Maestría

Seguridad Informática (Ciberseguridad)

Nº de RVOE: 20230354

RVOE
EDUCACIÓN SUPERIOR

tech universidad

tech universidad

Nº de RVOE: 20230354

Maestría

Seguridad Informática (Ciberseguridad)

Idioma: **Español**

Modalidad: **100% en línea**

Duración: **20 meses**

Fecha acuerdo RVOE: **10/02/2023**

Acceso web: www.techtitute.com/mx/informatica/maestria/maestria-seguridad-informatica-ciberseguridad

Índice

01

Presentación

Las herramientas informáticas han transformado la manera en que el mundo gestiona divisas y accede a la información, entre otros muchos aspectos. Esos avances han generado grandes volúmenes de datos sensibles, con altas probabilidades de ser vulnerados por ataques informáticos. En ese contexto, las empresas y organismos públicos reclaman cada vez más de expertos en Ciberseguridad, convirtiendo a esa especialidad en una de las más demandas del mercado profesional actual. TECH, ante ese contexto, presenta una titulación que recoge los contenidos más actualizados en esa materia. Además, los presenta de manera 100% online, en su innovadora plataforma de aprendizaje, dando a cada estudiante la oportunidad de autogestionar sus progresos de manera personalizada.

Conviértete en un experto en Ciberseguridad de la mano de TECH con un programa exhaustivo y 100% online de referencia en el mercado pedagógico"

La Ciberseguridad se ha convertido en una preocupación de primer orden para empresas privadas y organismos públicos. Esto se debe a que, gracias a los adelantos de la era digital, el mundo se ha informatizado a una acelerada velocidad, generando grandes volúmenes de datos que pueden ser fácilmente vulnerados por ciberataques. Con el afán de dar a sus clientes y usuarios mejores garantías de protección sobre su información personal y comportamiento en la web, las compañías reclaman de la asistencia especializada de expertos en Seguridad Informática. De ese modo, área del conocimiento han conseguidos niveles de competitividad hasta hace poco tiempo insospechados.

No obstante, la cualificación es indispensable en ese ámbito. Por eso, TECH lanza esta Maestría en Seguridad Informática (Ciberseguridad). A través de ella, el alumno analizará los últimos criterios en materia de criptografía digital y gestión de la seguridad tecnológica. Por otro lado, ahondará en los protocolos y estrategia más eficientes para salvaguardar datos en la nube y para blindar equipos conectados por medio del Internet de las Cosas. Igualmente, examinará las políticas y normativas que protegen hoy a los usuarios en caso de que ser víctimas de un ciberataque. Además, se abordarán las metodologías más eficientes de *hacking* ético y aquellas herramientas que facilitan el trabajo de los peritos informáticos.

Todo esos esos contenidos estarán presentes en una plataforma 100% online, acompañados de recursos multimedia como vídeos, infografías y resúmenes interactivos. Al mismo tiempo, el alumno no tendrá que preocuparse por horarios preestablecidos ni rígidos cronogramas didácticos a la hora de acceder a ellos. Por el contrario, tendrá todas las facilidades para autogestionar sus progresos de manera personalizada, de acuerdo con sus necesidades individuales. Para garantizar la asimilación más rápida y flexible de las habilidades prácticas más demandas dentro de esta especialidad, TECH también ha dispuesto métodos pedagógicos exhaustivos. Así, con ayuda del *Relearning* y el análisis de casos reales, los egresados conseguirán sus metas académicas y desarrollarán un perfil profesional polivalente.

TECH brinda la oportunidad de obtener la Maestría en Seguridad Informática (Ciberseguridad) en un formato 100% en línea, con titulación directa y un programa diseñado para aprovechar cada tarea en la adquisición de competencias para desempeñar un papel relevante en la empresa. Pero, además, con este programa, el estudiante tendrá acceso al estudio de idiomas extranjeros y formación continuada de modo que pueda potenciar su etapa de estudio y logre una ventaja competitiva con los egresados de otras universidades menos orientadas al mercado laboral.

Un camino creado para conseguir un cambio positivo a nivel profesional, relacionándose con los mejores y formando parte de la nueva generación de informáticos capaces de desarrollar su labor en cualquier lugar del mundo.

Con esta titulación, aprenderás a identificar y delimitar los riesgos de seguridad IT por medio del uso práctico de herramientas modernas de auditoría y peritaje informático"

02

Plan de estudios

Los docentes de TECH han conformado, para esta titulación, un plan de estudios de excelencia donde se recogen los contenidos más innovadores en materia de Seguridad Informática. Específicamente, el temario abarca las últimas tendencias de protección y detección de amenazas en los entornos *cloud*, dispositivos vinculados mediante el Internet de las Cosas y en operaciones de software. Asimismo, ahonda en todas las herramientas de criptografía que proliferan en la actualidad y como usarlas para compartimentar información e identificar debidamente a sus usuarios.

100% online y sin horarios preestablecidos: así encontrarás los módulos académicos que forman parte de esta Maestría de TECH"

Por otro lado, para esta experiencia educativa, TECH ha implementado metodologías didácticas de elevado rigor. Entre ellas resalta el *Relearning*, estrategia educativa basada en la repetición de los contenidos bajo criterios pedagógicos de excelencia. Además, está presente el análisis y simulación de casos reales. Ambos promueven el desarrollo de habilidades prácticas inmediatas en el alumno.

Asimismo, cada estudiante tendrá la oportunidad de autogestionar sus progresos de aprendizaje desde una plataforma 100% online, con múltiples recursos interactivos. En particular, ofrece una amplia gama de materiales multimedia como vídeos e infografías. Todos ellos han sido diseñados para ayudar en la asimilación de nuevos y complejos conceptos de interés.

