Maestría Oficial Universitaria

Gestión de Políticas de Seguridad Informática en la Empresa

Nº de RVOE: 20232122

RVOE
EDUCACIÓN SUPERIOR

tech universidad

tech universidad

Nº de RVOE: 20232122

Maestría Oficial Universitaria
Gestión de Políticas de Seguridad Informática en la Empresa

Idioma: **Español**

Modalidad: **100% online**

Duración: **20 meses**

Fecha de vigencia RVOE: **24/07/2023**

Acceso web: www.techtitute.com/mx/informatica/maestria-universitaria/maestria-universitaria-gestion-politicas-seguridad-informatica-empresa

Índice

01

Presentación del programa

La Gestión de Políticas de Seguridad Informática se ha convertido en un componente crucial para las empresas en un entorno digital cada vez más complejo y vulnerable. Según el informe de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el 60% de las empresas han experimentado al menos un incidente de seguridad, lo que subraya la necesidad de políticas efectivas de protección. En un mundo cada vez más digitalizado, la defensa y los sistemas organizacionales se han convertido en una prioridad estratégica. Por tal razón, TECH ofrece esta capacitación avanzada y de vanguardia, diseñada para preparar a los egresados en el liderazgo de la gestión de la seguridad informática. Todo ello, mediante una modalidad de aprendizaje 100% online.

Este es el momento, te estábamos esperando

Da el siguiente paso hacia tu futuro profesional con este título oficial reconocido internacionalmente. ¡Te convertirás en un experto en la protección digital de las empresas!"

La creciente dependencia de la tecnología, junto con la constante evolución de las amenazas cibernéticas, hace que la protección de la información y los recursos digitales sea una prioridad estratégica para las empresas. De hecho, una de las principales razones por las cuales la Gestión de Políticas de Seguridad Informática es indispensable es la protección contra los ciberataques. Y es que, amenazas como el *ransomware*, el *phishing* y las brechas de datos pueden tener consecuencias devastadoras para las empresas, incluyendo pérdidas económicas, daños a la reputación y sanciones regulatorias.

Esta Maestría Oficial Universitaria en Gestión de Políticas de Seguridad Informática en la Empresa ofrecerá a los informáticos una capacitación avanzada y estratégica, diseñada para enfrentar los desafíos del entorno digital moderno. Así, mediante un enfoque integral, el programa no solo proporcionará los conocimientos necesarios para proteger los activos digitales de las empresas, sino que también abrirá un abanico de oportunidades para el crecimiento profesional y personal.

Asimismo, uno de los principales beneficios de esta titulación será el aprendizaje de políticas de seguridad informática actualizadas y adaptadas a las necesidades del mercado. Además, se adquirirán habilidades en la implementación de medidas de protección, la gestión de incidentes de seguridad, el análisis de vulnerabilidades y la protección de datos sensibles. También se diseñarán estrategias de seguridad personalizadas, utilizando marcos normativos como el GDPR y la ISO 27001, siempre un paso adelante en la gestión de riesgos cibernéticos.

Adicionalmente, la modalidad 100% online ofrecerá la flexibilidad de estudiar autónomamente, sin importar la ubicación geográfica. Este enfoque, combinado con la innovadora metodología *Relearning*, permitirá a los egresados disfrutar de una experiencia de aprendizaje única y efectiva, ideal para aquellos que buscan desarrollar habilidades avanzadas en ciberseguridad sin interrumpir su vida diaria.

Tendrás acceso a una capacitación flexible, interactiva y altamente efectiva, que te permitirá avanzar en tu carrera y estar siempre preparado para enfrentar los retos de la seguridad digital"

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

Esta Maestría Oficial Universitaria preparará a los profesionales en la creación, implementación y supervisión de políticas de seguridad que protejan los activos digitales y fortalezcan la resiliencia organizacional frente a las amenazas cibernéticas. Así, se abordará de manera integral los aspectos técnicos, legales y estratégicos de la seguridad informática, combinando conocimientos avanzados en ciberseguridad con habilidades prácticas de liderazgo. Además, cada asignatura está cuidadosamente estructurado para proporcionar una comprensión profunda sobre temas clave, como análisis de riesgos, normativas internacionales, gestión de incidentes y desarrollo de infraestructuras seguras, asegurando una capacitación completa y orientada a las demandas actuales del mercado.

Un temario completo y bien desarrollado

Con un enfoque en la excelencia académica y la innovación, este programa te preparará para proteger y transformar el panorama digital empresarial. ¡Con todas las garantías de calidad de TECH!"

Asimismo, se distinguirá por ofrecer una experiencia académica innovadora, respaldada por recursos multimedia de última generación y materiales académicos diseñados para maximizar el aprendizaje. A través de la innovadora plataforma online, el alumnado tendrá acceso a un ecosistema de aprendizaje que incluye videos explicativos, casos prácticos y bibliografía especializada. Estos recursos están diseñados para profundizar en temas como la protección de datos, la gestión de incidentes de seguridad y el cumplimiento de normativas internacionales.

Con una metodología basada en el aprendizaje multimedia, podrás optimizar tu tiempo, estudiar a tu propio ritmo y desarrollar una visión integral sobre la seguridad informática en las empresas"

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	Sistema de gestión de seguridad de información
Asignatura 2	Aspectos organizativos en Políticas de Seguridad de la Información
Asignatura 3	Políticas de Seguridad para el análisis de amenazas en sistemas informáticos
Asignatura 4	Implementación de Políticas de Seguridad en software y hardware
Asignatura 5	Políticas de gestión de incidencias de seguridad
Asignatura 6	Implementación de Políticas de Seguridad física y ambiental en la empresa
Asignatura 7	Políticas de comunicaciones seguras en la empresa
Asignatura 8	Implementación de Políticas de Seguridad ante ataques
Asignatura 9	Herramientas de monitorización en Políticas de Seguridad de los sistemas de información
Asignatura 10	Políticas de recuperación de desastres de seguridad

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

Asignatura 1. Sistema de gestión de seguridad de información

1.1. Seguridad de la información. Aspectos Clave
- 1.1.1. Seguridad de la información
- 1.1.2. Confidencialidad
- 1.1.3. Integridad
- 1.1.4. Disponibilidad
- 1.1.5. Medidas de seguridad de la información

1.2. Sistema de gestión de la seguridad de la información
- 1.2.1. Modelos de Gestión de Seguridad de la Información
- 1.2.2. Documentos para implantar un Sistema de Gestión de Seguridad de la Información (SGSI)
- 1.2.3. Niveles y controles de un Sistema de Gestión de Seguridad de la Información (SGSI)

1.3. Normas y estándares internacionales
- 1.3.1. Estándares internacionales en la seguridad de la información
- 1.3.2. Origen y evolución del estándar
- 1.3.3. Estándares internacionales gestión de la seguridad de la información
- 1.3.4. Otras normas de referencia

1.4. Normas ISO/IEC 27000
- 1.4.1. Objeto y ámbito de aplicación
- 1.4.2. Estructura de la norma
- 1.4.3. Certificación
- 1.4.4. Fases de acreditación
- 1.4.5. Beneficios de las Normas ISO/IEC 27000

1.5. Diseño e implantación de un Sistema General de Seguridad de Información
- 1.5.1. Diseño e implantación de un Sistema General de Seguridad de Información
- 1.5.2. Fases de Implantación de un Sistema General de Seguridad de Información
- 1.5.3. Plan de Continuidad de Negocio

1.6. Fase I: diagnóstico
- 1.6.1. Diagnóstico preliminar
- 1.6.2. Identificación del nivel de estratificación
- 1.6.3. Nivel de cumplimiento de estándares/normas

1.7. Fase II: preparación
- 1.7.1. Contexto de la organización
- 1.7.2. Análisis de normativas de seguridad aplicables
- 1.7.3. Alcance del Sistema General de Seguridad de Información
- 1.7.4. Política del Sistema General de Seguridad de Información
- 1.7.5. Objetivos del Sistema General de Seguridad de Información

1.8. Fase III: planificación
- 1.8.1. Clasificación de activos
- 1.8.2. Valoración de riesgos
- 1.8.3. Identificación de amenazas y riesgos

1.9. Fase IV: implantación y seguimiento
- 1.9.1. Análisis de resultados
- 1.9.2. Asignación de responsabilidades
- 1.9.3. Temporalización del Plan de Acción
- 1.9.4. Seguimiento y auditorias

1.10. Políticas de Seguridad en la gestión de incidentes
- 1.10.1. Fases
- 1.10.2. Categorización de incidentes
- 1.10.3. Procedimientos y gestión de incidentes

