.6.9. Contraseñas poco seguras
- 4.6.10. Configuración débil o inexistente de Seguridad
- 4.6.11. Acceso Físico
- 4.6.12. Pérdida o robo del dispositivo
- 4.6.13. Suplantación de identidad (Integridad)
- 4.6.14. Criptografía débil o rota
- 4.6.15. Denegación de Servicio (DoS)

4.7. Principales ataques
- 4.7.1. Ataques de phishing
- 4.7.2. Ataques relacionados con los modos de comunicación
- 4.7.3. Ataques de Smishing
- 4.7.4. Ataques de software Criptojacking

4.8. Hackeo
- 4.8.1. Enraizamiento y supresión de limitaciones
- 4.8.2. Anatomía de un Ataque Móvil
  - 4.8.2.1. Propagación de la amenaza
  - 4.8.2.2. Instalación de Software malicioso en el Dispositivo
  - 4.8.2.3. Persistencia
  - 4.8.2.4. Ejecución de carga útil y extracción de la información
- 4.8.3. Hackeo en Dispositivos iOS: mecanismos y herramientas
- 4.8.4. Hackeo en Dispositivos Android: mecanismos y herramientas

4.9. Pruebas de Penetración
- 4.9.1. Prueba iOS Pentesting
- 4.9.2. Prueba Android Pentesting
- 4.9.3. Herramientas

4.10. Protección y Seguridad
- 4.10.1. Configuración de Seguridad
  - 4.10.1.1. En Dispositivos iOS
  - 4.10.1.2. En Dispositivos Android
- 4.10.2. Medidas de Seguridad
- 4.10.3. Herramientas de protección

Asignatura 5. Seguridad en Internet de las Cosas

5.1. Dispositivos
- 5.1.1. Tipos de Dispositivos
- 5.1.2. Arquitecturas Estandarizadas
  - 5.1.2.1. ONEM2M
  - 5.1.2.2. IoTWF
- 5.1.3. Protocolos de Aplicación
- 5.1.4. Tecnologías de conectividad

5.2. Áreas de aplicación
- 5.2.1. Automatización de casas (SmartHome)
- 5.2.2. Automatización de ciudades (SmartCity)
- 5.2.3. Transportes
- 5.2.4. Aparatos de uso personal (Wearables)
- 5.2.5. Sector Salud
- 5.2.6. Internet industrial de las cosas (IioT)

5.3. Protocolos de comunicación
- 5.3.1. Protocolo MQTT
- 5.3.2. Protocolo LWM2M
- 5.3.3. Protocolo OMA-DM
- 5.3.4. Protocolo TR-069

5.4. Automatización de casas
- 5.4.1. Domótica
- 5.4.2. Redes
- 5.4.3. Lectrodomésticos
- 5.4.4. Vigilancia y seguridad

5.5. Automatización de ciudades
- 5.5.1. Iluminación
- 5.5.2. Meteorología
- 5.5.3. Seguridad

5.6. Transportes
- 5.6.1. Localización
- 5.6.2. Realización de pagos y obtención de servicios
- 5.6.3. Conectividad

5.7. Aparatos de uso personal (Wearables)
- 5.7.1. Ropa inteligente
- 5.7.2. Joyas inteligentes
- 5.7.3. Relojes inteligentes

5.8. Sector Salud
- 5.8.1. Monitorización de ejercicio/Ritmo Cardiaco
- 5.8.2. Monitorización de pacientes y personas mayores Implantadles
- 5.8.3. Robots Quirúrgicos

5.9. Conectividad
- 5.9.1. WiFi/Gateway
- 5.9.2. Bluetooth
- 5.9.3. Conectividad incorporada

5.10. Securización
- 5.10.1. Redes dedicadas
- 5.10.2. Gestor de Contraseñas
- 5.10.3. Uso de protocolos cifrados
- 5.10.4. Consejos de uso

Asignatura 6. Hackeo Ético

6.1. Entorno de trabajo
- 6.1.1. Distribuciones Linux
  - 6.1.1.1. Programa Kali Linux - Offensive Security
  - 6.1.1.2. Programa Parrot OS
  - 6.1.1.3. Programa Ubuntu
- 6.1.2. Sistemas de Virtualización
- 6.1.3. Entornos de prueba
- 6.1.4. Despliegue de laboratorios

6.2. Metodologías
- 6.2.1. Metodología OSSTMM (Manual de la Metodología Abierta de Testeo de Seguridad)
- 6.2.2. Metodología OWASP (proyecto de código abierto)
- 6.2.3. Metodología NIST (Instituto Nacional de Estándares y Tecnología)
- 6.2.4. Metodología PTES (examen de penetración)
- 6.2.5. Metodología ISSAF

6.3. Huellas
- 6.3.1. Inteligencia de fuentes abiertas (OSINT)
- 6.3.2. Búsqueda de brechas y vulnerabilidades de datos
- 6.3.3. Uso de herramientas pasivas

6.4. Escaneo de Redes
- 6.4.1. Herramientas de escaneo
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Otras herramientas de escaneo
- 6.4.2. Técnicas de Escaneo
- 6.4.3. Técnicas de Evasión de cortafuegos y sistema de detección de intrusos Banner Grabbing
- 6.4.4. Diagramas de red

6.5. Enumeración
- 6.5.1. Enumeración SMTP
- 6.5.2. Enumeración DNS
- 6.5.3. Enumeración de NetBIOS y Samba
- 6.5.4. Enumeración de LDAP
- 6.5.5. Enumeración de SNMP
- 6.5.6. Otras técnicas de Enumeración

6.6. Análisis de Vulnerabilidades
- 6.6.1. Soluciones de Análisis de Vulnerabilidades
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3.CFI LanGuard
- 6.6.2. Sistemas de puntuación de Vulnerabilidades
  - 6.6.2.1.CVS.
  - 6.6.2.2.CVE
  - 6.6.2.3.NVD

6.7. Ataques a Redes Inalámbrica
- 6.7.1. Metodología de Hackeo en Redes inalámbricas
  - 6.7.1.1. WiFi Discovery
  - 6.7.1.2. Análisis de tráfico
  - 6.7.1.3. Ataques del aircrack
    - 6.7.1.3.1. Ataques WEP (Privacidad equivalente a cableado)
    - 6.7.1.3.2. Ataques WPA/WPA2 (Acceso WiFi protegido)
  - 6.7.1.4. Ataques de Evil Twin
  - 6.7.1.5. Ataques a WPS (Configuración de WiFi Segura)
  - 6.7.1.6. Interferencia
- 6.7.2. Herramientas para la Seguridad Inalámbrica

6.8. Hackeo de servidores webs
- 6.8.1. Secuencias de comandos entre sitios
- 6.8.2. Falsificación de petición en sitios cruzados (CSRF)
- 6.8.3. Secuestro de sesión
- 6.8.4. Inyección SQL

6.9. Explotación de vulnerabilidades
- 6.9.1. Uso de exploits conocidos
- 6.9.2. Uso de metasploit
- 6.9.3. Uso de software malicioso
  - 6.9.3.1. Definición y alcance
  - 6.9.3.2. Generación de software malicioso
  - 6.9.3.3. Derivación de soluciones antivirus

6.10. Persistencia
- 6.10.1. Instalación de rootkits
- 6.10.2. Uso de NCAT
- 6.10.3. Uso de tareas programadas para puertas traseras
- 6.10.4. Creación de usuarios
- 6.10.5. Detección de sistema de detección de intrusos en un alojamiento

Asignatura 7. Ingeniería Inversa

7.1. Compiladores
- 7.1.1. Tipos de Códigos
- 7.1.2. Fases de un compilador
- 7.1.3. Tabla de símbolos
- 7.1.4. Gestor de errores
- 7.1.5. Compilador GCC

7.2. Tipos de Análisis en compiladores
- 7.2.1. Análisis léxico
  - 7.2.1.1. Terminología
  - 7.2.1.2. Componentes léxicos
  - 7.2.1.3. Analizador léxico LEX

7.2.2. Análisis sintáctico
7.2.2.1. Gramáticas libres de contexto
7.2.2.2. Tipos de análisis sintácticos
7.2.2.2.1. Análisis descendente
7.2.2.2.2. Análisis ascendente
7.2.2.3. Árboles sintácticos y derivaciones
7.2.2.4. Tipos de analizadores sintácticos
7.2.2.4.1. Analizadores LR (Izquierda a Derecha)
7.2.2.4.2. Analizadores LALR
7.2.3. Análisis semántico
7.2.3.1. Gramáticas de atributos
7.2.3.2. S-Atribuidas
7.2.3.3. L-Atribuidas
7.3. Estructuras de Datos en Ensamblador
7.3.1. Variables
7.3.2. Vectores
7.3.3. Punteros
7.3.4. Estructuras
7.3.5. Objetos
7.4. Estructuras de Código en Ensamblador
7.4.1. Estructuras de selección
7.4.2. Estructuras de iteración
7.4.3. Funciones
7.5. Arquitectura Hardware x86
7.5.1. Arquitectura de procesadores x86
7.5.2. Estructuras de datos en x86
7.5.3. Estructuras de código en x86
7.6. Arquitectura Hardware ARM
7.6.1. Arquitectura de procesadores ARM
7.6.2. Estructuras de datos en ARM
7.6.3. Estructuras de código en ARM
7.7. Análisis de código estático
7.7.1. Desensambladores
7.7.2. Herramienta IDA
7.7.3. Reconstructores de código
7.8. Análisis de código dinámico
7.8.1. Análisis del comportamiento
7.8.1.1.Comunicaciones
7.8.1.2.Monitorización
7.8.2. Depuradores de código en Linux
7.8.3. Depuradores de código en Windows
7.9. Aislamiento de procesos
7.9.1. Arquitectura
7.9.2. Evasión
7.9.3. Técnicas de detección
7.9.4. Técnicas de evasión
7.9.5. Contramedidas
7.9.6. Implementación en Linux
7.9.7. Implementación en Windows
7.9.8. Implementación en MacOS
7.9.9. Implementación en Android
7.10. Análisis de Software malicioso
7.10.1. Métodos de análisis
7.10.2. Técnicas de ofuscación
7.10.2.1. Ofuscación de ejecutables
7.10.2.2. Restricción de entornos de ejecución
7.10.3. Herramientas de análisis