El mejor material didáctico ha sido integrado por TECH en esta titulación para que puedas convertirte en un experto en Ciberseguridad con rapidez y flexibilidad"

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

Dónde, cuándo y cómo se imparte

Esta Maestría se ofrece 100% en línea, por lo que el alumno podrá cursarla desde cualquier sitio, haciendo uso de una computadora, una tableta o simplemente mediante su smartphone.

Además, podrá acceder a los contenidos tanto *online* como *offline*. Para hacerlo *offline* bastará con descargarse los contenidos de los temas elegidos, en el dispositivo y abordarlos sin necesidad de estar conectado a internet.

El alumno podrá cursar la Maestría a través de sus 10 módulos, de forma autodirigida y asincrónica. Adaptamos el formato y la metodología para aprovechar al máximo el tiempo y lograr un aprendizaje a medida de las necesidades del alumno.

> *Esta titulación se ajusta a tus horarios y necesidades de estudio sin imponer rígidos cronogramas para que, en todo momento, puedas personalizar tus progresos académicos"*

Módulo 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)

Módulo 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

Módulo 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)

Módulo 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
- 4.3.2. 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

Módulo 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

Módulo 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

Módulo 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. 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

Módulo 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

Módulo 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

Módulo 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
10.9.3. 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

03
Objetivos

Este programa es idóneo para aquellos alumnos que, además de lograr un puesto competitivo de empleo, quieren resaltar en el panorama informático por su dominio de las herramientas de trabajo más actualizadas. Cumplirán sus metas de preparación a través de diversos objeticos académicos. Al completar el estudio de sus diferentes módulos, el egresado contará con las competencias más solicitadas por este competitivo mercado profesional. De manera global, estará listo para enfrentar los retos de diversa complejidad y aportar soluciones innovadoras.

Matricúlate cuanto antes en esta titulación y conseguirás ponerte al día sobre los softwares y herramientas de peritaje informático más potentes en el marco de la Ciberseguridad"

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 y desarrollar el concepto de riesgo, incertidumbre dentro del entorno en que vivimos
- Examinar el Modelo de Gestión de Riesgos basado en la ISO 31.000
- Examinar la ciencia de la criptología y la relación con sus ramas: criptografía, criptoanálisis, esteganografía y estegoanálisis
- Analizar los tipos de criptografía según el tipo de algoritmo y según su uso
- Examinar los certificados digitales
- Examinar la Infraestructura de Clave Pública (PKI)
- Desarrollar el concepto de gestión de identidades
- Identificar los métodos de autenticación
- 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
- Desarrollar las especificaciones de seguridad de cada tecnología LPWAN
- Analizar de forma comparativa la seguridad de las tecnologías LPWAN

Objetivos específicos

Módulo 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

Módulo 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
- Determinar las reglas de acceso al sistema y detectar intrusos

Módulo 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

Módulo 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
- Implementar buenas prácticas en programación orientadas a dispositivos móviles

Módulo 5. Seguridad en Internet de las Cosas

- Abordar las principales arquitecturas de Internet de las Cosas
- Dominar las tecnologías de conectividad y desarrollar los principales protocolos de aplicación
- Evaluar los niveles de riesgo y vulnerabilidades conocidas para implementar políticas de uso seguras

Módulo 6. Hackeo Ético

- Indagar en los métodos de inteligencia de fuentes abiertas
- Recopilar la información disponible en medios públicos
- 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

Módulo 7. Ingeniería Inversa

- Reconocer las fases de un compilador
- 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

Módulo 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

Módulo 9. Análisis Forense

- Identificar los diferentes elementos que ponen en evidencia un delito informático
- Obtener los datos de los diferentes medios antes de que se pierdan
- 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

Módulo 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
- Enfrentar los nuevos retos de seguridad y evitar la suplantación de identidad

Alcanza tus objetivos y metas profesionales gracias a las competencias que adquirirás egresándote de esta Maestría 100% online"

04
Competencias

Esta Maestría nace con la finalidad de proporcionar al alumno una especialización de alta calidad. Así, tras superar con éxito esta exclusiva titulación, el egresado habrá desarrollado las habilidades y destrezas necesarias para desempeñar un trabajo de primer nivel. Asimismo, obtendrá una visión innovadora y multidisciplinar de su campo laboral. Por ello, este vanguardista programa de TECH representa una oportunidad sin parangón para todo aquel profesional que quiera destacar en su sector y convertirse en un experto.

Impulsa tu carrera y tus metas profesionales con esta Maestría 100% online de TECH”

Competencias generales

- Aplicar las medidas de seguridad más adecuadas dependiendo de las amenazas
- Determinar la política y plan de seguridad en el sistema de información de una compañía, completando el diseño y puesta en marcha del Plan de Contingencia
- Establecer un programa de auditorías que cubra las necesidades de autoevaluación de la organización en materia de ciberseguridad
- Desarrollar un programa de análisis y control de vulnerabilidades y un plan de respuesta a incidentes de ciberseguridad
- Maximizar las oportunidades que se presenten y eliminar la exposición a todos los posibles riesgos desde el propio diseño
- Compilar los sistemas de gestión de claves
- Evaluar la seguridad de la información de una compañía
- Analizar los sistemas de acceso a la información
- Desarrollar las mejores prácticas en el desarrollo seguro
- Presentar los riesgos que supone a las compañías no tener un entorno de seguridad informática
- Desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI)
- Identificar los elementos claves que conforman un SGSI
- Aplicar la metodología MAGERIT para evolucionar el modelo y llevarlo un paso más allá
- Diseñar nuevas metodologías de gestión de riesgos propias, basadas en el concepto *agile Risk Management*

- Identificar, analizar, evaluar y tratar los riesgos a los que se enfrenta el profesional desde una nueva perspectiva empresarial basada en un modelo Risk-Driven o impulsado por el riesgo que permita no sólo sobrevivir en propio entorno, sino impulsar el aporte de valor propio
- Examinar el proceso de diseño de una estrategia de seguridad al desplegar servicios corporativos en *Cloud*
- Evaluar las diferencias en las implementaciones concretas de diferentes vendedores de *Cloud* pública
- Evaluar las opciones de conectividad IoT para afrontar un proyecto, con especial énfasis en tecnologías LPWAN
- Presentar las especificaciones básicas de las principales tecnologías LPWAN para el IoT

Actualiza tus competencias con la metodología teórico-práctica más eficiente del panorama académico actual, el Relearning de TECH"

05

¿Por qué nuestro programa?