Asignatura 2. Aspectos organizativos en Políticas de Seguridad de la Información

2.1. Organización interna
- 2.1.1. Asignación de responsabilidades
- 2.1.2. Segregación de tareas
- 2.1.3. Contactos con autoridades
- 2.1.4. Seguridad de la información en gestión de proyectos

2.2. Gestión de activos
- 2.2.1. Responsabilidad sobre los activos
- 2.2.2. Clasificación de la información
- 2.2.3. Manejo de los soportes de almacenamiento

2.3. Políticas de seguridad en los procesos de negocio
- 2.3.1. Análisis de los procesos de negocio vulnerables
- 2.3.2. Análisis de impacto de negocio
- 2.3.3. Clasificación procesos respecto al impacto de negocio

2.4. Políticas de seguridad ligada a los Recursos Humanos
- 2.4.1. Antes de contratación
- 2.4.2. Durante la contratación
- 2.4.3. Cese o cambio de puesto de trabajo

2.5. Políticas de Seguridad en Dirección
- 2.5.1. Directrices de la Dirección en seguridad de la información
- 2.5.2. Analizando del impacto en el negocio
- 2.5.3. Plan de recuperación como política de seguridad

2.6. Adquisición y mantenimientos de los sistemas de información
- 2.6.1. Requisitos de seguridad de los sistemas de información
- 2.6.2. Seguridad en los datos de desarrollo y soporte
- 2.6.3. Datos de prueba

2.7. Seguridad con Suministradores
- 2.7.1. Seguridad informática con suministradores
- 2.7.2. Gestión de la prestación del servicio con garantía
- 2.7.3. Seguridad en la cadena de suministro

2.8. Seguridad operativa
- 2.8.1. Responsabilidades en la operación
- 2.8.2. Protección contra código malicioso
- 2.8.3. Copias de seguridad
- 2.8.4. Registros de actividad y supervisión

2.9. Gestión de la seguridad y normativas
- 2.9.1. Gestión de la seguridad y normativas
- 2.9.2. Cumplimiento de los requisitos legales
- 2.9.3. Revisiones en la seguridad de la información

2.10. Seguridad en la gestión para la continuidad de negocio
- 2.10.1. Seguridad en la gestión para la continuidad de negocio
- 2.10.2. Continuidad de la seguridad de la información
- 2.10.3. Redundancias

Asignatura 3. Políticas de Seguridad para el análisis de amenazas en sistemas informáticos

3.1. La gestión de amenazas en las Políticas de Seguridad
- 3.1.1. La gestión del riesgo
- 3.1.2. El riesgo en seguridad
- 3.1.3. Metodologías en la gestión de amenazas
- 3.1.4. Puesta en marcha de metodologías

3.2. Fases de la gestión de amenazas
- 3.2.1. Identificación
- 3.2.2. Análisis
- 3.2.3. Localización
- 3.2.4. Medidas de salvaguarda

3.3. Sistemas de auditoria para localización de amenazas
- 3.3.1. Sistemas de auditoría para la localización de amenazas
- 3.3.2. Clasificación y flujo de información
- 3.3.3. Análisis de los procesos vulnerables

3.4. Clasificación del riesgo
  3.4.1. Tipos de riesgo
  3.4.2. Cálculo de la probabilidad de amenaza
  3.4.3. Riesgo residual
3.5. Tratamiento del riesgo
  3.5.1. Tratamiento del riesgo
  3.5.2. Implementación de medidas de salvaguarda
  3.5.3. Transferir o asumir
3.6. Control de riesgo
  3.6.1. Proceso continuo de gestión de riesgo
  3.6.2. Implementación de métricas de seguridad
  3.6.3. Modelo estratégico de métricas en seguridad de la información
3.7. Metodologías prácticas para el análisis y control de amenazas
  3.7.1. Catálogo de amenazas
  3.7.2. Catálogo de medidas de control
  3.7.3. Catálogo de salvaguardas
3.8. Norma ISO 27005
  3.8.1. Identificación del riesgo
  3.8.2. Análisis del riesgo
  3.8.3. Evaluación del riesgo
3.9. Matriz de riesgo, impacto y amenazas
  3.9.1. Datos, sistemas y personal
  3.9.2. Probabilidad de amenaza
  3.9.3. Magnitud del daño
3.10. Diseño de fases y procesos en el análisis de amenazas
  3.10.1. Identificación elementos críticos de la organización
  3.10.2. Determinación de amenazas e impactos
  3.10.3. Análisis del impacto y riesgo
  3.10.4. Metodologías

Asignatura 4. Implementación de Políticas de Seguridad en software y hardware

4.1. Implementación práctica de Políticas de Seguridad en software y hardware
  4.1.1. Implementación de identificación y autorización
  4.1.2. Implementación de técnicas de identificación
  4.1.3. Medidas técnicas de autorización
4.2. Tecnologías de identificación y autorización
  4.2.1. Identificador y contraseña de un único uso
  4.2.2. Token o tarjeta inteligente
  4.2.3. La llave “Confidencial Defensa”
  4.2.4. Tecnología RFID (identificación por radiofrecuencia) Activo
4.3. Políticas de seguridad en el acceso a software y sistemas
  4.3.1. Implementación de políticas de control de accesos
  4.3.2. Implementación de políticas de acceso a comunicaciones
  4.3.3. Tipos de herramientas de seguridad para control de acceso
4.4. Gestión de acceso a usuarios
  4.4.1. Gestión de los derechos de acceso
  4.4.2. Segregación de roles y funciones de acceso
  4.4.3. Implementación derechos de acceso en sistemas
4.5. Control de acceso a sistemas y aplicaciones
  4.5.1. Norma del mínimo acceso
  4.5.2. Tecnologías seguras de inicios de sesión
  4.5.3. Políticas de seguridad en contraseñas
4.6. Tecnologías de sistemas de identificación
  4.6.1. Directorio activo
  4.6.2. Contraseña dinámica
  4.6.3. Protocolo de autenticación por desafío mutuo
  4.6.4. Protocolo de autentificación de contraseña
  4.6.5. Protocolos de autentificación KERBEROS, DIAMETER, NTLM

4.7. Controles críticos de seguridad informática para bastionado de sistemas
- 4.7.1. Controles básicos
- 4.7.2. Controles fundamentales
- 4.7.3. Controles organizacionales

4.8. Seguridad en la operativa
- 4.8.1. Protección contra código malicioso
- 4.8.2. Copias de seguridad
- 4.8.3. Registro de actividad y supervisión

4.9. Gestión de las vulnerabilidades técnicas
- 4.9.1. Vulnerabilidades técnicas
- 4.9.2. Gestión de vulnerabilidades técnicas
- 4.9.3. Restricciones en la instalación de software

4.10. Implementación de prácticas de Políticas de Seguridad
- 4.10.1. Implementación de prácticas de Políticas de Seguridad
- 4.10.2. Vulnerabilidades lógicas
- 4.10.3. Implementación de políticas de defensa

Asignatura 5. Políticas de gestión de incidencias de seguridad

5.1. Políticas de gestión de incidencias de seguridad de la información y mejoras
- 5.1.1. Gestión de incidencias
- 5.1.2. Responsabilidades y procedimientos
- 5.1.3. Notificación de eventos

5.2. Sistemas de detección y prevención de intrusiones (IDS/IPS)
- 5.2.1. Datos de funcionamiento del sistema
- 5.2.2. Tipos de sistemas de detección de intrusos
- 5.2.3. Criterios para la ubicación de los IDS/IPS

5.3. Respuesta ante incidentes de seguridad
- 5.3.1. Procedimiento de recolección de información
- 5.3.2. Proceso de verificación de intrusión
- 5.3.3. Equipo de respuesta ante emergencias informáticas

5.4. Proceso de notificación y gestión de intentos de intrusión
- 5.4.1. Responsabilidades en el proceso de notificación
- 5.4.2. Clasificación de los incidentes
- 5.4.3. Proceso de resolución y recuperación

5.5. Análisis forense como política de seguridad
- 5.5.1. Evidencias volátiles y no volátiles
- 5.5.2. Análisis y recogida de evidencias electrónicas
- 5.5.3. Importancia de las evidencias electrónicas

5.6. Herramientas de sistemas de detección y prevención de intrusiones (IDS/IPS)
- 5.6.1. Sistema de detección de intrusos Snort
- 5.6.2. Motor de detección de amenazas de red Suricata
- 5.6.3. Software SolarWinds

5.7. Herramientas centralizadoras de eventos
- 5.7.1. Administración de la seguridad de la información
- 5.7.2. Administración de la seguridad de los eventos
- 5.7.3. Administración de la seguridad de eventos e información

5.8. NIST SP800-61
- 5.8.1. Capacidad de respuesta ante incidentes de seguridad informática
- 5.8.2. Manejo de un incidente
- 5.8.3. Coordinación e información compartida