Asignatura 8. Desarrollo seguro

8.1. Desarrollo Seguro
8.1.1. Calidad, funcionalidad y seguridad
8.1.2. Confidencialidad, integridad y disponibilidad
8.1.3. Ciclo de vida del desarrollo de software

8.2. Fase de Requerimientos
- 8.2.1. Control de la autenticación
- 8.2.2. Control de roles y privilegios
- 8.2.3. Requerimientos orientados al riesgo
- 8.2.4. Aprobación de privilegios

8.3. Fases de Análisis y Diseño
- 8.3.1. Acceso a componentes y administración del sistema
- 8.3.2. Pistas de auditoría
- 8.3.3. Gestión de sesiones
- 8.3.4. Datos históricos
- 8.3.5. Manejo apropiado de errores
- 8.3.6. Separación de funciones

8.4. Fase de Implementación y Codificación
- 8.4.1. Aseguramiento del ambiente de desarrollo
- 8.4.2. Elaboración de la documentación técnica
- 8.4.3. Codificación segura
- 8.4.4. Seguridad en las comunicaciones

8.5. Buenas prácticas de Codificación Segura
- 8.5.1. Validación de datos de entrada
- 8.5.2. Codificación de los datos de salida
- 8.5.3. Estilo de programación
- 8.5.4. Manejo de registro de cambios
- 8.5.5. Prácticas criptográficas
- 8.5.6. Gestión de errores y logs
- 8.5.7. Gestión de archivos
- 8.5.8. Gestión de. Memoria
- 8.5.9. Estandarización y reutilización de funciones de seguridad

8.6. Preparación del servidor y endurecimiento
- 8.6.1. Gestión de usuarios, grupos y roles en el servidor
- 8.6.2. Instalación de software
- 8.6.3. Endurecimiento del servidor
- 8.6.4. Configuración robusta del entorno de la aplicación

8.7. Preparación de la base de datos y endurecimiento
- 8.7.1. Optimización del motor de bases de datos
- 8.7.2. Creación del usuario propio para la aplicación
- 8.7.3. Asignación de los privilegios precisos para el usuario
- 8.7.4. Endurecimiento de la base de datos

8.8. Fase de pruebas
- 8.8.1. Control de calidad en controles de seguridad
- 8.8.2. Inspección del código por fases
- 8.8.3. Comprobación de la gestión de las configuraciones
- 8.8.4. Pruebas de caja negra

8.9. Preparación del Paso a producción
- 8.9.1. Realizar el control de cambios
- 8.9.2. Realizar procedimiento de paso a producción
- 8.9.3. Realizar procedimiento de reversión
- 8.9.4. Pruebas en fase de preproducción

8.10. Fase de mantenimiento
- 8.10.1. Aseguramiento basado en riesgos
- 8.10.2. Pruebas de mantenimiento de seguridad de caja blanca
- 8.10.3. Pruebas de mantenimiento de seguridad de caja negra

Asignatura 9. Análisis Forense

9.1. Adquisición de datos y duplicación
- 9.1.1. Adquisición de datos volátiles
  - 9.1.1.1. Información del sistema
  - 9.1.1.2. Información de la red
  - 9.1.1.3. Orden de volatilidad
- 9.1.2. Adquisición de datos estáticos
  - 9.1.2.1. Creación de una imagen duplicada
  - 9.1.2.2. Preparación de un documento para la cadena de custodia
- 9.1.3. Métodos de validación de los datos adquiridos
  - 9.1.3.1. Métodos para Linux
  - 9.1.3.2. Métodos para Windows

9.2. Evaluación y derrota de técnicas antiforenses
- 9.2.1. Objetivos de las técnicas antiforenses
- 9.2.2. Borrado de datos
  - 9.2.2.1. Borrado de datos y ficheros
  - 9.2.2.2. Recuperación de archivos
  - 9.2.2.3. Recuperación de particiones borradas
- 9.2.3. Protección por contraseña
- 9.2.4. Esteganografía
- 9.2.5. Borrado seguro de dispositivos
- 9.2.6. Encriptación

9.3. Análisis Forense del sistema operativo
- 9.3.1. Análisis Forense de Windows
- 9.3.2. Análisis Forense de Linux
- 9.3.3. Análisis Forense de Mac

9.4. Análisis Forense de la red
- 9.4.1. Análisis de los registros
- 9.4.2. Correlación de datos
- 9.4.3. Investigación de la red
- 9.4.4. Pasos a seguir en el análisis forense de la red

9.5. Análisis Forense Web
- 9.5.1. Investigación de los ataques webs
- 9.5.2. Detección de ataques
- 9.5.3. Localización de direcciones IPs

9.6. Análisis Forense de Bases de Datos
- 9.6.1. Análisis Forense en MSSQL
- 9.6.2. Análisis Forense en MySQL
- 9.6.3. Análisis Forense en PostgreSQL
- 9.6.4. Análisis Forense en MongoDB

9.7. Análisis Forense en la nube
- 9.7.1. Tipos de Crímenes en la nube
  - 9.7.1.1. La nube como Sujeto
  - 9.7.1.2. La nube como Objeto
  - 9.7.1.3. La nube como Herramienta
- 9.7.2. Retos del Análisis Forense en la nube
- 9.7.3. Investigación de los servicios de Almacenamiento la nube
- 9.7.4. Herramientas de Análisis Forense para la nube

9.8. Investigación de crímenes de Correo Electrónico
- 9.8.1. Sistemas de correo
  - 9.8.1.1. Clientes de Correo
  - 9.8.1.2. Servidor de Correo
  - 9.8.1.3. Servidor SMTP
  - 9.8.1.4. Servidor POP3
  - 9.8.1.5. Servidor IMAP4
- 9.8.2. Crímenes de correo
- 9.8.3. Mensaje de Correo
  - 9.8.3.1. Cabeceras Estándar
  - 9.8.3.2. Cabeceras Extendidas
- 9.8.4. Pasos para la investigación de estos crímenes
- 9.8.5. Herramientas Forenses para Correo Electrónico

9.9. Análisis Forense de Móviles
- 9.9.1. Redes Celulares
  - 9.9.1.1. Tipos de redes
  - 9.9.1.2. Contenidos del CDR
- 9.9.2. Tarjeta SIM (Módulo de Identidad del Suscriptor)
- 9.9.3. Adquisición lógica
- 9.9.4. Adquisición física
- 9.9.5. Adquisición del sistema de ficheros

9.10. Redacción y presentación de Informes Forenses
- 9.10.1. Aspectos importantes de un Informe Forense
- 9.10.2. Clasificación y tipos de informes
- 9.10.3. Guía para escribir un informe
- 9.10.4. Presentación del informe

Asignatura 10. Retos actuales y futuros en Seguridad Informática

10.1. Tecnología Blockchain
- 10.1.1. Ámbitos de aplicación
- 10.1.2. Garantía de confidencialidad
- 10.1.3. Garantía de no-repudio

10.2. Dinero Digital
- 10.2.1. Bitcoins
- 10.2.2. Critpomonedas
- 10.2.3. Minería de criptomonedas
- 10.2.4. Estafas piramidales
- 10.2.5. Otros potenciales delitos y problemas

10.3. Manipulación de videos (Deepfake)
- 10.3.1. Impacto en los medios
- 10.3.2. Peligros para la sociedad
- 10.3.3. Mecanismos de detección

10.4. El futuro de la inteligencia artificial
- 10.4.1. Inteligencia artificial y computación cognitiva
- 10.4.2. Usos para simplificar el servicio a clientes

10.5. Privacidad digital
- 10.5.1. Valor de los datos en la red
- 10.5.2. Uso de los datos en la red
- 10.5.3. Gestión de la privacidad e identidad digital

10.6. Ciberconflictos, cibercriminales y ciberataques
- 10.6.1. Impacto de la ciberseguridad en conflictos internacionales
- 10.6.2. Consecuencias de ciberataques en la población general
- 10.6.3. Tipos de cibercriminales. Medidas de Protección

10.7. Teletrabajo
- 10.7.1. Revolución del teletrabajo durante y post Covid19
- 10.7.2. Cuellos de botella en el acceso
- 10.7.3. Variación de la superficie de ataque
- 10.7.4. Necesidades de los trabajadores

10.8. Tecnologías inalámbricas emergentes
- 10.8.1. Acceso Wi-Fi protegido (WPA3)
- 10.8.2. Tecnología 5G
- 10.8.3. Ondas milimétricas
- 10.8.4. Tendencia en "Get Smart"

10.9. Direccionamiento futuro en redes
- 10.9.1. Problemas actuales con el direccionamiento IP
- 10.9.2. IPv6 9.3. IPv4+
- 10.9.4. Ventajas de IPv4+ sobre IPv4
- 10.9.5. Ventajas de IPv6 sobre IPv4