En esta Maestría, los alumnos de TECH encontrarán un programa hecho a la medida de sus necesidades de superación. Así, dispone de un completísimo temario que se ajusta y pone en vigor la última evidencia científica. Al mismo tiempo, se trata de una titulación donde cada estudiante tendrá acceso a un claustro de excelencia y podrá aclarar dudas y conceptos de interés en todo momento. Igualmente, el aprendizaje será accesible desde cualquier punto geográfico gracias a una plataforma de aprendizaje 100% online, interactiva y con múltiples recursos multimedia.

Con la simple ayuda de un dispositivo conectado a Internet, podrás acceder a los contenidos de este programa y convertirte en un experto en Ciberseguridad de prestigio"

01

Orientación 100% laboral

Con esta Maestría, el estudiante tendrá acceso a los mejores materiales didácticos del mercado. Todos ellos, además, concebidos con un enfoque eminentemente profesionalizante, es decir, que permiten al alumno trabajar en Ciberseguridad cuanto antes. Es todo un lujo que, solo estudiando en TECH, es posible.

02

La mejor institución

Estudiar en TECH Universidad supone una apuesta de éxito a futuro, que garantiza al estudiante una estabilidad profesional y personal. Gracias a los mejores contenidos académicos, 100% en línea, y al profesorado de esta Maestría, el alumno se asegura la mejor especialización del mercado. Y todo ello, desde casa y sin renunciar a su actividad profesional y personal.

03

Titulación directa

No hará falta que el estudiante haga una tesina, ni examen final, ni nada más para poder egresar y obtener su título. En TECH, el alumno tendrá una vía directa de titulación.

04

Los mejores recursos pedagógicos 100% en línea

TECH Universidad pone al alcance de los estudiantes de esta Maestría la última metodología educativa en línea, basada en una tecnología internacional de vanguardia, que permite estudiar sin tener que asistir a clase, y sin renunciar a adquirir ninguna competencia indispensable en materia de Seguridad Informática.

05

Educación adaptada al mundo real

TECH Universidad muestra al alumno las últimas tendencias, avances y estrategias para el ejercicio de la Ciberseguridad. Para ello contará con diversas herramientas didácticas como casos reales simulados y el *Relearning*. Ambas herramientas educativas se afanarán en perfeccionar sus habilidades prácticas y en convertirle en un profesional de élite.

06

Aprender idiomas y obtener su certificado oficial

TECH da la posibilidad, además de obtener la certificación oficial de Inglés en el nivel B2, de seleccionar de forma optativa hasta otros 6 idiomas en los que, si el alumno desea, podrá certificarse.

07 Especialización integral

En TECH Universidad, el profesional adquirirá una visión global acerca de las competencias y responsabilidades que debe poseer un experto en Seguridad Informática. Así conocerá como gestionar aspectos legislativos, tecnológicos e investigativos, hasta convertirse en un activo de primer nivel.

08 Innovaciones tecnológicas

A través de esta Maestría, el alumno tendrá acceso a las estrategias y procedimientos informáticas que garantizan la seguridad de los sistemas digitales. Asimismo, analizará una amplia gama de dispositivos y herramientas capaces de identificar el origen y alcance de un ataque reportado como una incidencia posterior.

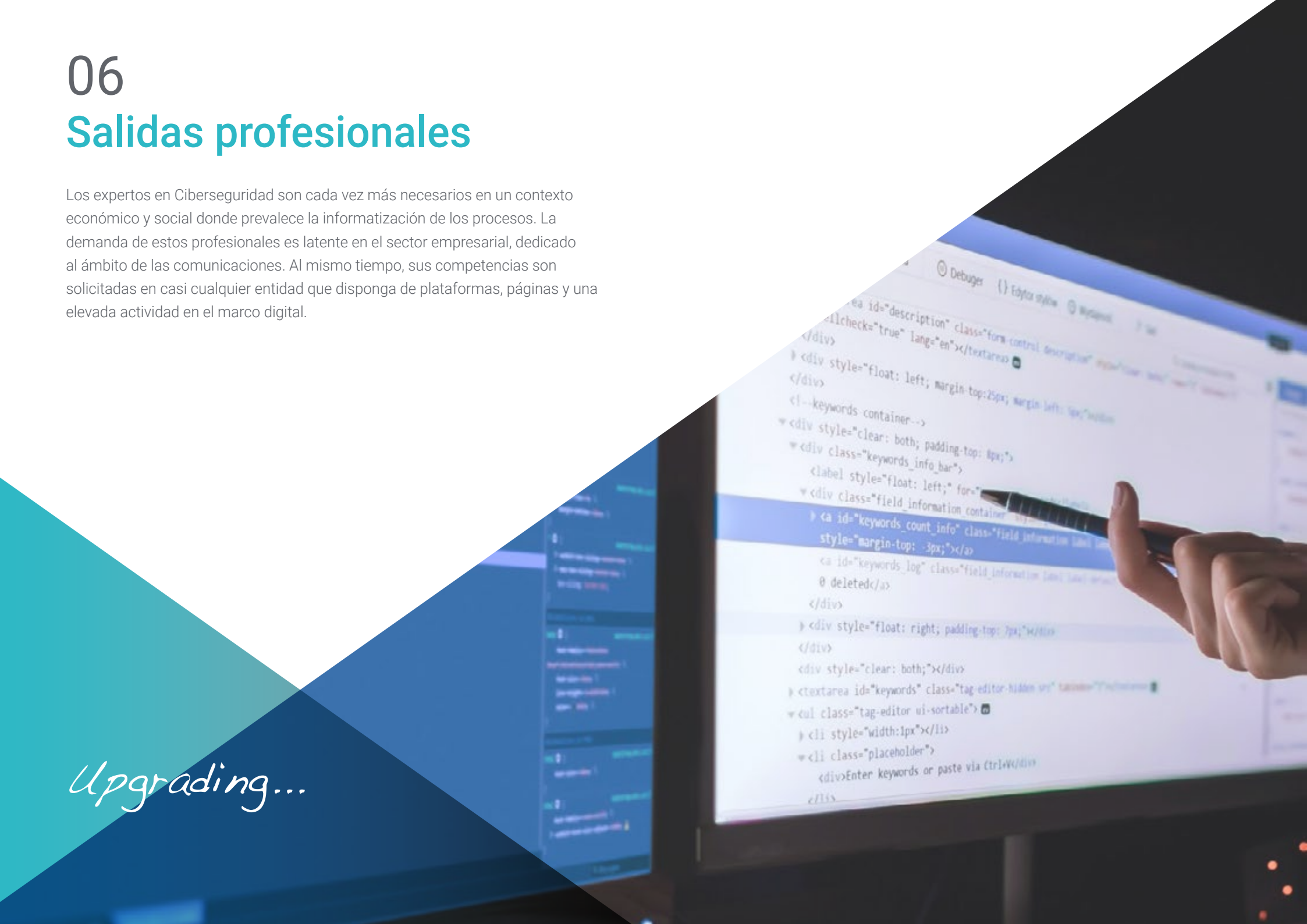
09 Formar parte de una comunidad exclusiva