5.9. Norma ISO 27035
- 5.9.1. Norma ISO 27035. Principios de la gestión de incidentes
- 5.9.2. Guías para la elaboración de un plan para la gestión de incidentes
- 5.9.3. Guías de operaciones en la respuesta a incidentes

Asignatura 6. Implementación de Políticas de Seguridad física y ambiental en la empresa

6.1. Áreas seguras
- 6.1.1. Perímetro de seguridad física
- 6.1.2. Trabajo en áreas seguras
- 6.1.3. Seguridad de oficinas, despachos y recursos

6.2. Controles físicos de entrada
- 6.2.1. Controles físicos de entrada
- 6.2.2. Políticas de control de acceso físico
- 6.2.3. Sistemas de control físico de entrada

6.3. Vulnerabilidades de accesos físicos
- 6.3.1. Vulnerabilidades de accesos físicos
- 6.3.2. Principales vulnerabilidades físicas
- 6.3.3. Implementación de medidas de salvaguardas

6.4. Sistemas biométricos fisiológicos
- 6.4.1. Huella dactilar
- 6.4.2. Reconocimiento facial
- 6.4.3. Reconocimiento de iris y retina
- 6.4.4. Otros sistemas biométricos fisiológicos

6.5. Sistemas biométricos de comportamiento
- 6.5.1. Reconocimiento de firma
- 6.5.2. Reconocimiento de escritor
- 6.5.3. Reconocimiento de voz
- 6.5.4. Otros sistemas biométricos de comportamientos

6.6. Gestión de riesgos en biometría
- 6.6.1. Gestión de riesgos en biometría
- 6.6.2. Implementación de sistemas biométricos
- 6.6.3. Vulnerabilidades de los sistemas biométricos

6.7. Implementación de políticas en dispositivos anfitriones
- 6.7.1. Instalación de suministro y seguridad de cableado
- 6.7.2. Emplazamiento de los equipos
- 6.7.3. Salida de los equipos fuera de las dependencias
- 6.7.4. Equipo informático desatendido y política de puesto despejado

6.8. Protección ambiental
- 6.8.1. Sistemas de protección ante incendios
- 6.8.2. Sistemas de protección ante seísmos
- 6.8.3. Sistemas de protección antiterremotos

6.9. Seguridad en centro de procesamiento de datos
- 6.9.1. Puertas de seguridad
- 6.9.2. Sistemas de videovigilancia (CCTV)
- 6.9.3. Control de Seguridad

6.10. Normativa Internacional de la Seguridad Física
- 6.10.1. IEC 62443-2-1 (europea)
- 6.10.2. NERC CIP-005-5 (EE.UU.)
- 6.10.3. NERC CIP-014-2 (EE.UU.)

Asignatura 7. Políticas de comunicaciones seguras en la empresa

7.1. Políticas de Comunicaciones Seguras en la Empresa
- 7.1.1. Gestión de la Seguridad en las Redes
- 7.1.2. Control y monitorización de red
- 7.1.3. Segregación de redes
- 7.1.4. Sistemas de seguridad en redes

7.2. Protocolos Seguros de Comunicación
- 7.2.1. Modelo de protocolos de red TCP/IP
- 7.2.2. Conjunto de Protocolos IPsec (seguridad del protocolo de Internet)
- 7.2.3. Protocolo de Seguridad de la Capa de Transporte (TLS)

7.3. Protocolo TLS 1.3.
- 7.3.1. Fases de un proceso TLS 1.3.
- 7.3.2. Protocolo *Handsake*
- 7.3.3. Protocolo de registro
- 7.3.4. Diferencias con TLS 1.2.

7.4. Algoritmos criptográficos
- 7.4.1. Algoritmos criptográficos usados en comunicaciones
- 7.4.2. Algoritmo de protección de red Cipher-suites
- 7.4.3. Algoritmos Criptográficos permitidos para TLS 1.3.

7.5. Funciones *Digest* de resumen de archivo
- 7.5.1. Importancia
- 7.5.2. Herramienta de seguridad MD6
- 7.5.3. Algoritmo de Hash Seguro

7.6. Infraestructura de Clave Pública o PKI
- 7.6.1. PKI y sus entidades
- 7.6.2. Certificado digital
- 7.6.3. Tipos de certificados digital

7.7. Comunicaciones de túnel y transporte
- 7.7.1. Comunicaciones túnel
- 7.7.2. Comunicaciones transporte
- 7.7.3. Implementación túnel cifrado

7.8. Protocolo y programa *Secure Shell* o *SSH*
- 7.8.1. Cápsula Segura
- 7.8.2. Funcionamiento de *SSH*
- 7.8.3. Herramientas *SSH*

7.9. Auditoria de sistemas criptográficos
- 7.9.1. Auditoría de sistemas criptográficos
- 7.9.2. Pruebas de integridad
- 7.9.3. Testeo Sistema criptográfico

7.10. Sistemas criptográficos
- 7.10.1. Sistemas Criptográficos
- 7.10.2. Vulnerabilidades sistemas criptográficos
- 7.10.3. Salvaguardas en criptografía

Asignatura 8. Implementación de Políticas de Seguridad ante ataques

8.1. Detección de vulnerabilidades de seguridad
- 8.1.1. Características e importancia
- 8.1.2. Riesgos y vulnerabilidades
- 8.1.3. Contramedidas

8.2. Sistemas operativos en servicios
- 8.2.1. Importancia en los servicios
- 8.2.2. Riesgos y vulnerabilidades
- 8.2.3. Contramedidas

8.3. Pérdida de sesión
- 8.3.1. Características
- 8.3.2. El proceso
- 8.3.3. Contramedidas

8.4. Evasión de sistemas de detección de intruso, sistemas de protección "*Firewalls* y *Honeypots*"
- 8.4.1. Evasión de los sistemas de protección
- 8.4.2. Técnicas de evasión
- 8.4.3. Implementación de contramedidas

8.5. Intrusión en servidores web
- 8.5.1. Características
- 8.5.2. Ataques a servidores webs
- 8.5.3. Implementación de medidas de defensa

8.6. Intrusión en aplicaciones
- 8.6.1. Características
- 8.6.2. Ataques a aplicaciones web
- 8.6.3. Implementación de medidas de defensa

8.7. Intrusión en internet inalámbrico
- 8.7.1. Ataque a red inalámbrica
- 8.7.2. Vulnerabilidades Redes Wifi
- 8.7.3. Implementación de Medidas de defensa

8.8. Intrusión en plataformas móviles
- 8.8.1. Ataque a plataformas móviles
- 8.8.2. Vulnerabilidades a plataformas móviles
- 8.8.3. Implementación de contramedidas

8.9. Intrusión mediante bloqueadores o *Ramsonware*
- 8.9.1. Características de los *Rams Ramsonware onware*
- 8.9.2. Vulnerabilidades causantes del *Ramsonware*
- 8.9.3. Implementación de contramedidas

8.10. Ingeniería Social
- 8.10.1. Ingeniería Social
- 8.10.2. Tipos de Ingeniería Social
- 8.10.3. Contramedidas para la Ingeniería Social

Asignatura 9. Herramientas de monitorización en Políticas de Seguridad de los sistemas de información

9.1. Políticas de monitorización de sistemas de la información
- 9.1.1. Monitorización de sistemas
- 9.1.2. Métricas
- 9.1.3. Tipos de métricas

9.2. Auditoria y registro en sistemas
- 9.2.1. Auditoría y registro en sistemas
- 9.2.2. Auditoria y registro en Windows
- 9.2.3. Auditoria y registro en Linux

9.3. Protocolo Simple de Administración de Red
- 9.3.1. Características
- 9.3.2. Funcionamiento
- 9.3.3. Herramientas

9.4. Monitorización de redes
- 9.4.1. Monitorización de redes
- 9.4.2. La monitorización de red en sistemas de control
- 9.4.3. Herramientas de monitorización para sistemas de control

9.5. Sistema de monitorización de Redes Nagios
- 9.5.1. Características de Nagios
- 9.5.2. Funcionamiento de Nagios
- 9.5.3. Instalación de Nagios

9.6. Sistema de monitorización de Redes Zabbix
- 9.6.1. Características de Zabbix
- 9.6.2. Funcionamiento de Zabbix
- 9.6.3. Instalación de Zabbix

9.7. Sistema de Monitorización de Redes Cacti
- 9.7.1. Características de Cacti
- 9.7.2. Funcionamiento de Cacti
- 9.7.3. Instalación de Cacti

9.8. Sistema de monitorización de Redes Pandora
- 9.8.1. Características de Pandora
- 9.8.2. Funcionamiento de Pandora
- 9.8.3. Instalación de Pandora