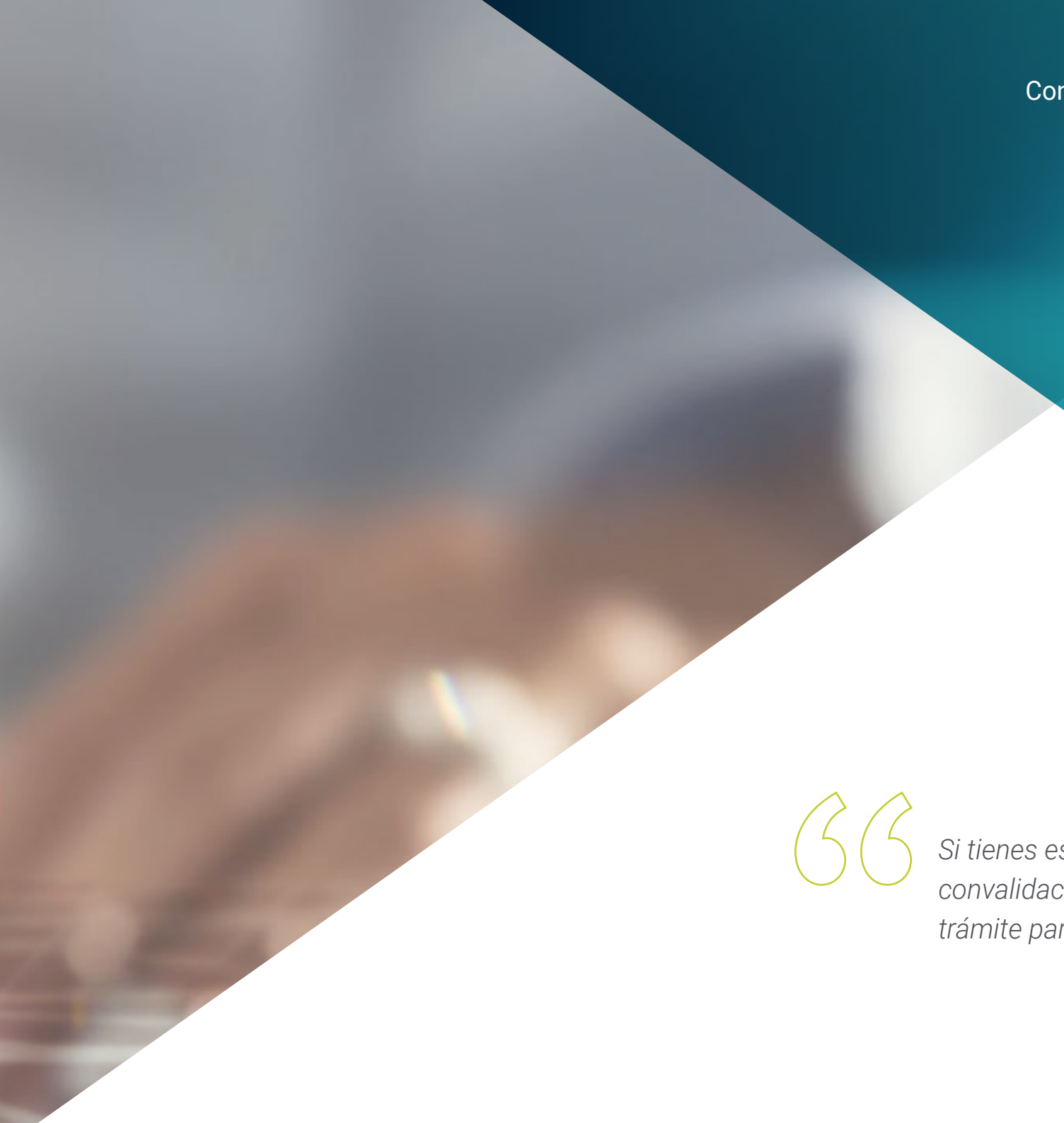
10.10. El reto de la concienciación de la formación temprana y continua de la población
- 10.10.1. Estrategias actuales de los gobiernos
- 10.10.2. Resistencia de la Población al aprendizaje
- 10.10.3. Planes de formación que deben adoptar las empresas

¿Buscas desarrollar aplicaciones seguras mediante las prácticas de codificación más modernas? Consíguelo mediante esta titulación universitaria en tan solo 20 meses"

04

Convalidación de asignaturas

Si el candidato a estudiante ha cursado otra Maestría Oficial Universitaria de la misma rama de conocimiento o un programa equivalente al presente, incluso si solo lo cursó parcialmente y no lo finalizó, TECH le facilitará la realización de un Estudio de Convalidaciones que le permitirá no tener que examinarse de aquellas asignaturas que hubiera superado con éxito anteriormente.



Si tienes estudios susceptibles de convalidación, TECH te ayudará en el trámite para que sea rápido y sencillo"

Cuando el candidato a estudiante desee conocer si se le valorará positivamente el estudio de convalidaciones de su caso, deberá solicitar una **Opinión Técnica de Convalidación de Asignaturas** que le permita decidir si le es de interés matricularse en el programa de Maestría Oficial Universitaria.

La Comisión Académica de TECH valorará cada solicitud y emitirá una resolución inmediata para facilitar la decisión de la matriculación. Tras la matrícula, el estudio de convalidaciones facilitará que el estudiante consolide sus asignaturas ya cursadas en otros programas de Maestría Oficial Universitaria en su expediente académico sin tener que evaluarse de nuevo de ninguna de ellas, obteniendo en menor tiempo, su nuevo título de Maestría Oficial Universitaria.

TECH le facilita a continuación toda la información relativa a este procedimiento:

Matricúlate en la Maestría Oficial Universitaria y obtén el estudio de convalidaciones de forma gratuita"

¿Qué es la convalidación de estudios?

La convalidación de estudios es el trámite por el cual la Comisión Académica de TECH equipara estudios realizados de forma previa, a las asignaturas del programa de Maestría Oficial Universitaria tras la realización de un análisis académico de comparación. Serán susceptibles de convalidación aquellos contenidos cursados en un plan o programa de estudio de Maestría Oficial Universitaria o nivel superior, y que sean equiparables con asignaturas de los planes y programas de estudio de esta Maestría Oficial Universitaria de TECH. Las asignaturas indicadas en el documento de Opinión Técnica de Convalidación de Asignaturas quedarán consolidadas en el expediente del estudiante con la leyenda "EQ" en el lugar de la calificación, por lo que no tendrá que cursarlas de nuevo.

¿Qué es la Opinión Técnica de Convalidación de Asignaturas?

La Opinión Técnica de Convalidación de Asignaturas es el documento emitido por la Comisión Académica tras el análisis de equiparación de los estudios presentados; en este, se dictamina el reconocimiento de los estudios anteriores realizados, indicando qué plan de estudios le corresponde, así como las asignaturas y calificaciones obtenidas, como resultado del análisis del expediente del alumno. La Opinión Técnica de Convalidación de Asignaturas será vinculante en el momento en que el candidato se matricule en el programa, causando efecto en su expediente académico las convalidaciones que en ella se resuelvan. El dictamen de la Opinión Técnica de Convalidación de Asignaturas será inapelable.

¿Cómo se solicita la Opinión Técnica de Convalidación de Asignaturas?

El candidato deberá enviar una solicitud a la dirección de correo electrónico *convalidaciones@techtitute.com* adjuntando toda la documentación necesaria para la realización del estudio de convalidaciones y emisión de la opinión técnica. Asimismo, tendrá que abonar el importe correspondiente a la solicitud indicado en el apartado de Preguntas Frecuentes del portal web de TECH. En caso de que el alumno se matricule en la Maestría Oficial Universitaria, este pago se le descontará del importe de la matrícula y por tanto el estudio de opinión técnica para la convalidación de estudios será gratuito para el alumno.

¿Qué documentación necesitará incluir en la solicitud?

La documentación que tendrá que recopilar y presentar será la siguiente:

- Documento de identificación oficial
- Certificado de estudios, o documento equivalente que ampare los estudios realizados. Este deberá incluir, entre otros puntos, los periodos en que se cursaron los estudios, las asignaturas, las calificaciones de las mismas y, en su caso, los créditos. En caso de que los documentos que posea el interesado y que, por la naturaleza del país, los estudios realizados carezcan de listado de asignaturas, calificaciones y créditos, deberán acompañarse de cualquier documento oficial sobre los conocimientos adquiridos, emitido por la institución donde se realizaron, que permita la comparabilidad de estudios correspondiente

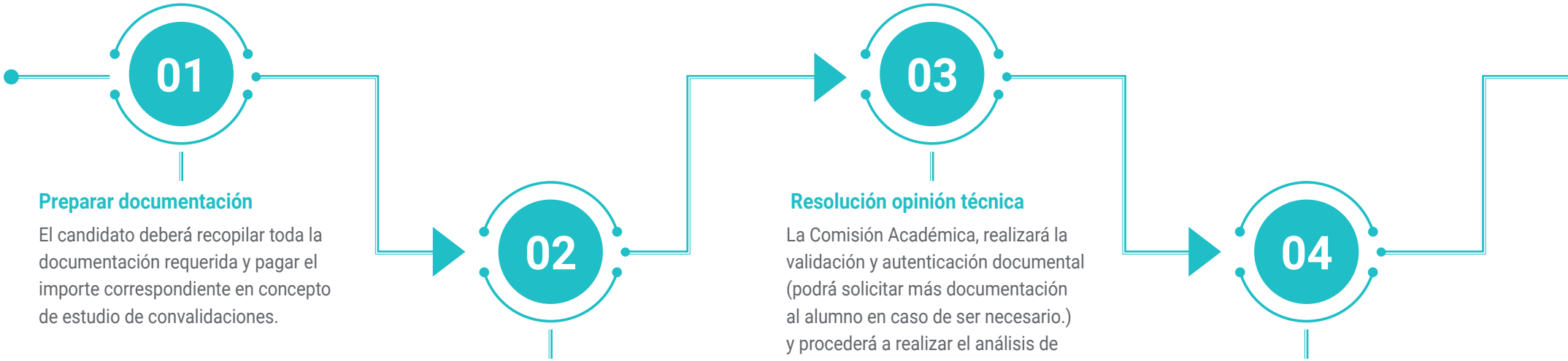
¿En qué plazo se resolverá la solicitud?