Estudiando en TECH, el ingeniero en Ciberseguridad tendrá acceso a una comunidad de profesionales de élite, grandes instituciones educativas, centros escolares de renombre y profesores cualificados procedentes de las universidades más prestigiosas del mundo: la comunidad TECH.

06

Salidas profesionales

Los expertos en Ciberseguridad son cada vez más necesarios en un contexto económico y social donde prevalece la informatización de los procesos. La demanda de estos profesionales es latente en el sector empresarial, dedicado al ámbito de las comunicaciones. Al mismo tiempo, sus competencias son solicitadas en casi cualquier entidad que disponga de plataformas, páginas y una elevada actividad en el marco digital.



Este programa ha sido diseñado para solucionar tus necesidades de superación profesional en materia de seguridad con totales garantías"

Perfil profesional

En su perfil profesional, el experto en Ciberseguridad debe poseer destrezas en dos campos fundamentales. Por un lado, debe ser capaz de crear por sí mismo mecanismos de contención y detección de amenazas. A su vez, entre sus competencias debe dominar los marcos legales y políticos que regularizan el monitoreo de la información y los datos. Los egresados de esta titulación de TECH conseguirán un elevado conocimiento de todos esos aspectos gracias a los rigurosos contenidos de su temario académico.

Perfil investigativo

Como parte de esta Maestría, TECH prepara a sus alumnos para estar al día sobre los adelantos más significativos de la Seguridad Informática. Al mismo tiempo, aspira que todos sus egresados sean capaces de incorporar nuevas herramientas y descubrir soluciones más efectivas para la protección de información, datos y otros componentes digitales. Ese marcado exponente de investigación y análisis formará parte de sus perfiles y podrán aplicar todas las metodologías de investigación en su ejercicio laboral cotidiano.

Gracias a TECH y la preparación que recibas en esta titulación, ocuparás un puesto laboral competitivo y exigente de manera inmediata"

Perfil ocupacional y campo de acción

Tras completar esta Maestría en Seguridad Informática (Ciberseguridad), los alumnos de TECH podrán asumir retos en empleos diversos. Esta titulación los habrá capacitados para asumir tareas que requieren de los conocimientos teóricos más precisos y disímiles habilidades prácticas. Así, conseguirá realizar con eficiencia auditorías, análisis forenses y aplicar el *sandboxing* en entornos diversos.

El egresado de TECH en Seguridad Informática (Ciberseguridad) estará preparado para desempeñar los siguientes puestos de trabajo:

- Analista de Seguridad Informática
- Administrador de sistemas y redes
- Perito Informático
- Director tecnológico en empresas informáticas
- Chief Information Security Officer
- Arquitecto de Ciberseguridad
- Consultor auditor de Seguridad Informática
- Hacker ético
- Pentester

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 en la Maestría, podrá aprender idiomas de un modo sencillo y práctico.

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

En el mundo competitivo de hoy, 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 certificado oficial que acredite y reconozca nuestra competencia en aquellos que dominemos. De hecho, ya son muchos las escuelas, las universidades y las empresas que sólo aceptan a candidatos que certifican su nivel mediante un certificado 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 poseemos.

TECH ofrece 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 *online*, el enfoque orientado a la acción y el enfoque de adquisición de compentencia lingüística, con la finalidad de prepararte para los exámenes oficiales de certificación de nivel.