9.9. Sistema de monitorización de Redes SolarWinds
- 9.9.1. Características de SolarWinds
- 9.9.2. Funcionamiento de SolarWinds
- 9.9.3. Instalación de SolarWinds

9.10. Normativa sobre monitorización
- 9.10.1. Normativa sobre monitorización
- 9.10.2. Controles sobre auditoria y registro
- 9.10.3. NIST 800-123

Asignatura 10. Políticas de recuperación de desastres de seguridad

10.1. Plan de Recuperación de Desastres o DRP
- 10.1.1. Objetivo de un DRP
- 10.1.2. Beneficios de un DRP
- 10.1.3. Consecuencias de su ausencia o no actualizado

10.2. Guía para definir un Plan de Recuperación de Desastres
- 10.2.1. Alcance y objetivos
- 10.2.2. Diseño de la estrategia de recuperación
- 10.2.3. Asignación de roles y responsabilidades
- 10.2.4. Realización de un Inventario de hardware, software y servicios
- 10.2.5. Tolerancia para tiempo de inactividad y pérdida de datos
- 10.2.6. Establecimiento de los tipos específicos de DRP que se requieren
- 10.2.7. Realización de un Plan de formación, concienciación y comunicación

10.3. Alcance y objetivos de un Plan de Recuperación de Desastres
- 10.3.1. Garantía de respuesta
- 10.3.2. Componentes tecnológicos
- 10.3.3. Alcance de la política de continuidad

10.4. Diseño de la Estrategia de un Plan de Recuperación de Desastre
- 10.4.1. Estrategia de Recuperación de Desastre
- 10.4.2. Presupuesto
- 10.4.3. Recursos Humanos y Físicos
- 10.4.4. Posiciones gerenciales en riesgo
- 10.4.5. Tecnología
- 10.4.6. Datos

10.5. Continuidad de los procesos de la información
- 10.5.1. Planificación de la continuidad
- 10.5.2. Implantación de la continuidad
- 10.5.3. Verificación evaluación de la continuidad

10.6. Alcance de un Plan de Continuidad Empresarial
- 10.6.1. Determinación de los procesos de mayor criticidad
- 10.6.2. Enfoque por activo
- 10.6.3. Enfoque por proceso

10.7. Implementación de los procesos garantizados de negocio
- 10.7.1. Actividades prioritarias
- 10.7.2. Tiempos de recuperación ideales
- 10.7.3. Estrategias de supervivencia

10.8. Análisis de la organización
- 10.8.1. Obtención de información
- 10.8.2. Análisis de Impacto sobre negocio (BIA)
- 10.8.3. Análisis de riesgos en la organización

10.9. Respuesta a la contingencia
- 10.9.1. Plan de Crisis
- 10.9.2. Planes Operativos de Recuperación de Entornos
- 10.9.3. Procedimientos técnicos de trabajo o de incidentes

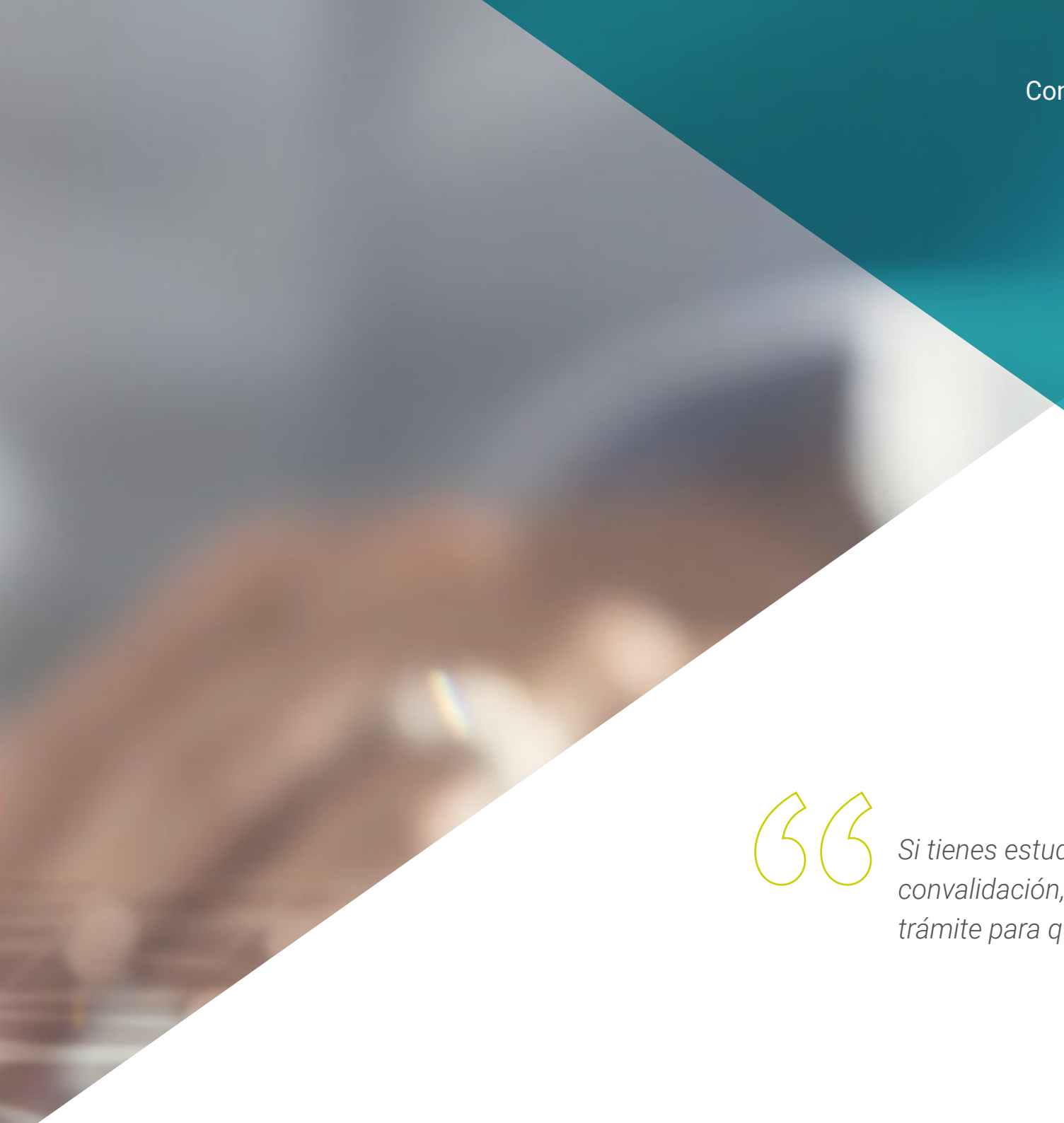
10.10. Norma Internacional ISO 27031
- 10.10.1. Objetivos
- 10.10.2. Términos y definiciones
- 10.10.3. Operación

Conocerás las últimas tendencias en Seguridad Informática de la mano de auténticos expertos en este campo. ¡Matricúlate ahora y avanza en tu profesión de la mano de la mejor universidad digital del mundo!"

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

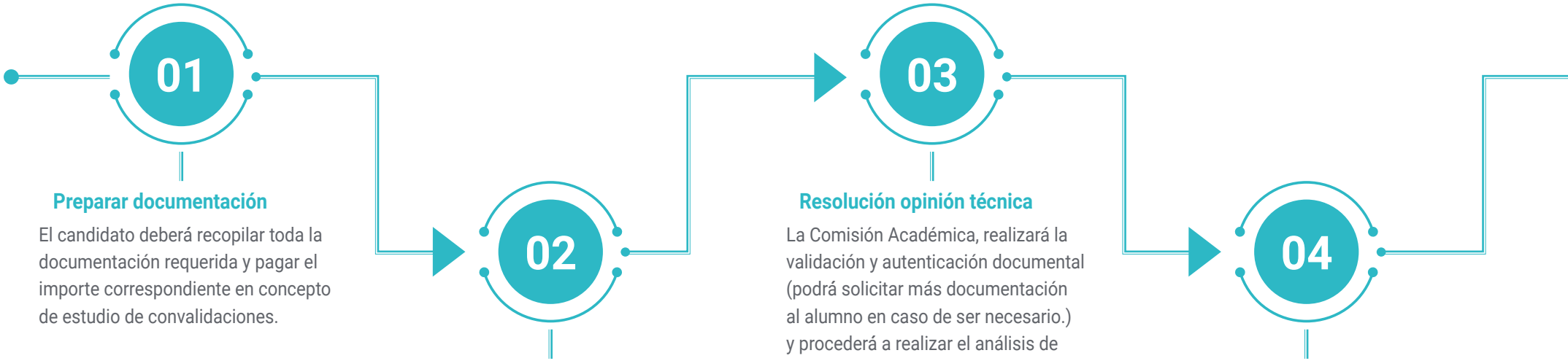
¿En qué plazo se resolverá la solicitud?