La Opinión Técnica se llevará a cabo en un plazo máximo de 48h desde que el interesado abone el importe del estudio y envíe la solicitud con toda la documentación requerida. En este tiempo la Comisión Académica analizará y resolverá la solicitud de estudio emitiendo una Opinión Técnica de Convalidación de Asignaturas que será informada al interesado mediante correo electrónico. Este proceso será rápido para que el estudiante pueda conocer las posibilidades de convalidación que permita el marco normativo para poder tomar una decisión sobre la matriculación en el programa.

¿Será necesario realizar alguna otra acción para que la Opinión Técnica se haga efectiva?

Una vez realizada la matrícula, deberá cargar en el campus virtual el informe de opinión técnica y el departamento de Servicios Escolares consolidarán las convalidaciones en su expediente académico. En cuanto las asignaturas le queden convalidadas en el expediente, el estudiante quedará eximido de realizar la evaluación de estas, pudiendo consultar los contenidos con libertad sin necesidad de hacer los exámenes.

Procedimiento paso a paso



05

Matriculación

Cuando el interesado reciba la Opinión Técnica de Convalidación de Asignaturas, la revisará para evaluar su conveniencia y podrá proceder a la matriculación del programa si es su interés.

Duración:
20 min

06

Carga de la opinión técnica en campus

Una vez matriculado, deberá cargar en el campus virtual el documento de la Opinión Técnica de Convalidación de Asignaturas firmado. El importe abonado del estudio de convalidaciones se le deducirá de la matrícula y por tanto será gratuito para el alumno.

Duración:
20 min

07

Consolidación del expediente

En cuanto el documento de Opinión Técnica de Convalidación de Asignaturas quede firmado y subido al campus virtual, el departamento de Servicios Escolares registrará en el sistema de TECH las asignaturas indicadas de acuerdo con la Opinión Técnica de Convalidación de Asignaturas, y colocará en el expediente del alumno la leyenda de "EQ", en cada asignatura reconocida, por lo que el alumno ya no tendrá que cursarlas de nuevo. Además, retirará las limitaciones temporales de todas las asignaturas del programa, por lo que podrá cursarlo en modalidad intensiva. El alumno tendrá siempre acceso a los contenidos en el campus en todo momento.

Convalida tus estudios realizados y no tendrás que evaluarte de las asignaturas superadas.

05

Objetivos docentes

La Maestría Oficial Universitaria en Seguridad Informática tiene por objetivo principal capacitar a los profesionales para enfrentar los desafíos que plantea la Ciberseguridad en el entorno actual. Este enfoque integral les permitirá comprender y aplicar las mejores estrategias y herramientas en diversas áreas de la Seguridad Informática, desde la protección de infraestructuras críticas hasta el análisis forense y la ingeniería inversa. Todo ello, en un itinerario académico vanguardista, directamente aplicable al entorno profesional.

Living success

Ejecutarás planes de seguridad a nivel organizacional, incluyendo políticas de privacidad y gestión de crisis”

Objetivos generales

- Generar conocimiento especializado sobre un sistema de información, tipos y aspectos de seguridad que deben ser tenidos en cuenta
- Identificar las vulnerabilidades de un sistema de información
- Desarrollar la normativa legal y tipificación del delito atacando a un sistema de información
- Evaluar los diferentes modelos de arquitectura de seguridad para establecer el modelo más adecuado a la organización
- Identificar los marcos normativos de aplicación y las bases reguladoras de los mismos
- Analizar la estructura organizativa y funcional de un área de seguridad de la información (la oficina del CISO)
- Analizar los tipos de criptografía según el tipo de algoritmo y según su uso
- Generar conocimiento especializado sobre el ecosistema de seguridad informática
- Evaluar el conocimiento en término de ciberseguridad
- Identificar los ámbitos de seguridad en *Cloud*
- Analizar los servicios y herramientas en cada uno de los ámbitos de seguridad
- Analizar de forma comparativa la seguridad de las tecnologías LPWAN

Objetivos específicos

Asignatura 1. Inteligencia y Seguridad Informática

- Analizar las metodologías usadas en materia de seguridad informática
- Examinar el ciclo de inteligencia y establecer su aplicación en la inteligencia informática
- Comprender las herramientas más comunes para la producción de inteligencia
- Llevar a cabo un análisis de riesgos conociendo las métricas usadas, así como comprender las Normativas vigentes en seguridad informática

Asignatura 2. Seguridad en el alojamiento

- Establecer políticas de respaldo de los datos de personales y profesionales
- Definir las herramientas necesarias para solucionar problemas específicos de seguridad

Asignatura 3. Seguridad en red perimetral

- Abordar las arquitecturas actuales de red para identificar el perímetro que se deben proteger
- Desarrollar las configuraciones concretas para mitigar los ataques más comunes
- Conocer las diferentes capas que proporcionan los cortafuegos de nueva generación y funcionalidades de red en entornos nube
- Manejar las herramientas para la protección de la red y demostrar por qué son fundamentales para una defensa multicapa

Asignatura 4. Seguridad en Teléfonos Inteligentes

- Examinar los distintos vectores de ataque y los principales ataques y tipos de software malicioso a los que se exponen los usuarios de dispositivos móviles
- Establecer una mayor seguridad en la configuración
- Concretar la metodología para realizar una prueba de penetración tanto en plataformas iOS como en plataformas Android y
- Implementar buenas prácticas en programación orientadas a dispositivos móviles

Asignatura 5. Seguridad en Internet de las Cosas

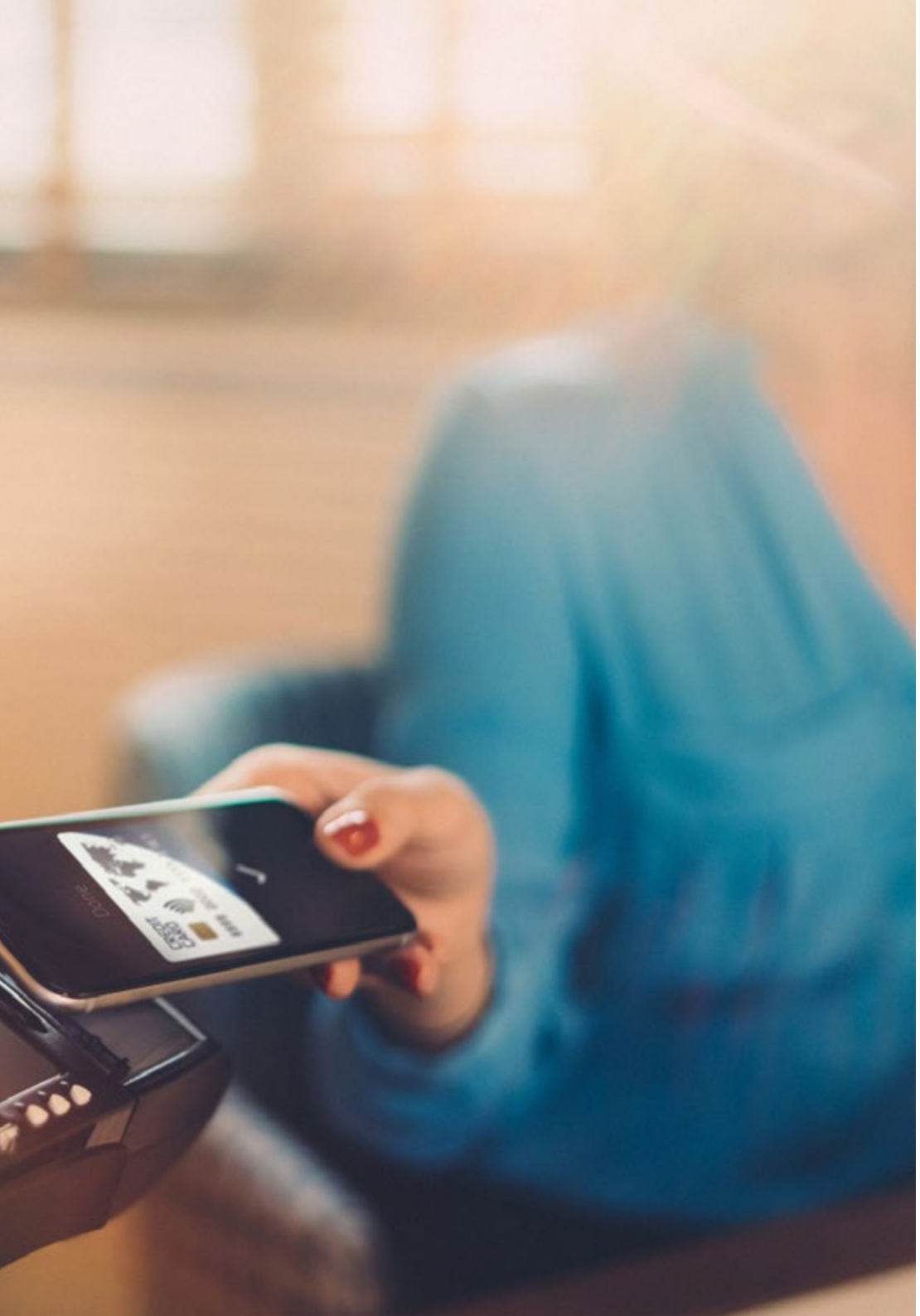
- Abordar las principales arquitecturas de Internet de las Cosas
- Evaluar los niveles de riesgo y vulnerabilidades conocidas para implementar políticas de uso seguras

