Maestría Oficial Universitaria
Seguridad Informática Avanzada

Nº de RVOE: 20231900

RVOE
EDUCACIÓN SUPERIOR

Título reconocido en USA

tech universidad

tech universidad

Nº de RVOE: 20231900

Maestría Oficial Universitaria Seguridad Informática Avanzada

Idioma: **Español**

Modalidad: **100% en línea**

Duración: **20 meses**

Fecha acuerdo RVOE: **06/07/2023**

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

Índice

01

Presentación del programa

La Seguridad en la comunicación entre dispositivos conectados a tecnologías como el Internet de las Cosas es una de las áreas más demandadas dentro de la Ciberseguridad. A medida que los hogares se llenan de dispositivos interconectados, que tienen acceso a datos personales sensibles, la protección de esta información se vuelve esencial. Por ello, los informáticos requieren mantenerse a la vanguardia de las últimas tendencias en este ámbito para desarrollar protocolos de prevención frente a amenazas cibernéticas como suplantaciones de identidad. Con esta idea en mente, TECH lanza una innovadora titulación universitaria focalizada en las estrategias más modernas para gestionar vulnerabilidades digitales de forma eficiente. Además, se imparte en una cómoda modalidad 100% online. Además, este título universitario está considerado equivalente en EE. UU. por un Master of Science.

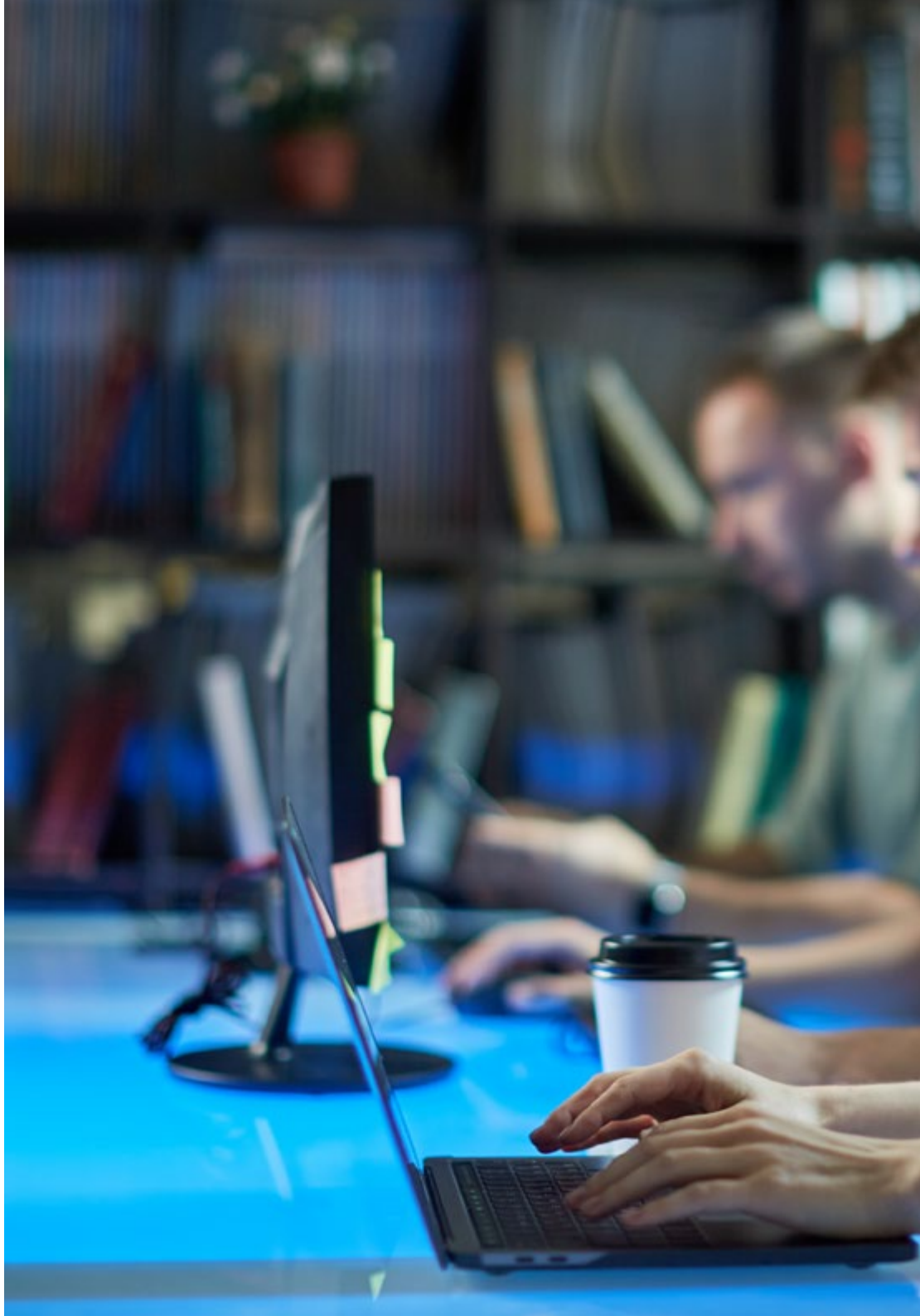
Este es el momento, te estábamos esperando