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.

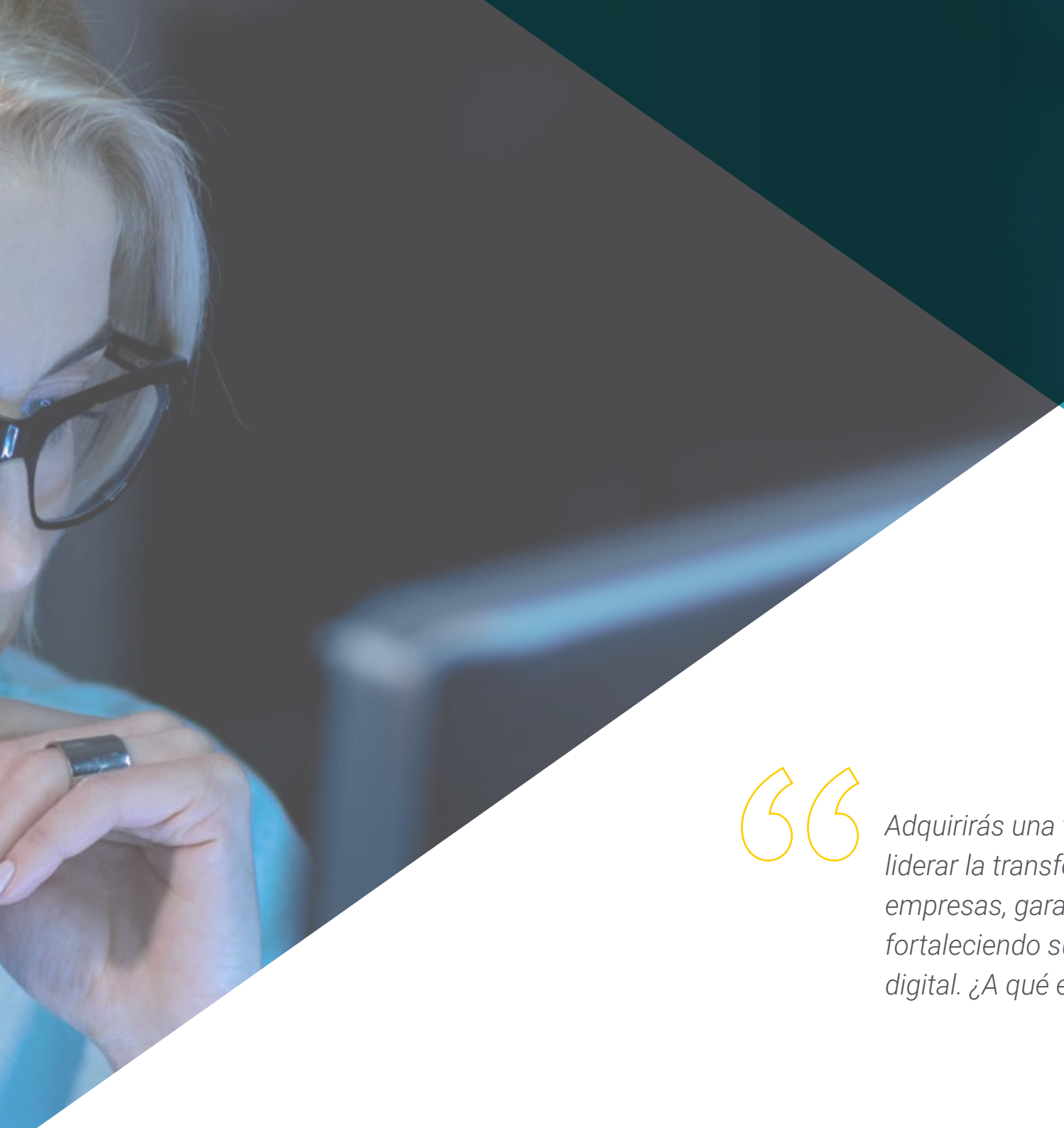
Convalida tus estudios realizados y no tendrás que evaluarte de las asignaturas superadas.

05

Objetivos docentes

Este programa universitario tendrá como meta preparar a profesionales altamente capacitados en el desarrollo, implementación y supervisión de políticas de seguridad informática, para enfrentar los desafíos más exigentes en un entorno digital en constante evolución. Así, mediante un enfoque multidisciplinario, los informáticos adquirirán las competencias necesarias para destacar en su carrera profesional. Además, entre los principales objetivos se encontrará la capacitación en el análisis de riesgos informáticos y en la aplicación de estrategias de protección que salvaguarden los datos sensibles de una organización.

Living success



Adquirirás una visión estratégica para liderar la transformación digital de las empresas, garantizando su seguridad y fortaleciendo su crecimiento en la era digital. ¿A qué esperas para matricularte?"

Objetivos generales

- Profundizar en los conceptos clave de la seguridad de la información
- Analizar las normativas y estándares aplicables en la actualidad a los SGSI
- Implementar un SGSI en la empresa
- Determinar qué departamentos debe abarcar la implementación del sistema de gestión de seguridad
- Desarrollar las medidas necesarias para garantizar buenas prácticas en materia de seguridad de la información
- Establecer qué es la autenticación e identificación
- Dominar los distintos métodos de autenticación que existen y su implementación práctica
- Implementar la política de control de accesos correcta al software y sistemas
- Adquirir conocimiento especializado sobre cómo gestionar incidencias causadas por eventos de seguridad informática
- Implementar el término de área segura y perímetro seguro
- Analizar los distintos algoritmos de cifrado utilizados en redes de comunicaciones
- Gestionar los distintos ataques reales a nuestro sistema de información

Objetivos específicos

Asignatura 1. Sistema de gestión de seguridad de información

- Ponerse al día de los procedimientos de gestión de incidentes de seguridad y determinando sus implicaciones en la organización interna de la entidad
- Ser capaz de explicar las fases que permiten el desarrollo y la implantación de un Sistema de Gestión de Seguridad de la Información

Asignatura 2. Aspectos organizativos en Políticas de Seguridad de la Información

- Profundizar en las medidas necesarias para garantizar buenas prácticas en materia de seguridad de la información y qué medidas deben ser observadas con suministradores y mantenimientos de sistemas de información
- Estudiar las contramedidas de seguridad necesaria en la operativa, considerando el papel del departamento de recursos humanos en materia de seguridad informática

Asignatura 3. Políticas de Seguridad para el análisis de amenazas en sistemas informáticos

- Ampliar el concepto de amenazas informáticas, así como las fases de una gestión preventiva de las mismas
- Ahondar en la comprensión de las diferentes metodologías que permiten un análisis exhaustivo, diferenciando las metodologías de auditoría con el fin de ser capaz de clasificar las amenazas por impacto y gravedad

Asignatura 4. Implementación de Políticas de Seguridad en software y hardware

- Comprender los conceptos de autenticación e identificación a través del estudio de los distintos métodos y tecnologías que existen actualmente y su operatividad en la empresa
- Ahondar en los sistemas de Directorio Activo y los distintos sistemas de autenticación con el propósito de ser capaz de definir políticas efectivas de control de accesos a redes y servicios y de control de código malicioso para la seguridad en hardware y software

Asignatura 5. Políticas de gestión de incidencias de seguridad

- Dominar el funcionamiento de un equipo de tratamiento de incidencias en materia de seguridad informática a través del estudio de las distintas herramientas utilizadas en el tratamiento y prevención de incidencias y explicando las distintas fases de una gestión de eventos en el área
- Gestionar la normativa ISO 27035, valorando la necesidad de un análisis informático para el estudio en profundidad de las incidencias registradas y asimilando los protocolos estandarizados para el tratamiento de incidencias de seguridad

Asignatura 6. Implementación de Políticas de Seguridad física y ambiental en la empresa

- Analizar los conceptos de área y perímetro seguro a través del estudio de los elementos que componen la biometría y los sistemas biométricos que hacen posible el control de acceso físico
- Actualizar la normativa vigente sobre el tema con el propósito de definir políticas de seguridad física correctas y los sistemas de control de acceso físico en Centros de Procesamiento de Datos

Asignatura 7. Políticas de comunicaciones seguras en la empresa

- Explicar los elementos que componen una red de comunicaciones mediante la división de la misma, a través del estudio de los distintos algoritmos de cifrado utilizados en redes de comunicaciones, así como las diversas técnicas de cifrado en la red
- Actualizar el concepto de Criptografía y sus tipos con el propósito de contar con los conocimientos requeridos que permitan implementar una red segura y establecer el funcionamiento de una Infraestructura de Clave Única