Asignatura 6. Hackeo Ético

- Indagar en los métodos de inteligencia de fuentes abiertas
- Escanear redes para obtener información de modo activo
- Manejar las herramientas para el desempeño de pruebas de penetración
- Catalogar y evaluar las diferentes vulnerabilidades de los sistemas y concretar las diferentes metodologías de hackeo

Asignatura 7. Ingeniería Inversa

- Evaluar la arquitectura de diferentes procesadores
- Implementar los diferentes tipos de análisis aplicando aislamiento de procesos y utilizando diferentes técnicas de análisis de software malicioso



Asignatura 8. Desarrollo seguro

- Establecer los requisitos necesarios para el correcto funcionamiento de una aplicación de forma segura
- Entender los mensajes de error en los archivos y analizar los diferentes eventos para decidir qué mostrar al usuario
- Ser capaz de generar un Código Sanitizado, fácilmente verificable y de calidad,
- Analizar la documentación adecuada para cada fase del desarrollo y desarrollar códigos modulares, reusables y mantenibles

Asignatura 9. Análisis Forense

- Identificar los diferentes elementos que ponen en evidencia un delito informático
- Recuperar los datos que hayan sido borrados intencionadamente
- Ahondar en los registros de los sistemas y fundamentar las pruebas para que sean consistentes
- Generar un informe y conclusiones de forma coherente

Asignatura 10. Retos actuales y futuros en Seguridad Informática

- Entender las tendencias en la informática actual tales como el uso de las Criptomonedas, las alteraciones de videos, el denominado analfabetismo digital y las alternativas al Protocolo de Internet versión 4 en el Direccionamiento de Redes
- Reflexionar acerca de la importancia de formar a la población en el uso correcto de las tecnologías

06

Salidas profesionales

Al finalizar esta Maestría Oficial Universitaria, los egresados estarán capacitados para asumir roles de alto nivel en el sector de la Ciberseguridad. Con el conocimiento adquirido durante el programa universitario, podrán desempeñarse en diversas áreas clave, como la gestión de seguridad en infraestructuras tecnológicas, la protección de datos sensibles y la respuesta ante incidentes de seguridad. Además, tendrán las competencias necesarias para liderar equipos en organizaciones de todos los tamaños, implementar políticas de protección digital, realizar auditorías de sistemas y participar en la creación de soluciones innovadoras para mitigar los riesgos cibernéticos.

Un plan de estudios que te abrirá las puertas a numerosos roles estratégicos, como la Dirección en Protección de Datos”

Perfil del egresado

Al completar esta titulación universitaria, los egresados serán expertos en la protección de sistemas informáticos y redes, con habilidades para diseñar, implementar y gestionar soluciones de seguridad en diversos entornos tecnológicos. De este modo, podrán integrarse exitosamente en empresas privadas, organismos públicos y consultoras, destacándose por su capacidad para adaptarse a los constantes cambios tecnológicos y por su enfoque práctico y especializado en la seguridad informática.

Brindarás un asesoramiento integral a las organizaciones sobre la adopción de medidas de protección ante amenazas cibernéticas.

- **Gestión de Riesgos Cibernéticos:** Capacidad para identificar, evaluar y mitigar los riesgos asociados con las amenazas cibernéticas, desarrollando políticas y estrategias de seguridad para proteger infraestructuras tecnológicas y datos sensibles
- **Respuesta ante Incidentes:** Habilidad para responder de manera efectiva ante incidentes de seguridad, determinando las causas, el alcance y las posibles soluciones para minimizar el impacto de los ataques cibernéticos
- **Desarrollo Seguro y Protección de Infraestructuras:** Competencia para integrar principios de seguridad en el ciclo de vida del desarrollo de software, así como diseñar, implementar y mantener infraestructuras seguras, protegiendo sistemas, redes y dispositivos contra posibles vulnerabilidades
- **Conocimiento en Tecnologías Emergentes:** Capacidad para abordar los retos de la ciberseguridad en plataformas emergentes, como el Internet de las Cosas, asegurando su integración segura en entornos empresariales y personales

Después de realizar esta Maestría Oficial Universitaria, podrás desempeñar tus conocimientos y habilidades en los siguientes cargos:

1. **Especialista en Ciberseguridad en Infraestructuras Tecnológicas:** En el ámbito empresarial, este profesional se encarga de proteger las infraestructuras tecnológicas y las redes de las organizaciones contra ciberamenazas.
   Responsabilidades: Supervisar y gestionar la seguridad de redes, servidores y aplicaciones, realizar auditorías de seguridad y mantener los sistemas protegidos frente a amenazas externas e internas.
2. **Consultor en Seguridad Informática:** El egresado podrá trabajar de manera independiente o en empresas de consultoría, ofreciendo asesoría a organizaciones sobre cómo mejorar su postura de seguridad informática.
   Responsabilidades: Realizar auditorías de seguridad, diseñar e implementar planes de seguridad, capacitar a los empleados sobre buenas prácticas de seguridad, y realizar análisis de riesgos y vulnerabilidades.
3. **Analista Forense Digital:** En el ámbito de la investigación, el analista forense digital se especializa en la recuperación de información y la investigación de incidentes cibernéticos, como fraudes, robos de datos o ataques de *malware*.
   Responsabilidades: Recopilar, analizar y preservar evidencia digital, reconstruir incidentes cibernéticos y proporcionar informes detallados sobre el ataque o el delito cibernético.
4. **Ingeniero de Seguridad en Redes:** Se encarga de diseñar y gestionar infraestructuras de seguridad perimetral, como *firewalls*, VPN y sistemas de detección de intrusos, para garantizar la seguridad de las comunicaciones y los datos dentro de una red corporativa.
   Responsabilidades: Implementar y mantener soluciones de seguridad de red, monitorear el tráfico para detectar posibles ataques y vulnerabilidades, y garantizar que la infraestructura de red cumpla con las normativas de seguridad.
5. **Profesional en Protección de Datos Personales:** Este perfil está enfocado en la protección de los datos personales de los usuarios, especialmente en el contexto de normativas internacionales como el GDPR (Reglamento General de Protección de Datos).
   Responsabilidades: Supervisar la implementación de políticas de privacidad, realizar auditorías de protección de datos, capacitar a los empleadWos en normativas de privacidad y responder ante incidentes relacionados con el manejo de datos personales.
6. **Especialista en Seguridad en Internet de las Cosas:** Este profesional se especializa en la protección de dispositivos conectados a la red, como electrodomésticos inteligentes, sistemas de control de edificios y dispositivos médicos.
   Responsabilidades: Evaluar y mitigar riesgos de seguridad en dispositivos IoT, diseñar soluciones de protección para entornos interconectados, y colaborar en el desarrollo de estándares de seguridad para dispositivos emergentes.
7. **Especialista en Seguridad en la Nube:** Con el creciente uso de servicios en la nube, el egresado de esta Maestría podrá desempeñarse en empresas que proveen servicios en la nube o en organizaciones que utilizan soluciones basadas en la nube para proteger sus datos y aplicaciones.
   Responsabilidades: Diseñar estrategias de seguridad para aplicaciones y datos en la nube, implementar controles de acceso, cifrado y auditoría, y realizar evaluaciones de seguridad para garantizar la integridad de los servicios basados en la nube.
8. **Auditor de Seguridad Informática:** Se especializan en realizar revisiones y evaluaciones de los sistemas de seguridad de una organización para detectar vulnerabilidades.
   Responsabilidades: Realizar auditorías de seguridad a los sistemas de TI de la organización, identificar debilidades y fallos de seguridad, elaborar informes detallados y proponer medidas correctivas para mitigar los riesgos.

Salidas académicas y de investigación

Además de todos los puestos laborales para los que serás apto mediante el estudio de este Máster Oficial Universitario de TECH, también podrás continuar con una sólida trayectoria académica e investigativa. Tras completar este programa universitario, estarás listo para continuar con tus estudios desarrollando un Doctorado asociado a este ámbito del conocimiento y así, progresivamente, alcanzar otros méritos científicos.

07

Idiomas gratuitos

Convencidos de que la formación en idiomas es fundamental en cualquier profesional para lograr una comunicación potente y eficaz, TECH ofrece un itinerario complementario al plan de estudios curricular, en el que el alumno, además de adquirir las competencias de la Maestría Oficial Universitaria, podrá aprender idiomas de un modo sencillo y práctico.

Acredita tu competencia lingüística

TECH te incluye el estudio de idiomas en la Maestría Oficial Universitaria de forma ilimitada y gratuita"

En el mundo competitivo actual, hablar otros idiomas forma parte clave de nuestra cultura moderna. Hoy en día, resulta imprescindible disponer de la capacidad de hablar y comprender otros idiomas, además de lograr un título oficial que acredite y reconozca las competencias lingüísticas adquiridas. De hecho, ya son muchos los colegios, las universidades y las empresas que solo aceptan a candidatos que certifican su nivel mediante un título oficial en base al Marco Común Europeo de Referencia para las Lenguas (MCER).

El Marco Común Europeo de Referencia para las Lenguas es el máximo sistema oficial de reconocimiento y acreditación del nivel del alumno. Aunque existen otros sistemas de validación, estos proceden de instituciones privadas y, por tanto, no tienen validez oficial. El MCER establece un criterio único para determinar los distintos niveles de dificultad de los cursos y otorga los títulos reconocidos sobre el nivel de idioma que se posee.