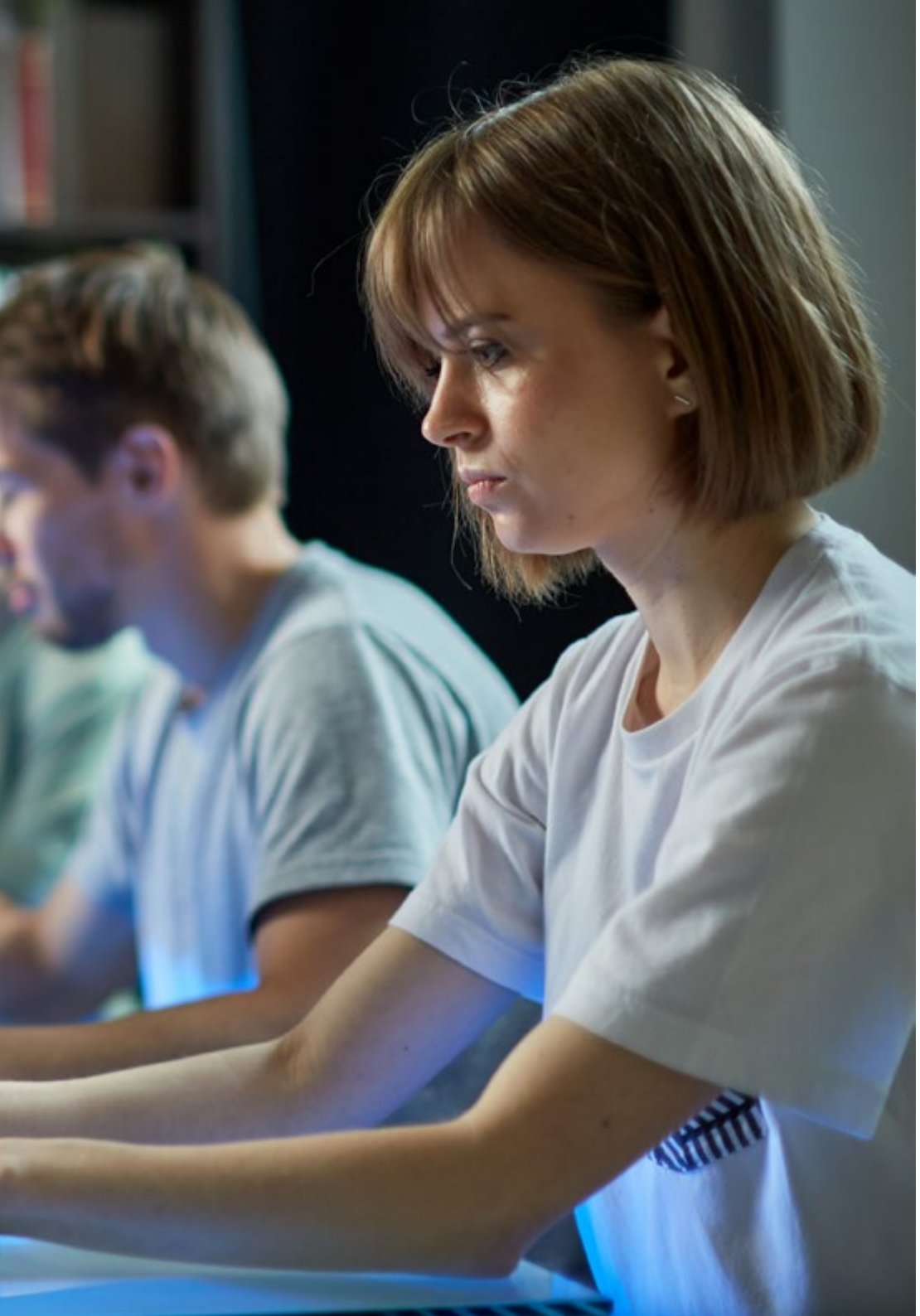
Forma parte de este programa 100% online y oficial de TECH y obtén una equivalencia académica reconocida en EE. UU.”

El análisis forense de ciberataques está adquiriendo cada vez más relevancia al identificar el origen y las consecuencias de los ataques digitales. Este campo impulsa el desarrollo de herramientas y estrategias para prevenir amenazas similares, además de generar debates éticos sobre la gestión de la información en las empresas. A pesar de su importancia, muchas organizaciones aún no reconocen el papel crítico de la ciberseguridad, lo que deja sus datos y los de sus clientes expuestos a ataques. Por eso, es fundamental que las instituciones cuenten con profesionales especializados en esta materia para garantizar el óptimo funcionamiento de su infraestructura tecnológica.