Asignatura 8. Implementación de Políticas de Seguridad ante ataques

- Reflexionar sobre las vulnerabilidades de las plataformas móviles y del internet de las cosas y las estrategias para evitarlas a través de estudio de los distintos ataques a los sistemas de información
- Definir medidas técnicas para mitigar las principales amenazas y conocer contramedidas para evitarlas en los servidores web y en las aplicaciones web

Asignatura 9. Herramientas de monitorización en Políticas de Seguridad de los sistemas de información

- Explicar los conceptos de monitorización e implementación de métricas mediante la configuración de los registros de auditoría en los sistemas de monitorización de las redes
- Ahondar en el manejo de las herramientas más actuales existentes en el mercado con el propósito de adquirir los conocimientos que permitan la instalación y seguimiento del Protocolo Simple de Administración de Red

Asignatura 10. Políticas de recuperación de desastres de seguridad

- Analizar el concepto de continuidad de la seguridad de la información mediante el estudio de las características de un plan de continuidad de negocio y de recuperación de desastres
- Considerar los distintos tipos de proyectos de continuidad con el propósito de asimilar los conocimientos que permitan un análisis de impacto de negocio para averiguar cuáles son los activos más vulnerables y con mayor impacto en su pérdida

¿Quieres ser capaz de detectar si una compañía es vulnerable ante ataques informáticos? En TECH, obtendrás todo el conocimiento y las destrezas que necesitas para lograrlo"

06
Salidas profesionales

Esta titulación académica abrirá un amplio abanico de oportunidades en el ámbito de la ciberseguridad. Así, los profesionales estarán altamente cualificados para desempeñar roles clave como *Chief Information Security Officer* (CISO), Consultor en Ciberseguridad, Analista de Riesgos o Auditor de Seguridad Informática en empresas de todos los sectores. Además, podrán diseñar e implementar estrategias de protección, establecer protocolos ante incidentes de seguridad y garantizar el cumplimiento de las normativas internacionales. Todo ello los convertirá en piezas clave en la gestión de la transformación digital de las organizaciones.

Tu perfil será altamente demandado y contarás con grandes perspectivas de crecimiento y estabilidad laboral en un sector en auge"

Perfil del egresado

El egresado será un profesional altamente capacitado y preparado para enfrentar los desafíos más complejos en el ámbito de la ciberseguridad. De hecho, su perfil se caracterizará por un dominio integral de las estrategias de protección de datos, la gestión de riesgos informáticos y la implementación de políticas de seguridad en entornos empresariales. También destacará por su capacidad para identificar, evaluar y mitigar vulnerabilidades dentro de las infraestructuras digitales de una organización, así como por su habilidad para diseñar y ejecutar planes de seguridad efectivos alineados con las mejores prácticas y normativas internacionales.

Con una visión estratégica y un enfoque práctico, podrás liderar la seguridad informática en empresas de cualquier sector.

- **Pensamiento crítico y resolución de problemas:** Identificar vulnerabilidades y proponer soluciones efectivas ante situaciones complejas de seguridad informática
- **Comunicación efectiva:** Comunicar de manera clara y persuasiva, tanto a equipos técnicos como a directivos, facilitando la toma de decisiones
- **Trabajo en equipo y liderazgo:** Liderar equipos multidisciplinarios y gestionar proyectos de seguridad de forma eficiente
- **Adaptabilidad y aprendizaje continuo:** Gestionar los cambios tecnológicos y aprender de manera autónoma en el campo de la ciberseguridad

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

1. **Director de Seguridad Informática:** Responsable de diseñar y ejecutar estrategias de ciberseguridad para proteger los sistemas informáticos y la información sensible de la empresa
   Responsabilidades: Diseña políticas de seguridad informática y lidera la implementación de estrategias para proteger los activos digitales de la empresa
2. **Consultor en Ciberseguridad:** Brinda asesoría a empresas sobre cómo implementar políticas de seguridad, gestionando riesgos y garantizando el cumplimiento de normativas
   Responsabilidades: Asesora a las empresas sobre la integración de políticas de seguridad, gestionando riesgos y cumpliendo con las regulaciones del sector
3. **Jefe de Protección de Datos:** Supervisa el manejo y protección de datos dentro de la organización, asegurando el cumplimiento de leyes como el GDPR y otras normativas de privacidad
   Responsabilidades: Supervisa la protección de datos sensibles y asegura el cumplimiento de las normativas de privacidad y protección de información
4. **Gerente de Riesgos Tecnológicos:** Identifica y evalúa amenazas tecnológicas, implementando políticas y medidas para mitigar riesgos informáticos y proteger los activos digitales
   Responsabilidades: Evalúa amenazas tecnológicas y desarrolla planes para mitigar los riesgos, protegiendo la infraestructura y los datos de la empresa
5. **Analista de Seguridad en Redes:** Se encarga de monitorizar y defender las redes corporativas contra amenazas externas, asegurando la integridad y la disponibilidad de los sistemas
   Responsabilidades: Monitorea redes y sistemas, detectando y neutralizando amenazas externas para garantizar la disponibilidad y seguridad de la infraestructura
6. **Responsable de Cumplimiento en Ciberseguridad:** Asegura que la empresa cumpla con todas las normativas de seguridad informática, realizando auditorías y gestionando procesos de certificación
   Responsabilidades: Realiza auditorías, verifica el cumplimiento de normativas de seguridad y gestiona procesos de certificación de ciberseguridad
7. **Administrador de Sistemas de Seguridad:** Gestiona y configura los sistemas de protección de la red y los dispositivos de la empresa, garantizando su funcionamiento adecuado y seguro
   Responsabilidades: Configura y mantiene los sistemas de protección de redes y dispositivos, asegurando su correcta operación y respuesta ante incidentes
8. **Coordinador de Respuesta a Incidentes:** Lidera el equipo de respuesta ante incidentes de ciberseguridad, gestionando la detección, análisis y resolución de brechas de seguridad
   Responsabilidades: Gestiona la respuesta ante incidentes de seguridad, coordinando la detección, análisis y resolución de ataques o brechas

Salidas académicas y de investigación

Además de todos los puestos laborales para los que serás apto mediante el estudio de esta Maestría Oficial Universitaria 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, podrá aprender idiomas de un modo sencillo y práctico.

Acredita tu competencia lingüística

TECH te incluye el estudio de idiomas en la Maestría 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.

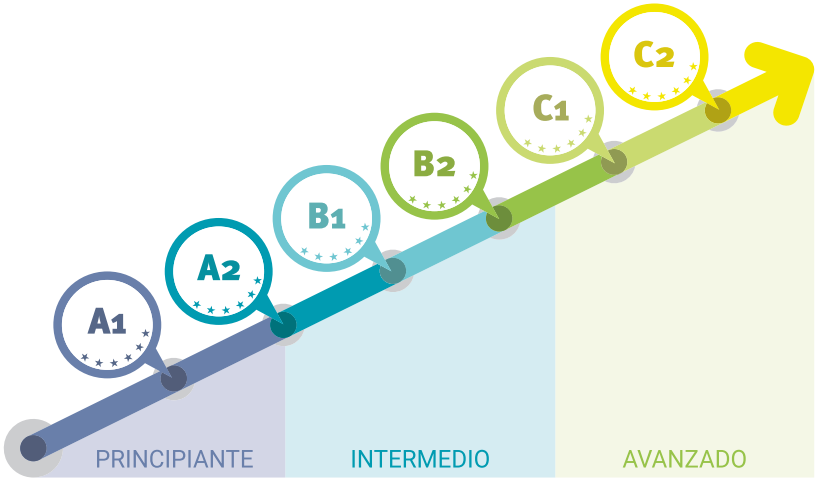
El estudiante aprenderá, mediante actividades en contextos reales, la resolución de situaciones cotidianas de comunicación en entornos simulados de aprendizaje y se enfrentará a simulacros de examen para la preparación de la prueba de certificación de nivel.

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.