En TECH se ofrecen los únicos cursos intensivos de preparación para la obtención de certificaciones oficiales de nivel de idiomas, basados 100% en el MCER. Los 48 Cursos de Preparación de Nivel Idiomático que tiene la Escuela de Idiomas de TECH están desarrollados en base a las últimas tendencias metodológicas de aprendizaje en línea, el enfoque orientado a la acción y el enfoque de adquisición de competencia lingüística, con la finalidad de preparar los exámenes oficiales de certificación de nivel.

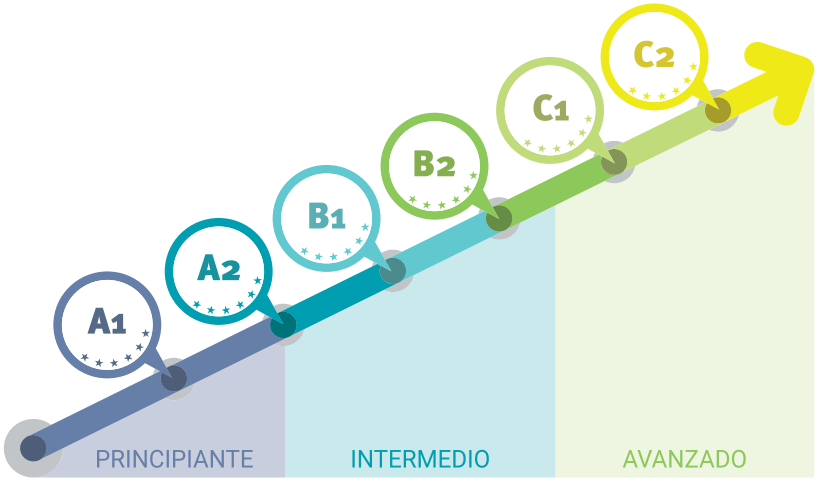
El estudiante aprenderá, mediante actividades en contextos reales, la resolución de situaciones cotidianas de comunicación en entornos simulados de aprendizaje y se enfrentará a simulacros de examen para la preparación de la prueba de certificación de nivel.

Solo el coste de los Cursos de Preparación de idiomas y los exámenes de certificación, que puedes llegar a hacer gratis, valen más de 3 veces el precio de la Maestría Oficial Universitaria”

TECH incorpora, como contenido extracurricular al plan de estudios oficial, la posibilidad de que el alumno estudie idiomas, seleccionando aquellos que más le interesen de entre la gran oferta disponible:

- Podrá elegir los Cursos de Preparación de Nivel de los idiomas y nivel que desee, de entre los disponibles en la Escuela de Idiomas de TECH, mientras estudie la Maestría Oficial Universitaria, para poder prepararse el examen de certificación de nivel
- En cada programa de idiomas tendrá acceso a todos los niveles MCER, desde el nivel A1 hasta el nivel C2
- Cada año podrá presentarse a un examen telepresencial de certificación de nivel, con un profesor nativo experto. Al terminar el examen, TECH le expedirá un certificado de nivel de idioma
- Estudiar idiomas NO aumentará el coste del programa. El estudio ilimitado y la certificación anual de cualquier idioma están incluidas en la Maestría Oficial Universitaria

"48 Cursos de Preparación de Nivel para la certificación oficial de 8 idiomas en los niveles MCER A1, A2, B1, B2, C1 y C2"



08
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.

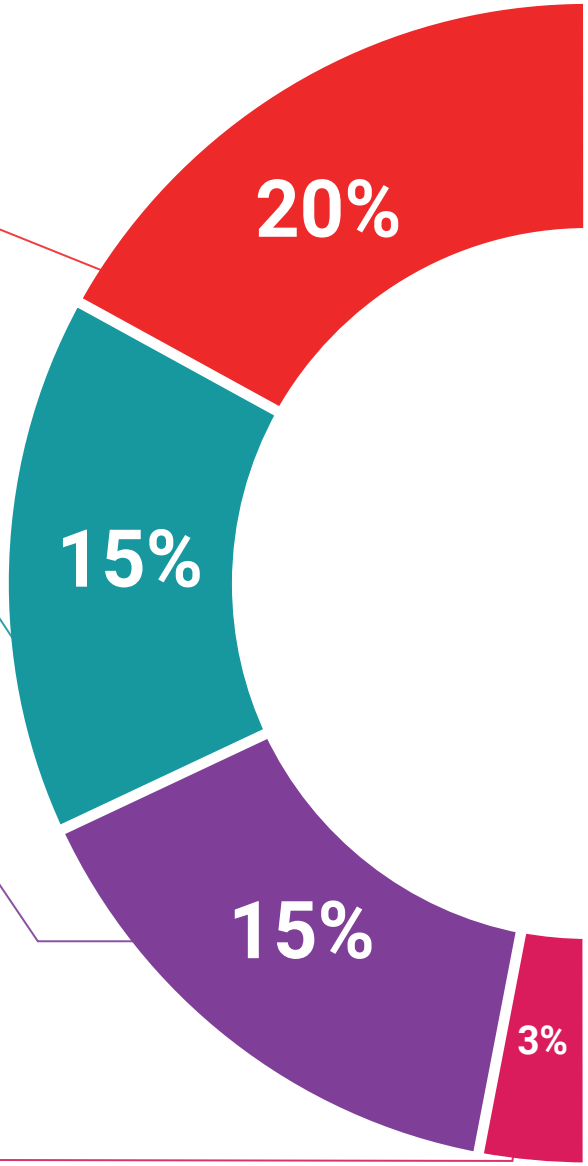
Resúmenes interactivos

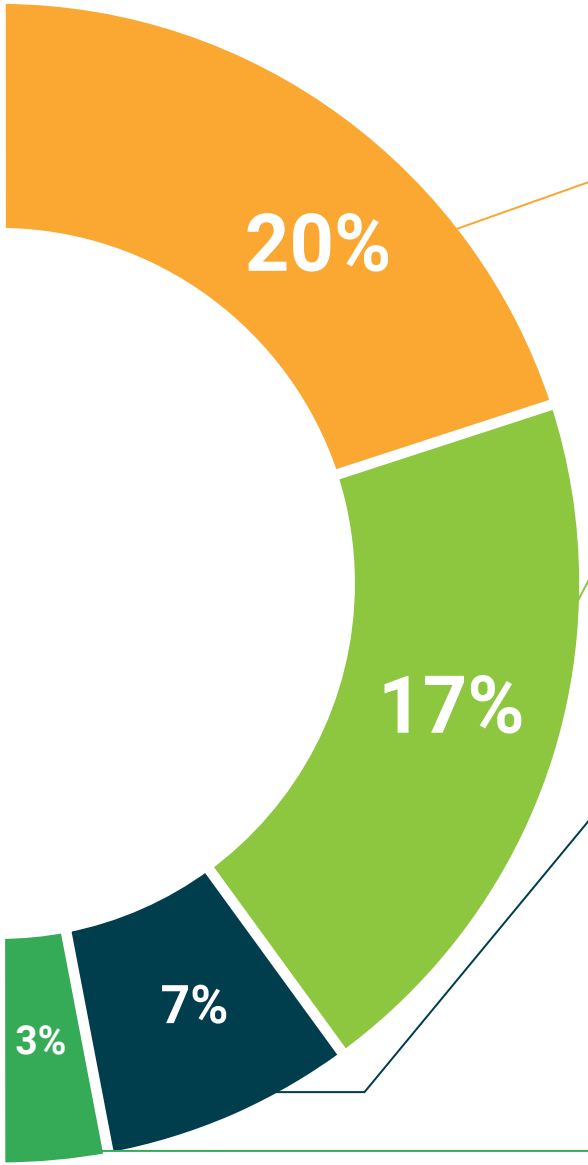
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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.

09
Cuadro docente

El claustro docente de esta Maestría Oficial Universitaria en Seguridad Informática destaca por su dilatada experiencia en este ámbito en pleno auge. Gracias a esto, los profesionales han diseñado múltiples contenidos didácticos caracterizados por su elevada calidad y adaptación a las demandas del mercado laboral actual. De este modo, los egresados disfrutarán de una experiencia de alta intensidad que les permitirá ampliar sus perspectivas laborales significativamente.

Disfrutarás de un plan de estudios confeccionado por un versado equipo docente especializado en Seguridad Informática, que te garantizará un aprendizaje exitoso"

Dirección

D. Olalla Bonal, Martín

- Gerente Senior de Práctica de *Blockchain* en EY
- Especialista Técnico Cliente *Blockchain* para IBM
- Director de Arquitectura para *Blocknitive*
- Coordinador de Equipo en Bases de Datos Distribuidas no Relacionales para WedoIT, Subsidiaria de IBM
- Arquitecto de Infraestructuras en Bankia
- Responsable del Departamento de Maquetación en T-Systems
- Coordinador de Departamento para Bing Data España SL

Profesores

D. Gozalo Fernández, Juan Luis

- Gerente de Productos basados en Blockchain para Open Canarias
- Director Blockchain DevOps en Alastria
- Director de Tecnología Nivel de Servicio en Santander España
- Director Desarrollo Aplicación Móvil Tinkerlink en Cronos Telecom
- Director Tecnología Gestión de Servicio IT en Barclays Bank España
- Licenciado en Ingeniería Superior de Informática en la UNED
- Especialización en *Deep Learning* en DeepLearning.ai

D. Gonzalo Alonso, Félix

- Director general y fundador de Smart REM Solutions
- Responsable de Ingeniería de Riesgos e Innovación en Dynargy
- Gerente y socio fundador del gabinete pericial de tecnologías Risknova
- Máster en Dirección Aseguradora por el Instituto para la Colaboración entre Entidades Aseguradoras
- Grado en Ingeniería Técnica Industrial, especialidad Electrónica Industrial por la Universidad Pontificia de Comillas