En este contexto, TECH presenta una exclusiva Maestría Oficial Universitaria en Seguridad Informática Avanzada. Diseñado por referencias en este ámbito, el itinerario académico profundizará en aspectos que comprenden desde los fundamentos de la protección en tecnologías de la información o métodos para analizar los riesgos en la arquitectura digital hasta el manejo de instrumentos emergentes como el Internet de las Cosas. De esta forma, los egresados adquirirán competencias avanzadas para proteger a los sistemas informáticos de amenazas sofisticadas como virus, *phishing* o *ransomware*. A su vez, los alumnos serán capaces de gestionar con inmediatez respuestas ante incidentes realizando análisis forenses exhaustivos y tomando las decisiones más eficaces para salvaguardar los intereses de las organizaciones.

Por otra parte, esta titulación universitaria adquiere un mayor dinamismo gracias a las píldoras multimedia y a la amplia variedad de recursos didácticos que ofrece TECH (como lecturas especializadas, resúmenes interactivos o casos de estudio). Asimismo, su disruptiva metodología *Relearning* permitirá a los profesionales de la Informática obtener una puesta al día mucho más efectiva y en un menor tiempo. Así su proceso de aprendizaje será totalmente natural y progresivo, por lo que no tendrán que invertir largas horas al estudio.





Diseñarás e implementarás políticas de Ciberseguridad adaptadas tanto a las necesidades como a los recursos de las organizaciones”

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

Los alumnos han posicionado a TECH como la universidad mejor valorada del mundo en los principales portales de opinión, destacando su calificación más alta de 4,9 sobre 5, obtenida a partir de más de 1.000 reseñas. Estos resultados consolidan a TECH como la institución universitaria de referencia a nivel internacional, reflejando la excelencia y el impacto positivo de su modelo educativo.

03

Plan de estudios

El temario de este programa oficial de TECH está compuesto por 10 asignaturas en los cuales el alumnado podrá analizar e interiorizar todos los avances el ámbito de la Ciberseguridad Informática. Así, los contenidos didácticos profundizarán en las técnicas más efectivas para analizar riegos en la infraestructura digital de las entidades. De este modo, los egresados adquirirán habilidades avanzadas que les permitirán diseñar estrategias sofisticadas para garantizar la Seguridad Informática de las compañías y anticiparse a posibles situaciones de crisis como ataques por parte de *hackers*.

Un temario completo y bien desarrollado

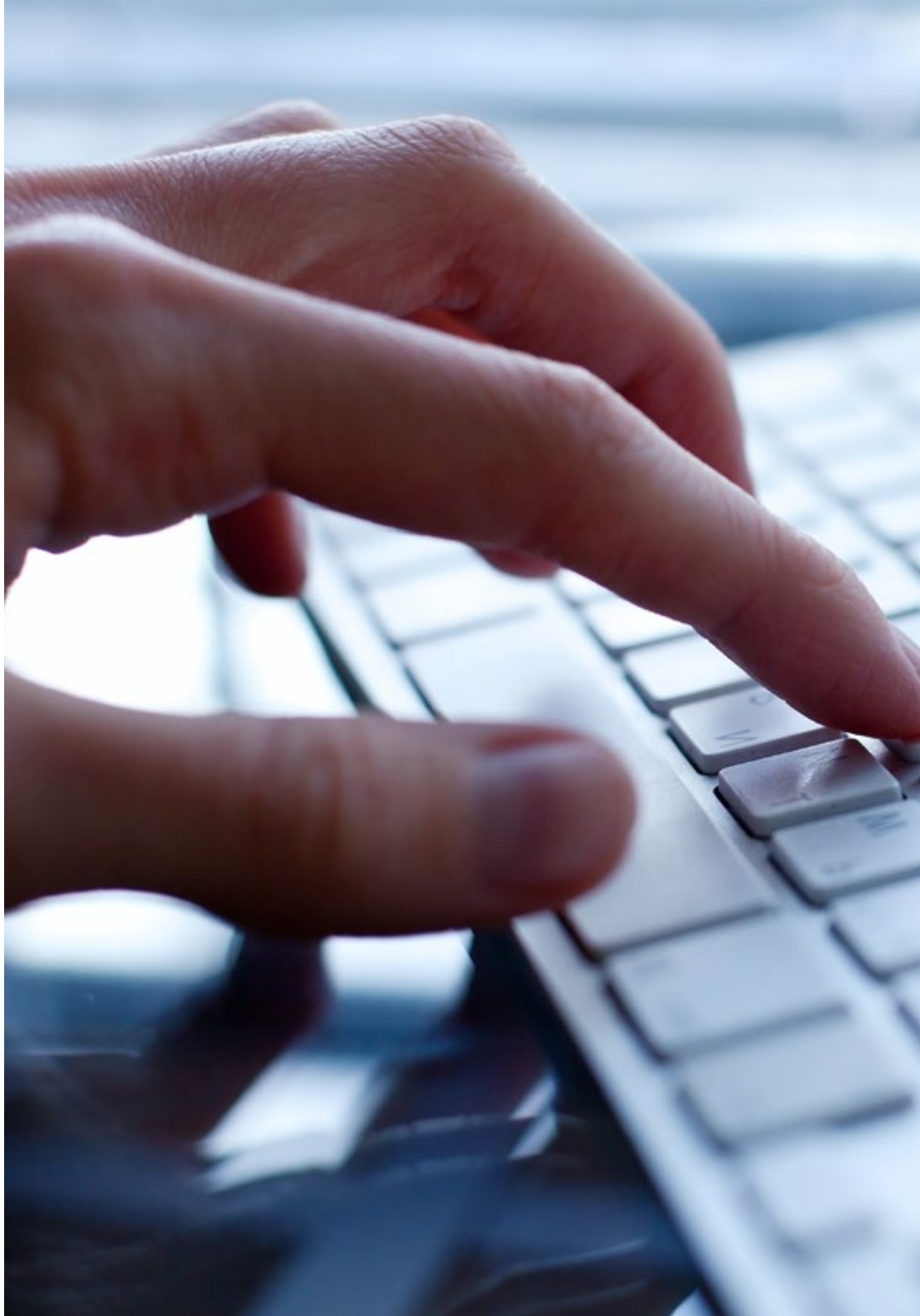
Profundizarás en los estándares internacionales de Seguridad Informáticas, garantizando que tus prácticas cumplan con las normativas legales vigentes"