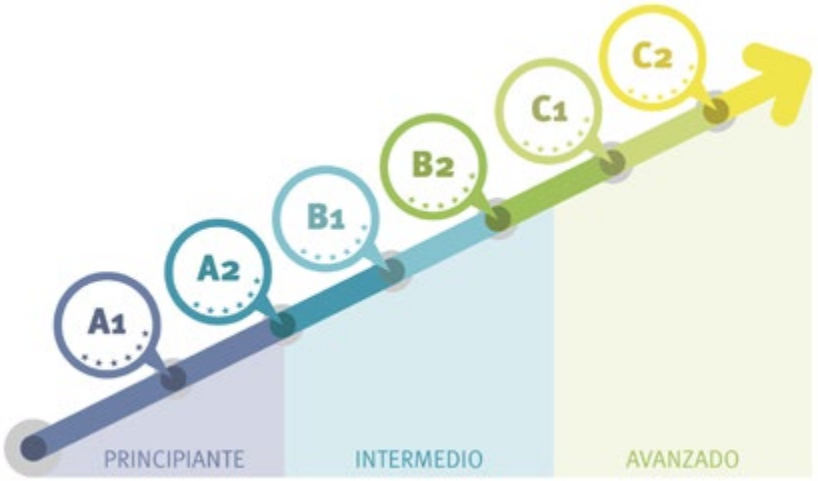
El estudiante aprenderá, mediante actividades en contextos reales, la resolución de situaciones cotidianas de comunicación en entornos simulados de aprendizaje y se enfrentará a simulacros de examen para la preparación de la prueba de certificación de nivel.

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"

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

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, 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
- Podrá presentarse a un único examen telepresencial de certificación de nivel, con un profesor nativo experto en evaluación lingüística. Si supera 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 única de cualquier idioma, están incluidas en la maestría



08
Metodología

Este programa de capacitación ofrece una forma diferente de aprender. Nuestra metodología se desarrolla a través de un modo de aprendizaje de forma cíclica: ***el Relearning***.
Este sistema de enseñanza es utilizado, por ejemplo, en las facultades de medicina más prestigiosas del mundo y se ha considerado uno de los más eficaces por publicaciones de gran relevancia como el ***New England Journal of Medicine.***

Descubre el Relearning, un sistema que abandona el aprendizaje lineal convencional para llevarte a través de sistemas cíclicos de enseñanza: una forma de aprender que ha demostrado su enorme eficacia, especialmente en las materias que requieren memorización"

Estudio de Caso para contextualizar todo el contenido

Nuestro programa ofrece un método revolucionario de desarrollo de habilidades y conocimientos. Nuestro objetivo es afianzar competencias en un contexto cambiante, competitivo y de alta exigencia.

Con TECH podrás experimentar una forma de aprender que está moviendo los cimientos de las universidades tradicionales de todo el mundo"

Accederás a un sistema de aprendizaje basado en la reiteración, con una enseñanza natural y progresiva a lo largo de todo el temario.

El alumno aprenderá, mediante actividades colaborativas y casos reales, la resolución de situaciones complejas en entornos empresariales reales.

Un método de aprendizaje innovador y diferente

El presente programa de TECH es una enseñanza intensiva, creada desde 0, que propone los retos y decisiones más exigentes en este campo, ya sea en el ámbito nacional o internacional. Gracias a esta metodología se impulsa el crecimiento personal y profesional, dando un paso decisivo para conseguir el éxito. El método del caso, técnica que sienta las bases de este contenido, garantiza que se sigue la realidad económica, social y profesional más vigente.

> *Nuestro programa te prepara para afrontar nuevos retos en entornos inciertos y lograr el éxito en tu carrera"*

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de Informática del mundo desde que éstas existen. Desarrollado en 1912 para que los estudiantes de Derecho no solo aprendiesen las leyes a base de contenidos teóricos, el método del caso consistió en presentarles situaciones complejas reales para que tomasen decisiones y emitiesen juicios de valor fundamentados sobre cómo resolverlas. En 1924 se estableció como método estándar de enseñanza en Harvard.

Ante una determinada situación, ¿qué debería hacer un profesional? Esta es la pregunta a la que te enfrentamos en el método del caso, un método de aprendizaje orientado a la acción. A lo largo del curso, los estudiantes se enfrentarán a múltiples casos reales. Deberán integrar todos sus conocimientos, investigar, argumentar y defender sus ideas y decisiones.

Relearning Methodology

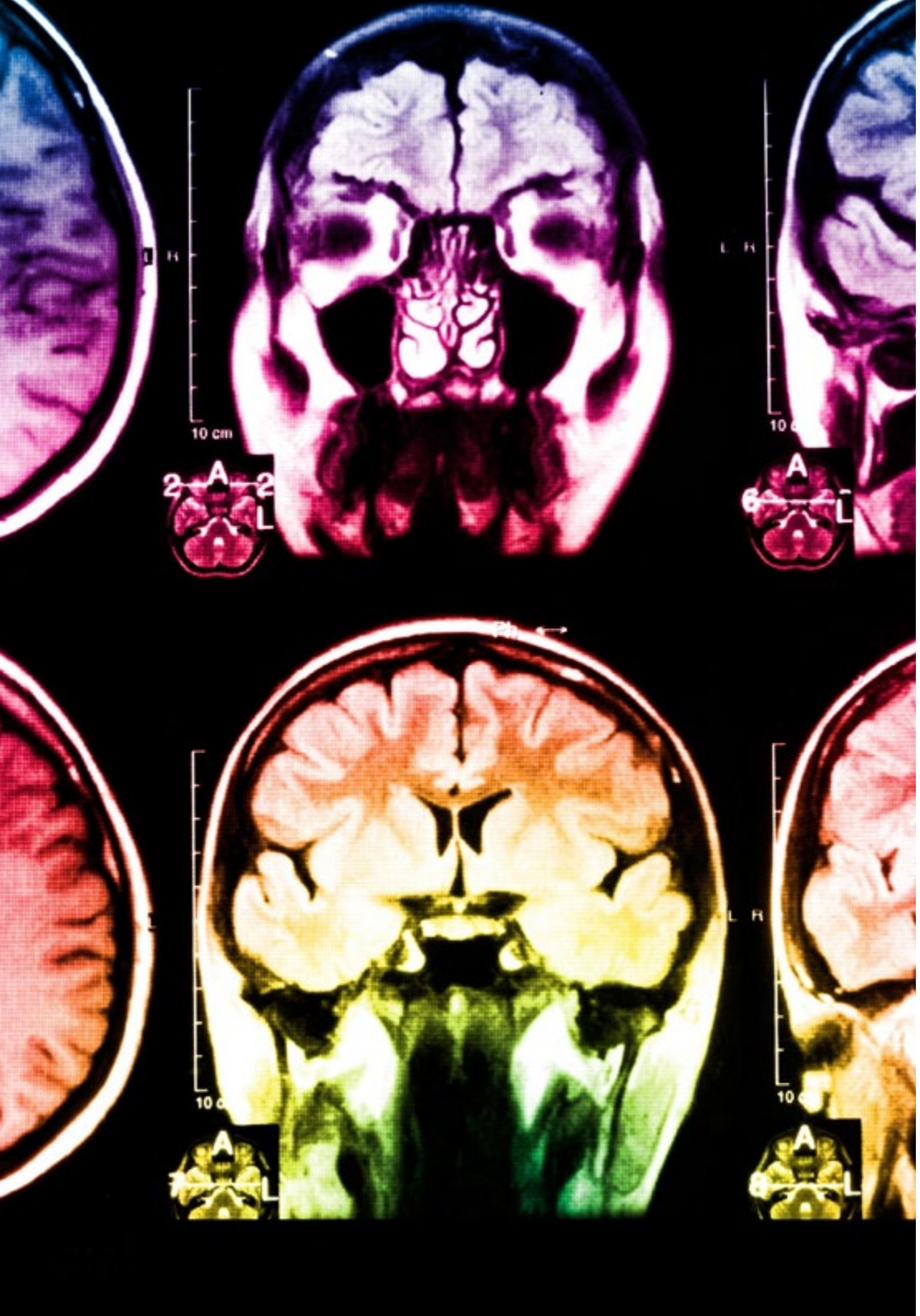
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