D. Entrenas, Alejandro

- Jefe de Proyecto en Ciberseguridad. Entelgy Innotec Security
- Consultor de Ciberseguridad. Entelgy
- Analista de Seguridad de la Información. Innovery España
- Analista en Seguridad de la Información. Atos
- Licenciado en Ingeniería Técnica en Informática de Sistemas por la Universidad de Córdoba
- Máster en Dirección y Gestión de la Seguridad de la Información en la Universidad Politécnica de Madrid
- ITIL v4 Foundation Certificate in IT Service Management. ITIL Certified
- IBM Security QRadar SIEM 7.1 Advanced. Avnet
- IBM Security QRadar SIEM 7.1 Foundations. Avnet

D. Gómez Rodríguez, Antonio

- Ingeniero Principal de Soluciones Cloud para Oracle
- Coorganizador de Malaga Developer Meetup
- Consultor Especialista para Sopra Group y Everis
- Líder de equipos en System Dynamics
- Desarrollador de Softwares en SGO Software
- Máster en E-Business por la Escuela de Negocios La Salle
- Postgrado en Tecnologías y Sistemas de Información, Instituto Catalán de Tecnología
- Licenciado en Ingeniería Superior de Telecomunicación por la Universidad Politécnica de Cataluña

D. Del Valle Arias, Jorge

- Smart City Solutions & Software Business Development Manager España. Itron, Inc
- Consultor IoT
- Director de Negocios Interino de IoT. TCOMET
- Responsable de la Unidad de Negocio IoT, Industria 4.0. Diode España
- Gerente de Área de Ventas de IoT y Telecomunicaciones. Aicox Soluciones
- Director Técnico (CTO) y Gerente de Desarrollo de Negocios. Consultoría TELYC
- Fundador y CEO de Sensor Intelligence
- Jefe de Operaciones y Proyectos. Codio
- Director de Operaciones en Codium Networks
- Ingeniero jefe de diseño de hardware y firmware. AITEMIN
- Jefe Regional de Planificación y Optimización RF - Red LMDS 3,5 GHz. Clearwire
- Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid
- Executive MBA por la International Graduate School de La Salle de Madrid
- Máster en Energías Renovables. CEPYME

D. Nogales Ávila, Javier

- Enterprise Cloud and Sourcing Senior Consultant en Quint
- Cloud and Technology Consultant en Indra
- Associate Technology Consultant en Accenture
- Graduado en Ingeniería de Organización Industrial por la Universidad de Jaén
- MBA en Administración y Dirección de Empresas por *ThePower Business School*

Dña. Jurado Jabonero, Lorena

- Responsable de Seguridad de la Información (CISO). Grupo Pascual
- Cybersecurity Manager. KPMG España
- Consultor de procesos TI / Control y Gestión de Proyectos de Infraestructura. Bankia
- Ingeniero Herramientas Explotación. Dalkia
- Desarrollador aplicaciones. Universidad Politécnica de Madrid
- Desarrollador. Grupo Banco Popular
- Graduada en Ingeniería Informática. Universidad Alfonso X El Sabio
- Ingeniero Técnico en Informática de Gestión. Universidad Politécnica de Madrid
- Certified Data Privacy Solutions Engineer (CDPSE). ISACA

D. Ortega Esteban, Octavio

- Especialista en marketing y desarrollo web
- Programador de aplicaciones informáticas y desarrollador de web *Freelance*
- *Chief Operating Officer* en Smallsquid SL
- Administrador de Ortega y Serrano e-Commerce
- Docente en cursos de Certificados de Profesionalidad en la rama de Informática y Comunicaciones
- Docente en cursos de Seguridad Informática
- Licenciado en Psicología por la Universidad Oberta de Catalunya
- Técnico Superior Universitario en Análisis, Diseño y Soluciones del *Software*
- Técnico Superior Universitario en Programación Avanzada

D. Embid Ruiz, Mario

- Abogado experto en TIC y protección de datos en Martínez-Echevarría Abogados
- Responsable legal de Branddocs SL
- Analista de riesgo en el Segmento Pymes de BBVA
- Docente en estudios de posgrado universitario relacionados con el Derecho
- Licenciatura en Derecho por la Universidad Rey Juan Carlos
- Licenciado en Administración y Dirección de Empresas por la Universidad Rey Juan Carlos
- Máster en Derecho de las Nuevas Tecnologías, Internet y Audiovisual por el Centro de Estudios Universitarios Villanueva

D. Rodrigo Estébanez, Juan Manuel

- Cofundador de Ismet Tech
- Gerente de Seguridad de la Información en Ecix Group
- Operational *Security Officer* en Atos IT Solutions and Services A/S
- Docente de Gestión de Ciberseguridad en estudios universitarios
- Graduado en Ingeniería por la Universidad de Valladolid
- Máster en Sistemas de Gestión Integrados por la Universidad CEU San Pablo

10

Titulación

La Maestría Oficial Universitaria en Seguridad Informática es un programa ofrecido por TECH Universidad que cuenta con Reconocimiento de Validez Oficial de Estudios (RVOE), otorgado por la Secretaría de Educación Pública (SEP) y, por tanto, tiene validez oficial en México.

Obtén un título oficial de Maestría en Seguridad Informática y da un paso adelante en tu carrera profesional"

El plan de estudios de esta Maestría Oficial Universitaria en Seguridad Informática se encuentra incorporado a la Secretaría de Educación Pública y al Sistema Educativo Nacional mexicano, mediante número de RVOE 20230354, de fecha 13/02/2023, en modalidad no escolarizada. Otorgado por la Dirección de Instituciones Particulares de Educación Superior (DIPES).

Al documento oficial de RVOE expedido por el SEP se puede acceder desde el siguiente enlace:

Ver documento RVOE

RVOE
EDUCACIÓN SUPERIOR

Supera con éxito este programa y recibe tu titulación oficial para ejercer con total garantía en un campo profesional exigente como Seguridad Informática"

Este título permitirá al alumno desempeñar las funciones profesionales al más alto nivel y su reconocimiento académico asegura que la formación cumple con los estándares de calidad y exigencia académica establecidos en México y a nivel internacional, garantizando la validez, pertinencia y competitividad de los conocimientos adquiridos para ponerlos en práctica en el entorno laboral.

Además, de obtener el título de Maestría Oficial Universitaria con el que podrá optar a puestos bien remunerados y de responsabilidad como profesional, este programa **permitirá al alumno el acceso a los estudios de nivel de Doctorado** con el que progresar en la carrera académica.

Título: **Maestría en Seguridad Informática**

No. de RVOE: **20230354**

Fecha de vigencia RVOE: **13/02/2023**

Modalidad: **100% online**

Duración: **20 meses**

*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.

Estados Unidos Mexicanos
Secretaría de Educación Pública
Dirección General de Acreditación, Incorporación y Revalidación
Constancia de Autenticación del Título Electrónico

Clave Única de Registro de Población

Folio Digital
https://www.siged.sep.gob.mx/titulos/utenticacion/

Datos del profesionista

Nombre(s)	Primer Apellido	Segundo Apellido

MAESTRÍA EN ________________

Nombre del perfil o carrera	Clave del perfil o carrera

Datos de la institución

TECH MÉXICO UNIVERSIDAD TECNOLÓGICA

Nombre

Número del Acuerdo de Reconocimiento de Validez Oficial de Estudios (RVOE)

Lugar y fecha de expedición

CIUDAD DE MÉXICO	
Entidad	Fecha

Responsables de la institución

RECTOR. GERARDO DANIEL OROZCO MARTÍNEZ

Firma electrónica de la autoridad educativa

Nombre:

Cargo: DIRECTORA DE REGISTROS ESCOLARES, OPERACIÓN Y EVALUACIÓN

No. Certificado: 00001000000510871752

Sello Digital: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Fecha de Autenticación:

La presente constancia de autenticación se expide como un registro fiel del trámite de autenticación a que se refiere el Artículo 14 de la Ley General de Educación Superior. La impresión de la constancia de autenticación acompañada del formato electrónico con extensión XML, que pertenece al título profesional, diploma o grado académico electrónico que generan las Instituciones, en papel bond, a color o blanco y negro, es válida y debe ser aceptada para realizar todo trámite inherente al mismo, en todo el territorio nacional.

La presente constancia de autenticación ha sido firmada mediante el uso de la firma electrónica, amparada por un certificado vigente a la fecha de su emisión y es válido de conformidad con lo dispuesto en el artículo 1; 2, fracciones IV, V, XIII y XIV; 3, fracciones I y II; 7; 8; 9; 13; 14; 16 y 25 de la Ley de Firma Electrónica Avanzada; 7 y 12 del Reglamento de la Ley de Firma Electrónica Avanzada.

La integridad y autoría del presente documento se podrá comprobar a través de la página electrónica de la Secretaría de Educación Pública por medio de la siguiente liga: https://www.siged.sep.gob.mx/titulos/autenticacion/, con el folio digital señalado en la parte superior de este documento. De igual manera, se podrá verificar el documento electrónico por medio del código QR.

11

Homologación del título

Para que el título universitario obtenido, tras finalizar la **Maestría Oficial Universitaria en Seguridad Informática**, tenga validez oficial en cualquier país, se deberá realizar un trámite específico de reconocimiento del título en la Administración correspondiente. TECH facilitará al egresado toda la documentación necesaria para tramitar su expediente con éxito.

Tras finalizar este programa recibirás un título académico oficial con Reconocimiento de Validez Oficial de Estudios (RVOE)"

Cualquier estudiante interesado en tramitar el reconocimiento oficial del título de **Maestría Oficial Universitaria en Seguridad Informática** en un país diferente a México, necesitará la documentación académica y el título emitido con la Apostilla de la Haya, que podrá solicitar al departamento de Servicios Escolares a través de correo electrónico: *homologacion@techtitute.com*.