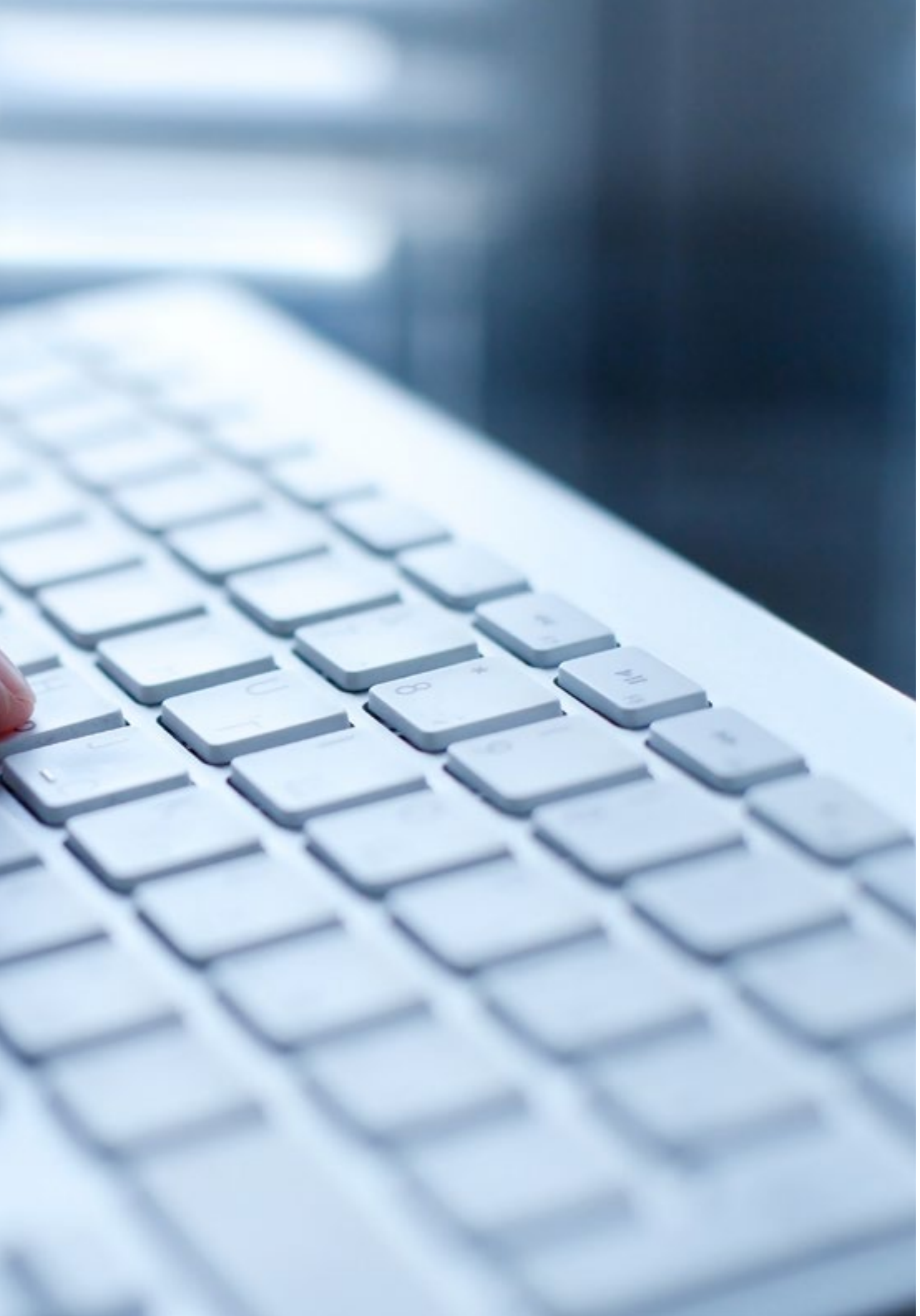
Estos contenidos didácticos se encuentran situados en una plataforma 100% online, por lo que los alumnos podrán planificar individualmente sus horarios y ritmo de estudio. De hecho, lo único que requerirán es un dispositivo electrónico con conexión a internet para acceder al Campus Virtual. Además, en este entorno los expertos hallarán una amplia gama de recursos multimedia que amenizarán su experiencia académica. Entre ellos, figuran los vídeos explicativos, las lecturas especializadas o los casos de estudio prácticos reales.