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

En 2019 obtuvimos los mejores resultados de aprendizaje de todas las universidades online en español en el mundo.

En TECH aprenderás con una metodología vanguardista concebida para capacitar a los directivos del futuro. Este método, a la vanguardia pedagógica mundial, se denomina Relearning.

Nuestra universidad es la única en habla hispana licenciada para emplear este exitoso método. En 2019, conseguimos mejorar los niveles de satisfacción global de nuestros alumnos (calidad docente, calidad de los materiales, estructura del curso, objetivos…) con respecto a los indicadores de la mejor universidad online en español.



En nuestro programa, el aprendizaje no es un proceso lineal, sino que sucede en espiral (aprender, desaprender, olvidar y reaprender). Por eso, se combinan cada uno de estos elementos de forma concéntrica. Con esta metodología se han capacitado más de 650.000 graduados universitarios con un éxito sin precedentes en ámbitos tan distintos como la bioquímica, la genética, la cirugía, el derecho internacional, las habilidades directivas, las ciencias del deporte, la filosofía, el derecho, la ingeniería, el periodismo, la historia o los mercados e instrumentos financieros. Todo ello en un entorno de alta exigencia, con un alumnado universitario de un perfil socioeconómico alto y una media de edad de 43,5 años.

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

A partir de la última evidencia científica en el ámbito de la neurociencia, no solo sabemos organizar la información, las ideas, las imágenes y los recuerdos, sino que sabemos que el lugar y el contexto donde hemos aprendido algo es fundamental para que seamos capaces de recordarlo y almacenarlo en el hipocampo, para retenerlo en nuestra memoria a largo plazo.

De esta manera, y en lo que se denomina Neurocognitive context-dependent e-learning, los diferentes elementos de nuestro programa están conectados con el contexto donde el participante desarrolla su práctica profesional.

Este programa ofrece los mejores materiales educativos, preparados a conciencia para los profesionales:

Material de estudio

Todos los contenidos didácticos son creados por los especialistas que van a impartir el curso, específicamente para él, de manera que el desarrollo didáctico sea realmente específico y concreto.

Estos contenidos son aplicados después al formato audiovisual, para crear el método de trabajo online de TECH. Todo ello, con las técnicas más novedosas que ofrecen piezas de gran calidad en todos y cada uno los materiales que se ponen a disposición del alumno.

Clases magistrales

Existe evidencia científica sobre la utilidad de la observación de terceros expertos.

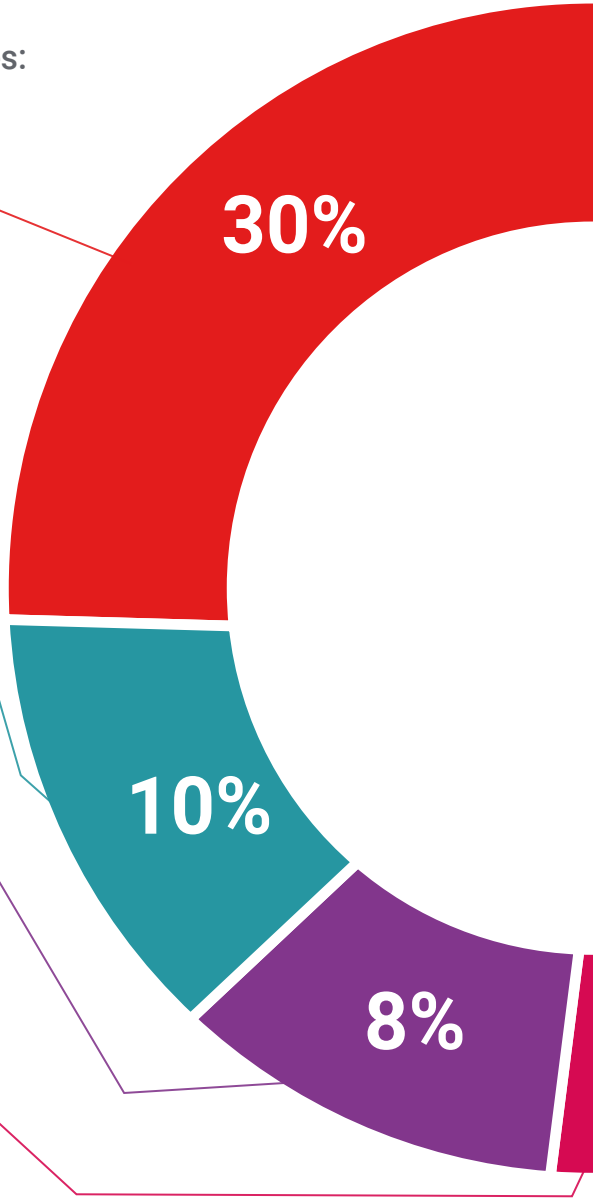
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