La Apostilla de la Haya otorgará validez internacional a la documentación y permitirá su uso ante los diferentes organismos oficiales en cualquier país.

Una vez el egresado reciba su documentación deberá realizar el trámite correspondiente, siguiendo las indicaciones del ente regulador de la Educación Superior en su país. Para ello, TECH facilitará en el portal web una guía que le ayudará en la preparación de la documentación y el trámite de reconocimiento en cada país.

Con TECH podrás hacer válido tu título oficial de Maestría en cualquier país.

El trámite de homologación permitirá que los estudios realizados en TECH tengan validez oficial en el país de elección, considerando el título del mismo modo que si el estudiante hubiera estudiado allí. Esto le confiere un valor internacional del que podrá beneficiarse el egresado una vez haya superado el programa y realice adecuadamente el trámite.

El equipo de TECH le acompañará durante todo el proceso, facilitándole toda la documentación necesaria y asesorándole en cada paso hasta que logre una resolución positiva.

El procedimiento y la homologación efectiva en cada caso dependerá del marco normativo del país donde se requiera validar el título.

El equipo de TECH te acompañará paso a paso en la realización del trámite para lograr la validez oficial internacional de tu título"

12

Requisitos de acceso

La **Maestría Oficial Universitaria en Seguridad Informática** de TECH Universidad cuenta con el Registro de Validez Oficial de Estudios (RVOE) ente la Secretaría de Educación Pública (SEP). En consonancia con esa acreditación, los requisitos de acceso del programa académico se establecen en conformidad con lo exigido por el contexto normativo vigente.

Revisa los requisitos de acceso de esta Maestría Oficial Universitaria y prepárate para iniciar este itinerario académico con el que actualizarás todas tus competencias profesionales"

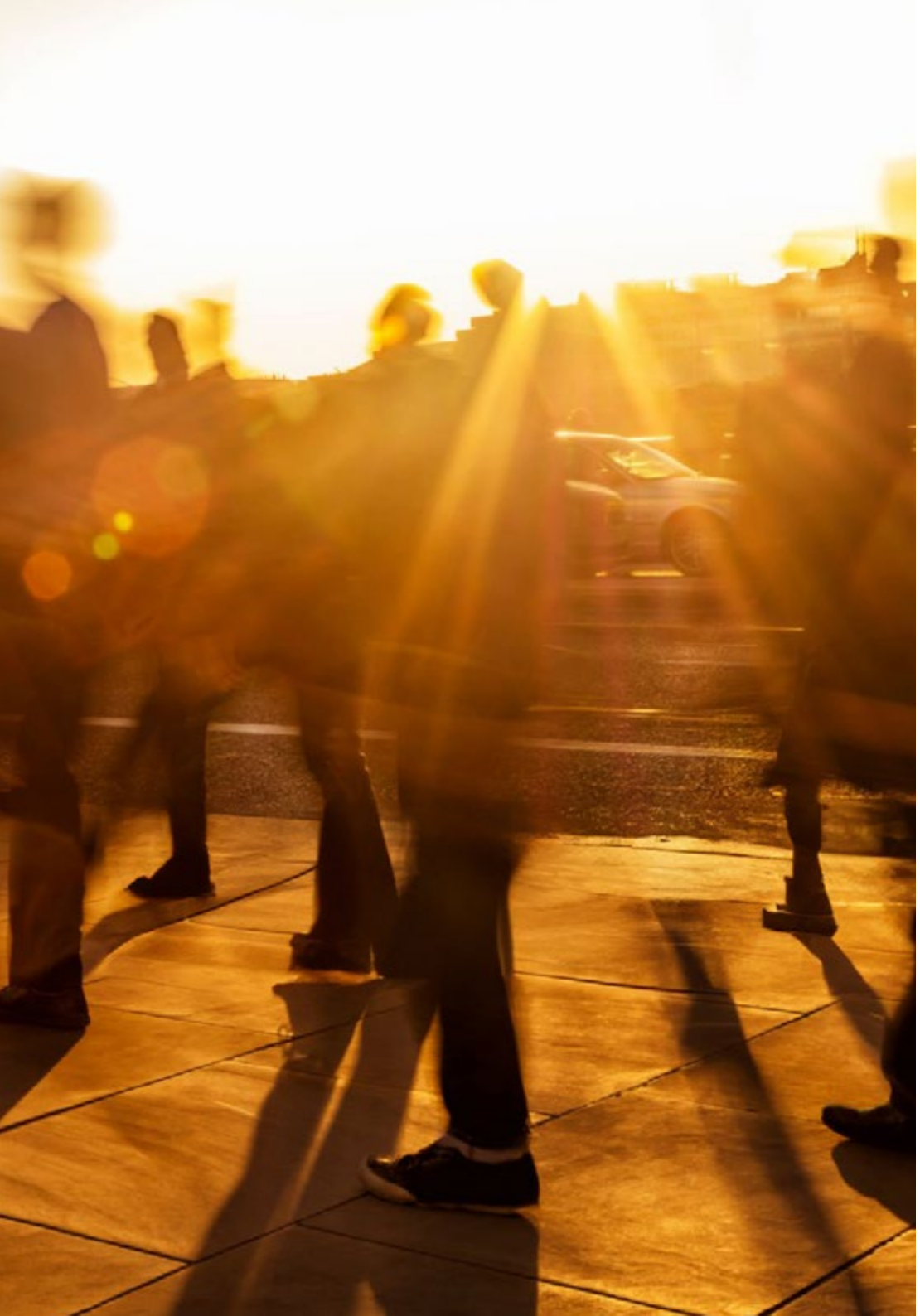
La norma establece que para inscribirse en la **Maestría Oficial Universitaria en Seguridad Informática** con Registro de Validez Oficial de Estudios (RVOE), es imprescindible cumplir con un perfil académico de ingreso específico.

Los candidatos interesados en cursar esta maestría oficial deben **haber finalizado los estudios de Licenciatura o nivel equivalente**. Haber obtenido el título será suficiente, sin importar a qué área de conocimiento pertenezca.

Aquellos que no cumplan con este requisito o no puedan presentar la documentación requerida en tiempo y forma, no podrán obtener el grado de Maestría.

Para ampliar la información de los requisitos de acceso al programa y resolver cualquier duda que surja al candidato, podrá ponerse en contacto con el equipo de TECH Universidad en la dirección de correo electrónico: *requisitosdeacceso@techtitute.com*.

Cumple con los requisitos de acceso y consigue ahora tu plaza en esta Maestría Oficial Universitaria.



Si cumples con el perfil académico de ingreso de este programa con RVOE, contacta ahora con el equipo de TECH y da un paso definitivo para impulsar tu carrera"

13

Proceso de admisión

El proceso de admisión de TECH es el más sencillo de todas las universidades online. Se podrá comenzar el programa sin trámites ni esperas: el alumno empezará a preparar la documentación y podrá entregarla más adelante, sin apuros ni complicaciones. Lo más importante para TECH es que los procesos administrativos sean sencillos y no ocasionen retrasos, ni incomodidades.

TECH Universidad ofrece el procedimiento de admisión a los estudios de Maestría Oficial Universitaria más sencillo y rápido de todas las universidades virtuales"

Para TECH lo más importante en el inicio de la relación académica con el alumno es que esté centrado en el proceso de enseñanza, sin demoras ni preocupaciones relacionadas con el trámite administrativo. Por ello, se ha creado un procedimiento más cómodo en el que podrá enfocarse desde el primer momento a su formación, contando con un plazo de tiempo para la entrega de la documentación pertinente.

Los pasos para la admisión son simples:

1. Facilitar los datos personales al asesor académico para realizar la inscripción.
2. Recibir un email en el correo electrónico en el que se accederá a la página segura de TECH y aceptar las políticas de privacidad y las condiciones de contratación e introducir los datos de tarjeta bancaria.
3. Recibir un nuevo email de confirmación y las credenciales de acceso al campus virtual.
4. Comenzar el programa en la fecha de inicio oficial.
   De esta manera, el estudiante podrá incorporarse al curso académico sin esperas. Posteriormente, se le informará del momento en el que se podrán ir enviando los documentos, a través del campus virtual, de manera muy práctica, cómoda y rápida. Sólo se deberán subir en el sistema para considerarse enviados, sin traslados ni pérdidas de tiempo.

Todos los documentos facilitados deberán ser rigurosamente válidos y estar en vigor en el momento de subirlos.

Los documentos necesarios que deberán tenerse preparados con calidad suficiente para cargarlos en el campus virtual son:
Copia digitalizada del documento que ampare la identidad legal del alumno (documento de identificación oficial, pasaporte, acta de nacimiento, carta de naturalización, acta de reconocimiento o acta de adopción)

- Copia digitalizada de Certificado de Estudios Totales de Bachillerato legalizado
  Para resolver cualquier duda que surja, el estudiante podrá realizar sus consultas a través del correo: *procesodeadmision@techtitute.com*.

Este procedimiento de acceso te ayudará a iniciar tu Maestría Oficial Universitaria cuanto antes, sin trámites ni demoras.

tech universidad

Nº de RVOE: 20230354

Maestría Oficial Universitaria
Seguridad Informática

Idioma: **Español**

Modalidad: **100% online**

Duración: **20 meses**

Fecha de vigencia RVOE: **13/02/2023**

Maestría Oficial Universitaria
Seguridad Informática

Nº de RVOE: 20230354

RVOE
EDUCACIÓN SUPERIOR

tech universidad