El sistema Relearning aplicado por TECH en esta Maestría Oficial Universitaria reduce las largas horas de estudio tan frecuentes en otros métodos de enseñanza. ¡Asimilarás los conceptos esenciales de manera natural!"

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	Seguridad en el diseño y desarrollo de sistemas
Asignatura 2	Arquitecturas y modelos de Seguridad de la información
Asignatura 3	Gestión de la Seguridad en tecnologías de la información
Asignatura 4	Análisis de riesgos y entorno de Seguridad en tecnología de la información
Asignatura 5	Criptografía en tecnología de la información
Asignatura 6	Gestión de identidad y accesos en Seguridad de las tecnologías de la información y las comunicaciones
Asignatura 7	Seguridad en comunicaciones y operación *software*
Asignatura 8	Seguridad en entornos de la nube
Asignatura 9	Seguridad en comunicaciones de dispositivos de Internet de las Cosas (IoT)
Asignatura 10	Plan de continuidad del negocio asociado a Seguridad

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

Asignatura 1. Seguridad en el diseño y desarrollo de sistemas

1.1. Sistemas de Información
- 1.1.1. Dominios de un Sistema de Información
- 1.1.2. Componentes de un Sistema de Información
- 1.1.3. Actividades de un Sistema de Información
- 1.1.4. Ciclo de vida de un Sistema de Información
- 1.1.5. Recursos de un Sistema de Información

1.2. Sistemas de Información. Tipología
- 1.2.1. Tipos de Sistemas de Información
- 1.2.2. Sistemas de Información. Ejemplos Reales
- 1.2.3. Evolución de los Sistemas de Información: Etapas
- 1.2.4. Metodologías de los Sistemas de Información

1.3. Seguridad de los Sistemas de Información. Implicaciones Legales
- 1.3.1. Acceso a datos
- 1.3.2. Amenazas de seguridad: Vulnerabilidades
- 1.3.3. Implicaciones legales: Delitos
- 1.3.4. Procedimientos de mantenimiento de un Sistema de Información

1.4. Seguridad de un Sistema de Información. Protocolos de Seguridad
- 1.4.1. Seguridad de un Sistema de Información
- 1.4.2. Servicios de Seguridad
- 1.4.3. Protocolos de Seguridad de la Información. Tipología
- 1.4.4. Sensibilidad de un Sistema de Información

1.5. Seguridad en un Sistema de Información. Medidas y Sistemas de Control de Acceso
- 1.5.1. Medidas de Seguridad
- 1.5.2. Tipo de medidas de seguridad
- 1.5.3. Sistemas de Control de Acceso. Tipología
- 1.5.4. Criptografía

1.6. Seguridad en Redes e Internet
- 1.6.1. Dispositivo de seguridad "Firewall"
- 1.6.2. Identificación Digital
- 1.6.3. Virus y Gusanos
- 1.6.4. Ejemplos y Casos Reales

1.7. Delitos Informáticos
- 1.7.1. Delitos informáticos. Tipología
- 1.7.2. Delito Informático. Ataque. Tipologías
- 1.7.3. El Caso de la Realidad Virtual
- 1.7.4. Perfiles de delincuentes y víctimas. Tipificación del delito
- 1.7.5. Delitos Informáticos. Ejemplos y Casos Reales

1.8. Plan de Seguridad en un Sistema de Información
- 1.8.1. Plan de Seguridad. Objetivos
- 1.8.2. Plan de Seguridad. Planificación
- 1.8.3. Plan de Riesgos. Análisis
- 1.8.4. Política de Seguridad. Implementación en la Organización
- 1.8.5. Plan de Seguridad. Implementación en la Organización
- 1.8.6. Procedimientos de Seguridad. Tipos
- 1.8.7. Planes de Seguridad. Ejemplos

1.9. Plan de contingencia
- 1.9.1. Plan de Contingencia. Funciones
- 1.9.2. Plan de Emergencia: Elementos y Objetivos
- 1.9.3. Plan de Contingencia en la Organización. Implementación
- 1.9.4. Planes de Contingencia. Ejemplos

1.10. Gobierno de la Seguridad de Sistemas de Información
- 1.10.1. Normativa legal
- 1.10.2. Estándares
- 1.10.3. Certificaciones
- 1.10.4. Tecnologías

Asignatura 2. Arquitecturas y modelos de Seguridad de la información

2.1. Arquitectura de seguridad de la información
- 2.1.1. Sistemas de Gestión de Seguridad
- 2.1.2. Alineación estratégica
- 2.1.3. Gestión del riesgo
- 2.1.4. Medición del desempeño

2.2. Modelos de Seguridad de la información
- 2.2.1. Basados en políticas de seguridad
- 2.2.2. Basados en herramientas de protección
- 2.2.3. Basados en equipos de trabajo

2.3. Modelo de Seguridad. Componentes Clave
- 2.3.1. Identificación de riesgos
- 2.3.2. Definición de controles
- 2.3.3. Evaluación continua de niveles de riesgo
- 2.3.4. Plan de concienciación de empleados, proveedores, socios, etc.