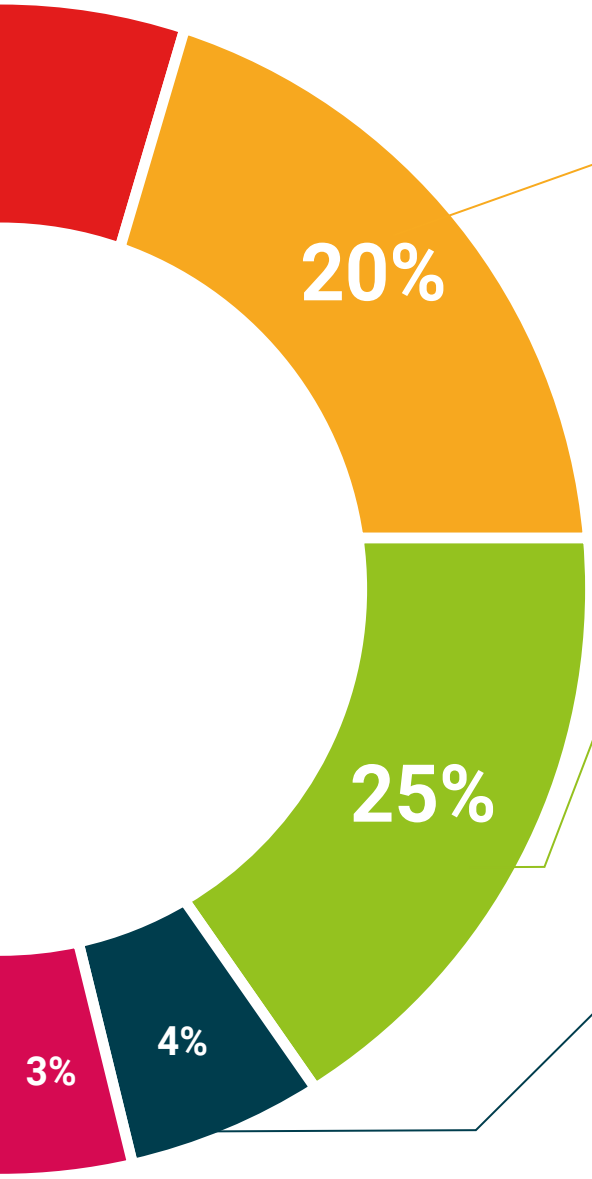
Prácticas de habilidades y competencias

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

Lecturas complementarias

Artículos recientes, documentos de consenso y guías internacionales, entre otros. En la biblioteca virtual de TECH el estudiante tendrá acceso a todo lo que necesita para completar su capacitación.





Case studies

Completarán una selección de los mejores casos de estudio elegidos expresamente para esta titulación. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.

Resúmenes interactivos

El equipo de TECH presenta los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audios, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

Este exclusivo sistema educativo para la presentación de contenidos multimedia fue premiado por Microsoft como "Caso de éxito en Europa".

Testing & Retesting

Se evalúan y reevalúan periódicamente los conocimientos del alumno a lo largo del programa, mediante actividades y ejercicios evaluativos y autoevaluativos para que, de esta manera, el estudiante compruebe cómo va consiguiendo sus metas.

09

Dirección del curso

TECH ha seleccionado de manera minuciosa a los docentes que integran el claustro de esta titulación. Su trayectoria, en activo, les permite estar al día sobre los principales adelantos en materia de software y hardware para garantizar la seguridad de sistemas informáticos. Sus conocimientos y experiencias prácticas han quedado volcadas en un completísimo temario. Además, a lo largo de la titulación, ofrecerá al alumno una guía personalizada con la cual se aclararán dudas y conceptos de interés.

TECH ha elegido a los mejores docentes para conformar el plan de estudios con el que te especializarás de manera rápida y flexible en Seguridad Informática"

Dirección

Dr. Olalla Bonal, Martín

- Gerente Senior de Práctica de Blockchain en EY
- Especialista Técnico Cliente Blockchain para IBM
- Director de Arquitectura para Blocknitive
- Coordinador Equipo 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. 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. 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*

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. 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

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

Requisitos de acceso y proceso de admisión

El proceso de admisión de TECH es el más sencillo de las universidades en línea en todo el país. Podrás comenzar la Maestría sin trámites ni demoras: empieza a preparar la documentación y entrégala más adelante, sin premuras. Lo más importante para TECH es que los procesos administrativos, para ti, sean sencillos y no te ocasionen retrasos, ni incomodidades.

Ayudándote desde el inicio, TECH ofrece el procedimiento de admisión más sencillo y rápido de todas las universidades en línea del país"

Requisitos de acceso

Los programas con Registro de Validez Oficial de Estudios registrados ante la Autoridad Educativa, requieren de un perfil académico de ingreso que es requisito indispensable para poder realizar la inscripción.

Para poder acceder a los estudios de Maestría en Seguridad Informática (Ciberseguridad) es necesario haber concluido una licenciatura o equivalente, 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 nunca el título de Maestría.