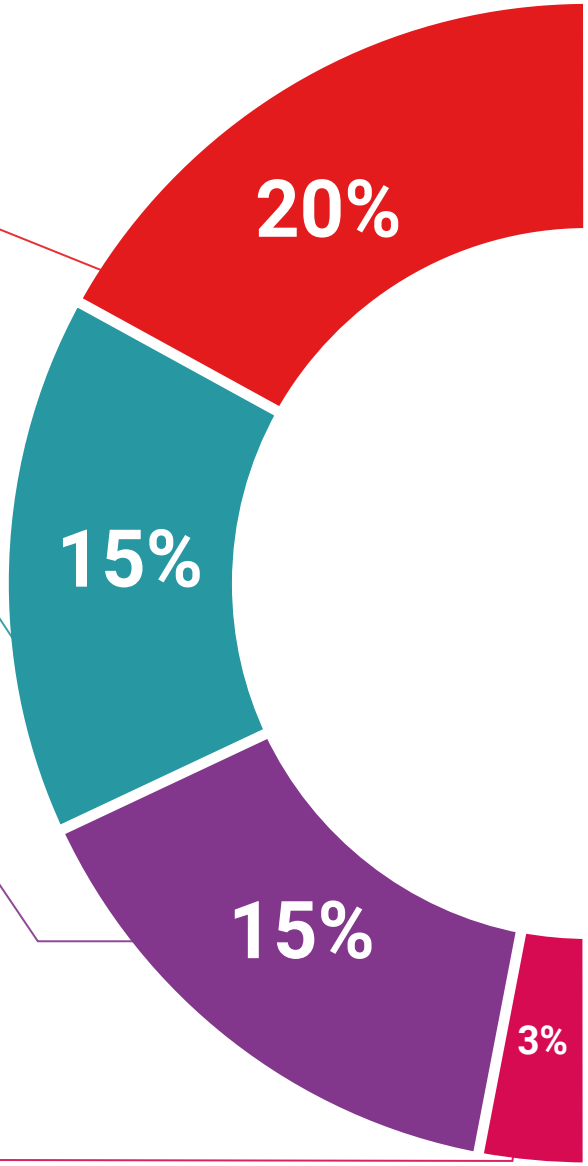
Resúmenes interactivos

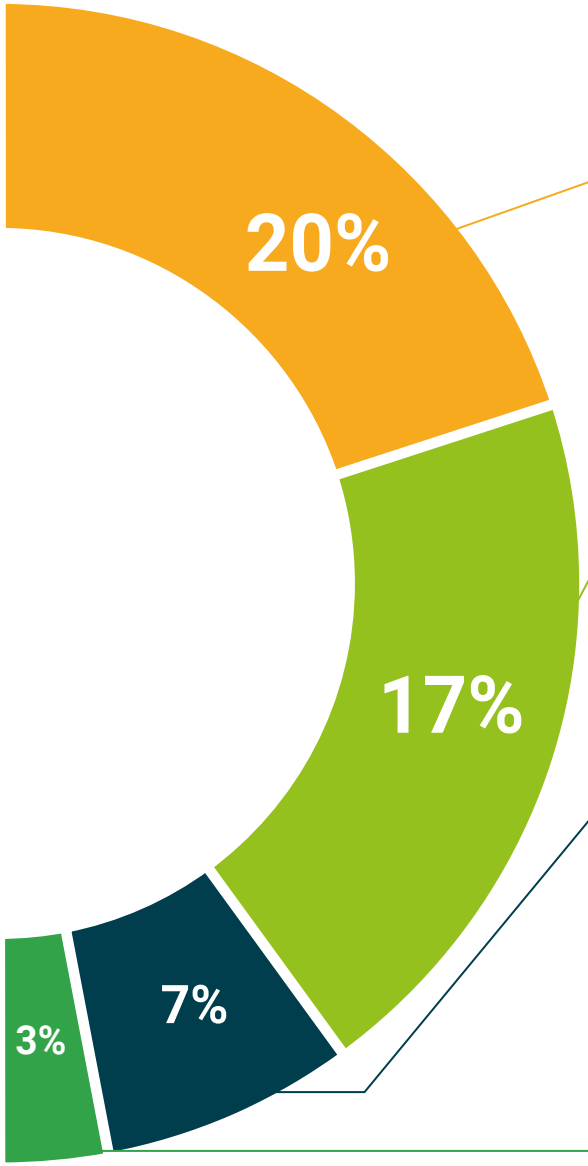
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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 cuadro docente es uno de los pilares que garantizan la calidad de este programa. Integrado por expertos con amplio bagaje en ciberseguridad, análisis de riesgos y gestión tecnológica, el claustro está compuesto por profesionales en activo que han liderado proyectos en empresas internacionales, desarrollado estrategias de protección de datos y asesorado a organizaciones en el cumplimiento de normativas globales. Esto significará recibir capacitación de la mano de líderes del sector, quienes no solo compartirán su experiencia, sino que también inspirarán a los egresados a alcanzar un nivel de excelencia profesional.

Gracias a la orientación recibida por los docentes expertos de TECH, dominarás eficientemente la gestión de la seguridad informática en cualquier organización"

Dirección

Dña. Fernández Sapena, Sonia

- Formadora de Seguridad Informática y Hacking Ético en el Centro de Referencia Nacional de Getafe en Informática y Telecomunicaciones de Madrid
- Instructora certificada E-Council
- Formadora en las siguientes certificaciones: EXIN Ethical Hacking Foundation y EXIN Cyber & IT Security Foundation. Madrid
- Formadora acreditada experta por la CAM de los siguientes certificados de profesionalidad: Seguridad Informática (IFCT0190), Gestión de Redes de Voz y datos (IFCM0310), Administración de Redes departamentales (IFCT0410), Gestión de Alarmas en redes de telecomunicaciones (IFCM0410), Operador de Redes de voz y datos (IFCM0110), y Administración de servicios de internet (IFCT0509)
- Colaboradora externa CSO/SSA (Chief Security Officer/Senior Security Architect) en la Universidad de las Islas Baleares
- Ingeniera en Informática por la Universidad de Alcalá de Henares de Madrid
- Máster en DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Profesores

D. Oropesiano Carrizosa, Francisco

- Ingeniero Informático
- Técnico en Microinformática, Redes y Seguridad en CAS Training
- Desarrollador de Servicios Web, CMS, e-commerce, UI y UX en Fersa Reparaciones
- Gestor de Servicios Web, Contenidos, Correo y DNS en Oropesia Web & Network
- Diseñador Gráfico y de Aplicaciones Web en Xarxa Sakai Projectes SL
- Diplomado en Informática de Sistemas por la Universidad de Alcalá
- Máster en DevOps: Docker and Kubernetes por Cyber Business Center
- Técnico de Redes y Seguridad Informática por la Universidad de las Islas Baleares
- Experto en Diseño Gráfico por la Universidad Politécnica de Madrid

D. Peralta Alonso, Jon

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

D. Ortega López, Florencio

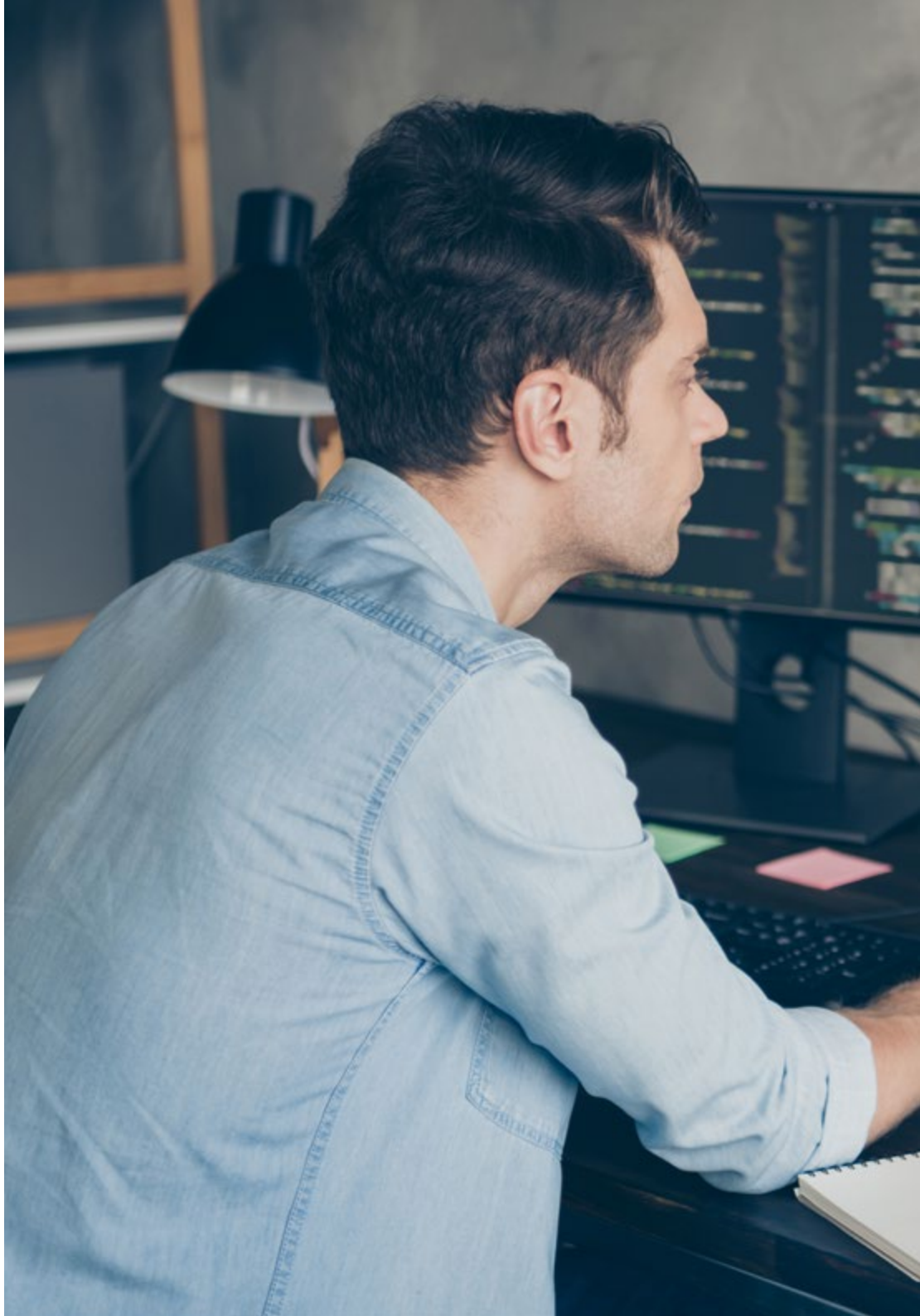
- Consultor de TIC y Seguridad
- Consultor de Seguridad en Gestión de Identidades en SIA Group
- Consultor de TIC y Seguridad como profesional independiente
- Profesor formador en Sector TI
- Graduado en Ingeniería Técnica Industrial por la Universidad de Alcalá
- Máster en Profesorado por la UNIR
- MBA en Gestión y Dirección de Empresas por IDE-CESEM
- Máster en Dirección y Gestión de Tecnología de la Información por IDE-CESEM
- Certified Information Security Management (CISM) por la ISACA