2.4. Proceso de Gestión de Riesgos
- 2.4.1. Identificación de activos
- 2.4.2. Identificación de amenazas
- 2.4.3. Evaluación de riesgos
- 2.4.4. Priorización de controles
- 2.4.5. Re-evaluación y riesgo residual

2.5. Procesos de Negocio y Seguridad de la Información
- 2.5.1. Procesos de Negocio
- 2.5.2. Evaluación de riesgos basados en Parámetros de Negocio
- 2.5.3. Análisis de impacto al Negocio
- 2.5.4. Las Operaciones de Negocio y la Seguridad de la Información

2.6. Proceso de Mejora Continua
- 2.6.1. El Ciclo de Deming
  - 2.6.1.1. Planificar
  - 2.6.1.2. Hacer
  - 2.6.1.3. Verificar
  - 2.6.1.4. Actuar

2.7. Arquitecturas de Seguridad
- 2.7.1. Selección y Homogeneización de Tecnologías
- 2.7.2. Gestión de identidades. Autenticación
- 2.7.3. Gestión de accesos. Autorización
- 2.7.4. Seguridad de Infraestructura de Red
- 2.7.5. Tecnologías y Soluciones de Cifrado
- 2.7.6. Seguridad de Equipos Terminales

2.8. El Marco Normativo
- 2.8.1. Normativas sectoriales
- 2.8.2. Certificaciones
- 2.8.3. Legislaciones

2.9. La norma ISO 27001
- 2.9.1. Implementación
- 2.9.2. Certificación
- 2.9.3. Auditorías y pruebas de Intrusión
- 2.9.4. Gestión continua del riesgo
- 2.9.5. Clasificación de la información

2.10. Legislación sobre privacidad. RGPD (GDPR)
- 2.10.1. Alcance del reglamento general de protección de datos
- 2.10.2. Datos personales
- 2.10.3. Roles en el tratamiento de Datos personales
- 2.10.4. Derechos Acceso, Rectificación Cancelación y Oposición (ARCO)
- 2.10.5. El Delegado de Protección de Datos. Funciones

Asignatura 3. Gestión de la Seguridad en tecnologías de la información

3.1. Gestión de la Seguridad
- 3.1.1. Operaciones de seguridad
- 3.1.2. Aspecto legal y regulatorio
- 3.1.3. Habilitación del negocio
- 3.1.4. Gestión de riesgos
- 3.1.5. Gestión de identidades y accesos

3.2. Estructura del Área de Seguridad. La Oficina del Responsable de Seguridad Informática
- 3.2.1. Estructura organizativa
- 3.2.2. Las líneas de defensa
- 3.2.3. Organigrama de la oficina del responsable de seguridad
- 3.2.4. Gestión presupuestaria

3.3. Gobierno de seguridad
- 3.3.1. Comité de Seguridad
- 3.3.2. Comité de Seguimiento de Riesgos
- 3.3.3. Comité de Auditoría
- 3.3.4. Comité de Crisis

3.4. Gobierno de Seguridad. Funciones
- 3.4.1. Políticas y normas
- 3.4.2. Plan Director de Seguridad
- 3.4.3. Cuadros de Mando
- 3.4.4. Concienciación y formación
- 3.4.5. Seguridad en la Cadena de Suministro

3.5. Operaciones de seguridad
- 3.5.1. Gestión de Identidades y Accesos
- 3.5.2. Configuración de Reglas de Seguridad de Red
- 3.5.3. Gestión de Plataformas IDS e IPS
- 3.5.4. Análisis de Vulnerabilidades

3.6. Marco de trabajo de Ciberseguridad. Herramientas NIST y CSF
- 3.6.1. Metodología
  - 3.6.1.1. Identificar
  - 3.6.1.2. Proteger
  - 3.6.1.3. Detectar
  - 3.6.1.4. Responder
  - 3.6.1.5. Recuperar

3.7. Centro de Operaciones de Seguridad
- 3.7.1. Protección
- 3.7.2. Detección
- 3.7.3. Respuesta

3.8. Auditorías de seguridad
- 3.8.1. Prueba de Intrusión
- 3.8.2. Ejercicios de herramienta equipo rojo
- 3.8.3. Auditorías de Código Fuente. Desarrollo seguro
- 3.8.4. Seguridad de Componentes
- 3.8.5. Análisis Forense

3.9. Respuesta a incidentes
- 3.9.1. Preparación
- 3.9.2. Detección, análisis y notificación
- 3.9.3. Contención, erradicación y recuperación
- 3.9.4. Actividad post incidente
- 3.9.5. Guías oficiales de Gestión de Ciberincidentes