Proceso de admisión

Para TECH es del todo fundamental que, en el inicio de la relación académica, el alumno esté centrado en el proceso de enseñanza, sin demoras ni preocupaciones relacionadas con el trámite administrativo. Por ello, hemos creado un protocolo más sencillo en el que podrás concentrarte, desde el primer momento en tu capacitación, contando con un plazo mucho mayor de tiempo para la entrega de la documentación pertinente.

De esta manera, podrás incorporarte al curso tranquilamente. Algún tiempo más tarde, te informaremos del momento en el que podrás ir enviando los documentos, a través del campus virtual, de manera muy sencilla, cómoda y rápida. Sólo deberás cargarlos y enviarlos, sin traslados ni pérdidas de tiempo.

Una vez que llegue el momento podrás contar con nuestro soporte, si te hace falta

Todos los documentos que nos facilites deberán ser rigurosamente ciertos y estar en vigor en el momento en que los envías.

Estudiantes con estudios universitarios realizados en México

En cada caso, los documentos que debes tener listos para cargar en el campus virtual son:

Deberán subir al Campus Virtual, escaneados con calidad suficiente para su lectura, los siguientes documentos:

- Copia digitalizada del documento que ampare la identidad legal del alumno: acta de nacimiento, carta de naturalización, acta de reconocimiento, acta de adopción, Cédula de Identificación Personal o Documento Nacional de Identidad, Pasaporte, Certificado Consular o, en su caso, Documento que demuestre el estado de refugiado
- Copia digitalizada de la Clave Única de Registro de Población (CURP)
- Copia digitalizada de Certificado de Estudios Totales de Licenciatura legalizado
- Copia digitalizada del título legalizado

En caso de haber estudiado la licenciatura fuera de méxico, consulta con tu asesor académico. Se requerirá documentación adicional en casos especiales, como inscripciones a la maestría como opción de titulación o que no cuenten con el perfil académico que el plan de estudios requiera. Tendrás un máximo de 2 meses para cargar todos estos documentos en el campus virtual.

Estudiantes con estudios universitarios realizados fuera de México

Deberán subir al Campus Virtual, escaneados con calidad suficiente para su lectura, los siguientes documentos:

- Copia digitalizada del documento que ampare la identidad legal del alumno: acta de nacimiento, carta de naturalización, acta de reconocimiento, acta de adopción, Cédula de Identificación Personal o Documento Nacional de Identidad, Pasaporte, Certificado Consular o, en su caso, Documento que demuestre el estado de refugiado
- Copia digitalizada del Título, Diploma o Grado Académico oficiales de Licenciatura que ampare los estudios realizados en el extranjero
- Copia digitalizada del Certificado de Estudios de Licenciatura. En el que aparezcan las asignaturas con las calificaciones de los estudios cursados, que describan las unidades de aprendizaje, periodos en que se cursaron y calificaciones obtenidas

Se requerirá documentación adicional en casos especiales como inscripciones a maestría como opción de titulación o que no cuenten con el perfil académico que el plan de estudios requiera. Tendrás un máximo de 2 meses para cargar todos estos documentos en el campus virtual.

Es del todo necesario que atestigües que todos los documentos que nos facilitas son verdaderos y mantienen su vigencia en el momento en que los envías.

11
Titulación

Este programa te permite alcanzar la titulación de Maestría en Seguridad Informática (Ciberseguridad) obteniendo un título universitario válido por la Secretaría de Educación Pública, y si gustas, la Cédula Profesional de la Dirección General de Profesiones.

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

Este programa te permite alcanzar el grado de **Maestría en Seguridad Informática (Ciberseguridad)**, obteniendo un reconocimiento universitario oficial válido tanto en tu país como de modo internacional.

Los títulos de la Universidad TECH están reconocidos por la Secretaría de Educación Pública (SEP). Este plan de estudios se encuentra incorporado al Sistema Educativo Nacional, con fecha 10 FEBRERO de 2023 y número de acuerdo de Registro de Validez Oficial de Estudios (RVOE): 20230354.

Puedes consultar la validez de este programa en el acuerdo de Registro de Validez Oficial de Estudios: **RVOE Maestría en Seguridad Informática (Ciberseguridad)**

Para más información sobre qué es el RVOE puedes consultar *aquí:*

RVOE

EDUCACIÓN SUPERIOR

Titulación: **Maestría en Seguridad Informática (Ciberseguridad)**

Nº de RVOE: **20230354**

Fecha de RVOE: **10/02/2023**

Modalidad: **100% en línea**

Duración: **20 meses**

Para recibir el presente título no será necesario realizar ningún trámite.
TECH Universidad realizará todas las gestiones oportunas ante las diferentes administraciones públicas en su nombre, para hacerle llegar a su domicilio*:

- Título de la Maestría
- Certificado total de estudios
- Cédula Profesional

Si requiere que cualquiera de estos documentos le lleguen apostillados a su domicilio, póngase en contacto con su asesor académico.
TECH Universidad se hará cargo de todos los trámites.


tech universidad

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

Maestría en Seguridad Informática (Ciberseguridad)

Con Reconocimiento de Validez Oficial de Estudios de la Secretaría de Educación Pública, según Acuerdo Nº. 20230354 en virtud de que demostró cumplir con los estudios correspondientes y aprobó conforme titulación automática el 10 febrero 2023.

A 10 de febrero de 2023

Mtro. Gerardo Daniel Orozco Martínez
Rector

código único TECH: AFWOR23S techtitute.com/titulos

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

tech universidad

Nº de RVOE: 20230354

Maestría

Seguridad Informática (Ciberseguridad)

Idioma: **Español**

Modalidad: **100% en línea**

Duración: **20 meses**

Fecha acuerdo RVOE: **10/02/2023**

Maestría

Seguridad Informática (Ciberseguridad)

Nº de RVOE: 20230354

RVOE
EDUCACIÓN SUPERIOR

tech universidad