D. Solana Villarias, Fabián

- Consultor de Tecnologías de la Información
- Creador y Administrador de servicios de encuestas en Investigación, Planificación y Desarrollo SA
- Especialista en Mantenimiento de Mercados Financieros y Sistemas Informáticos en Iberia Financial Software
- Desarrollador Web y Especialista en Accesibilidad en Indra
- Licenciado en Ingeniería Superior de Sistemas por la Universidad de Gales/CESINE
- Diplomado en Ingeniería Técnica en Informática de Sistemas por la Universidad de Gales/ CESINE

Dña. López García, Rosa María

- Especialista en Información de Gestión
- Profesora en Linux Professional Institute
- Colaboradora en Academia Hacker Incibe
- Capitana de Talento en Ciberseguridad en Teamciberhack
- Administrativa y Gestora Contable y Financiera en Integra2Transportes
- Auxiliar Administrativo en Recursos de Compras en el Centro de Educación Cardenal Marcelo Espínola
- Técnico Superior en Ciberseguridad y *Hacking* Ético
- Miembro de: Ciberpatrulla



Todos los docentes de este programa acumulan una amplia experiencia, ofreciéndote una perspectiva innovadora sobre los principales avances en este campo de estudios”

10

Titulación

La Maestría Oficial Universitaria en Gestión de Políticas de Seguridad Informática en la Empresa 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 Gestión de Políticas de Seguridad Informática en la Empresa y da un paso adelante en tu carrera profesional”

El plan de estudios de esta Maestría Oficial Universitaria en Gestión de Políticas de Seguridad Informática en la Empresa se encuentra incorporado a la Secretaría de Educación Pública y al Sistema Educativo Nacional mexicano, mediante número de RVOE 20232122, de fecha 24/07/2023, 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:

RVOE
EDUCACIÓN SUPERIOR

Ver documento RVOE

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

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 Gestión de Políticas de Seguridad Informática en la Empresa**

No. de RVOE: **20232122**

Fecha de vigencia RVOE: **24/07/2023**

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: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

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 Gestión de Políticas de Seguridad Informática en la Empresa**, 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 validez internaciona"

Cualquier estudiante interesado en tramitar el reconocimiento oficial del título de **Maestría Oficial Universitaria en Gestión de Políticas de Seguridad Informática en la Empresa** 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 Gestión de Políticas de Seguridad Informática en la Empresa** de TECH Universidad cuenta con el Registro de Validez Oficial de Estudios (RVOE) ante 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"

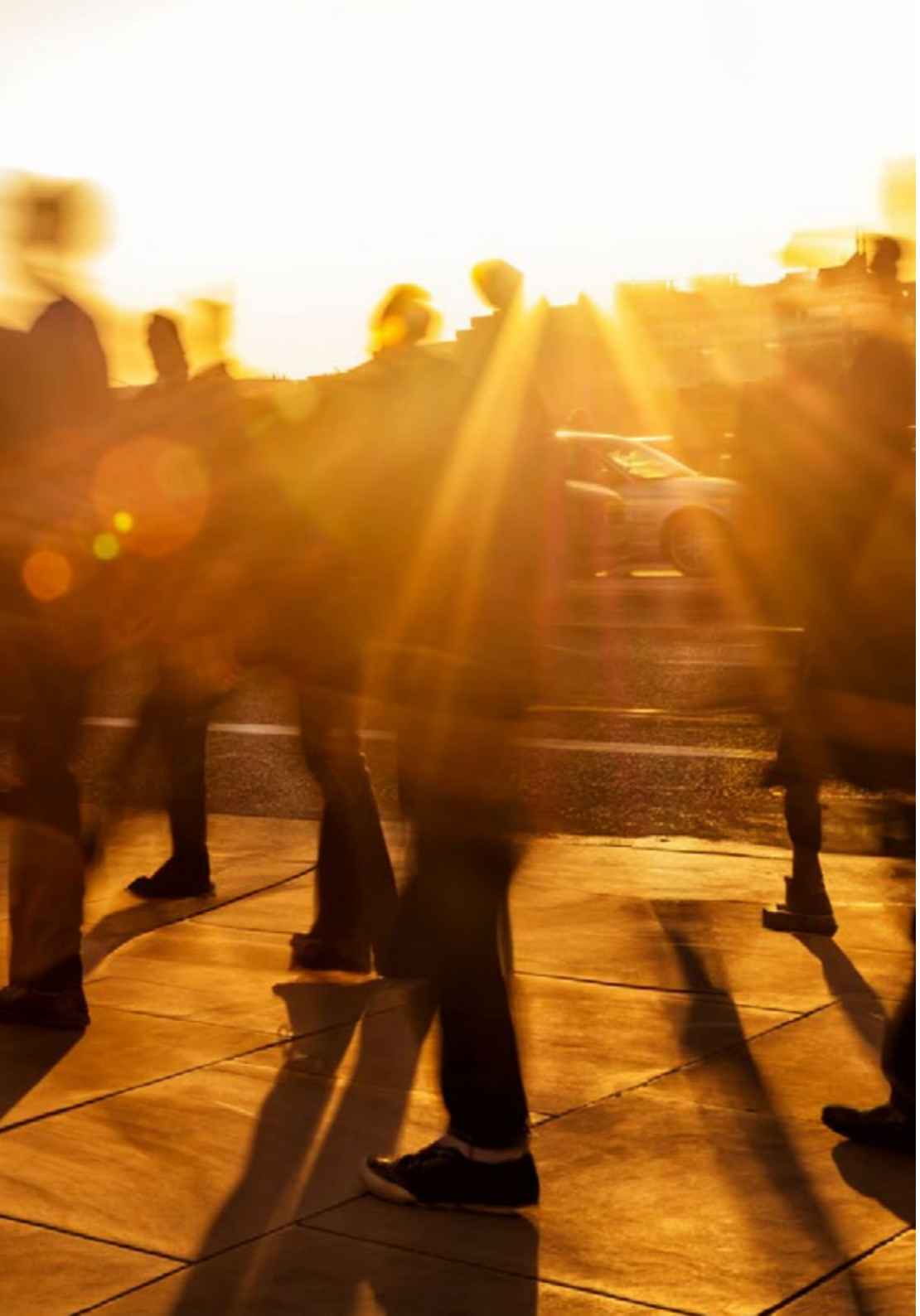
La norma establece que para inscribirse en la **Maestría Oficial Universitaria en Gestión de Políticas de Seguridad Informática en la Empresa** con Registro de Validez Oficial de Estudios (RVOE), es imprescindible cumplir con un perfil académico de ingreso específico.

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 Máster Oficial Universitario 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: 20232122

Maestría Oficial Universitaria
Gestión de Políticas de Seguridad Informática en la Empresa

Idioma: **Español**

Modalidad: **100% online**

Duración: **20 meses**

Fecha de vigencia RVOE: **24/07/2023**

Maestría Oficial Universitaria

Gestión de Políticas de Seguridad Informática en la Empresa

Nº de RVOE: 20232122

RVOE
EDUCACIÓN SUPERIOR

tech universidad