3.10. Gestión de Vulnerabilidades
- 3.10.1. Análisis de vulnerabilidades
- 3.10.2. Valoración de vulnerabilidad
- 3.10.3. Bastionado de sistemas
- 3.10.4. Vulnerabilidades de "día 0"

Asignatura 4. Análisis de riesgos y entorno de Seguridad en tecnología de la información

4.1. Análisis del Entorno
- 4.1.1. Análisis de la Situación Coyuntural
- 4.1.2. Análisis del Entorno General
- 4.1.3. Análisis de la situación interna

4.2. Riesgo e incertidumbre
- 4.2.1. Riesgo
- 4.2.2. Gerencia de Riesgos
- 4.2.3. Estándares de Gestión de Riesgos

4.3. Directrices para la Gestión de Riesgos ISO 31000: 2018
- 4.3.1. Objeto
- 4.3.2. Principios
- 4.3.3. Marco de referencia
- 4.3.4. Proceso

4.4. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
- 4.4.1. Objetivos
- 4.4.2. Método
- 4.4.3. Elementos
- 4.4.4. Técnicas
- 4.4.5. Herramientas disponibles

4.5. Transferencia del Riesgo Cibernético
- 4.5.1. Transferencia de Riesgos
- 4.5.2. Riesgos Cibernéticos. Tipología
- 4.5.3. Seguros de Ciber riesgos

4.6. Metodologías Ágiles para la Gestión de Riesgos
- 4.6.1. Metodologías Ágiles
- 4.6.2. Proceso de práctica "Scrum" para la Gestión del riesgo
- 4.6.3. Metodología ágil de gestión de riesgos

4.7. Tecnologías para la Gestión del Riesgo
- 4.7.1. Inteligencia Artificial aplicada a la Gestión de Riesgos
- 4.7.2. Métodos de Preservación del Valor
- 4.7.3. Computación Cuántica. Oportunidad o Amenaza

4.8. Elaboración de Mapas de Riesgos basados en Metodologías Ágiles
- 4.8.1. Representación de la Probabilidad y el Impacto en Entornos Ágiles
- 4.8.2. El Riesgo como Amenaza del Valor
- 4.8.3. Re-evolución en la Gestión de Proyectos y Procesos Ágiles

4.9. Gestión impulsada por el Riesgo o "Risk Driven"
- 4.9.1. Metodología "Risk Driven"
- 4.9.2. Metodología "Risk Driven" en la Gestión de Riesgos
- 4.9.3. Elaboración de un Modelo de Gestión Empresarial impulsado por el Riesgo

4.10. Innovación y Transformación Digital en la Gestión de Riesgos
- 4.10.1. La Gestión de Riesgos Ágiles como fuente de Innovación Empresarial
- 4.10.2. Transformación de Datos en Información Útil para la Toma de Decisiones
- 4.10.3. Visión holística de la empresa a través del riesgo

Asignatura 5. Criptografía en tecnología de la información

5.1. Criptografía
- 5.1.1. Antecedentes
- 5.1.2. Fundamentos matemáticos
- 5.1.3. Componentes

5.2. Criptología
- 5.2.1. Antecedentes de la Criptología
- 5.2.2. Criptoanálisis
- 5.2.3. Esteganografía y Estegoanálisis

5.3. Protocolos criptográficos
- 5.3.1. Bloques básicos
- 5.3.2. Protocolos básicos
- 5.3.3. Protocolos intermedios
- 5.3.4. Protocolos avanzados

5.4. Técnicas criptográficas
- 5.4.1. Longitud de claves
- 5.4.2. Manejo de claves
- 5.4.3. Tipos de algoritmos
- 5.4.4. Funciones resumen
- 5.4.5. Generadores de números pseudoaleatorios
- 5.4.6. Uso de algoritmos

5.5. Criptografía simétrica
- 5.5.1. Cifrados de bloque
- 5.5.2. Algoritmo de cifrados de información DES
- 5.5.3. Algoritmo RC4
- 5.5.4. Esquema de cifrado por bloques AES
- 5.5.5. Combinación de cifrados de bloques
- 5.5.6. Derivación de claves

5.6. Criptografía asimétrica
- 5.6.1. Protocolo criptográfico Diffie-Hellman
- 5.6.2. Algoritmo de firma digital
- 5.6.3. Sistema criptográfico de clave pública RSA
- 5.6.4. Curva elíptica
- 5.6.5. Criptografía asimétrica. Tipología

5.7. Certificados digitales
- 5.7.1. Firma digital
- 5.7.2. Certificados X509
- 5.7.3. Infraestructura de clave pública

5.8. Implementaciones
- 5.8.1. Protocolo de autenticación Kerberos
- 5.8.2. Procesador criptográfico IBM CCA
- 5.8.3. Programa de protección "Pretty Good Privacy" o PGP
- 5.8.4. Tarjetas inteligentes en medios de pago
- 5.8.5. Protocolos de telefonía móvil

5.9. Esteganografía
- 5.9.1. Fundamentos de Esteganografía
- 5.9.2. Fundamentos de Estegoanálisis
- 5.9.3. Aplicaciones y usos

5.10. Criptografía Cuántica
- 5.10.1. Algoritmos cuánticos
- 5.10.2. Protección de algoritmos frente a computación cuántica
- 5.10.3. Distribución de claves cuántica

Asignatura 6. Gestión de identidad y accesos en Seguridad de las tecnologías de la información y las comunicaciones

6.1. Gestión de identidad y accesos
- 6.1.1. Identidad digital
- 6.1.2. Gestión de identidad
- 6.1.3. Federación de identidades

6.2. Control de acceso físico
- 6.2.1. Sistemas de Protección
- 6.2.2. Seguridad de las áreas
- 6.2.3. Instalaciones de recuperación

6.3. Control de acceso lógico
- 6.3.1. Autenticación: Tipología
- 6.3.2. Protocolos de autenticación
- 6.3.3. Ataques de autenticación

6.4. Control de acceso lógico. Autenticación de múltiples factores o MFA
- 6.4.1. Autenticación MFA. Características
- 6.4.2. Contraseñas. Importancia
- 6.4.3. Ataques de Autenticación

6.5. Control de acceso lógico. Autenticación Biométrica
- 6.5.1. Autenticación Biométrica. Características
- 6.5.2. Autenticación biométrica. Requisitos
- 6.5.3. Funcionamiento
- 6.5.4. Modelos y técnicas

6.6. Sistemas de Gestión de Autenticación
- 6.6.1. Inicio de sesión único
- 6.6.2. Protocolo Kerberos
- 6.6.3. Protocolos AAA: autenticación, autorización y contabilización

6.7. Sistemas de Gestión de Autenticación: Sistemas AAA
- 6.7.1. Protocolo TACACS
- 6.7.2. Servidor RADIUS
- 6.7.3. Protocolo de red DIAMETER

6.8. Servicios de Control de Acceso
- 6.8.1. Cortafuegos
- 6.8.2. Redes Privadas Virtuales
- 6.8.3. Sistema de Detección de Intrusiones

6.9. Sistemas de Control de Acceso a la Red
- 6.9.1. Control de acceso a la red o "NAC"
- 6.9.2. Arquitectura y elementos
- 6.9.3. Funcionamiento y estandarización

6.10. Acceso a redes inalámbricas
- 6.10.1. Tipos de Redes Inalámbricas
- 6.10.2. Seguridad en Redes Inalámbricas
- 6.10.3. Ataques en Redes Inalámbricas

Asignatura 7. Seguridad en comunicaciones y operación *software*

7.1. Seguridad Informática en Comunicaciones y Operación Software
- 7.1.1. Seguridad Informática
- 7.1.2. Ciberseguridad
- 7.1.3. Seguridad en la nube

7.2. Seguridad informática en Comunicaciones y Operación Software. Tipología
- 7.2.1. Antecedentes
- 7.2.2. Seguridad Física
- 7.2.3. Seguridad Lógica

7.3. Seguridad en Comunicaciones
- 7.3.1. Principales elementos
- 7.3.2. Seguridad de redes
- 7.3.3. Mejores prácticas

7.4. Ciberinteligencia
- 7.4.1. Ingeniería social
- 7.4.2. La red profunda o "Deep web"
- 7.4.3. Engaño o "Phishing"
- 7.4.4. Programa malicioso o "Malware"

7.5. Desarrollo Seguro en Comunicaciones y Operación Software
- 7.5.1. Protocolo de transferencia de hipertexto "HTTP"
- 7.5.2. Ciclo de Vida
- 7.5.3. Seguridad en preprocesador PHP
- 7.5.4. Seguridad NET
- 7.5.5. Mejores prácticas

7.6. Sistemas de Gestión de la Seguridad de la Información en Comunicaciones y Operación Software
- 7.6.1. Marco legal en protección de datos
- 7.6.2. Norma ISO 27021
- 7.6.3. Norma ISO 27017/18

7.7. Tecnologías SIEM
- 7.7.1. Bases y fundamentos
- 7.7.2. Tecnologías de Información de seguridad y gestión de eventos o SIEM
- 7.7.3. Operativa de un Centro de Operaciones de Seguridad

7.8. El Rol de la Seguridad en las Organizaciones
- 7.8.1. Roles en las organizaciones
- 7.8.2. Rol de los especialistas de Internet de las cosas en las compañías
- 7.8.3. Certificaciones reconocidas en el mercado

7.9. Análisis Forense
- 7.9.1. Análisis Forense
- 7.9.2. Metodología
- 7.9.3. Herramientas e implantación

7.10. La Ciberseguridad en la actualidad
- 7.10.1. Principales ataques informáticos
- 7.10.2. Previsiones de empleabilidad
- 7.10.3. Retos

Asignatura 8. Seguridad en entornos de la nube

8.1. Seguridad en Entornos de la nube
- 8.1.1. Antecedentes e importancia
- 8.1.2. Amenazas y riesgos seguridad
- 8.1.3. Aspectos clave de seguridad

8.2. Tipos de infraestructura en la nube
- 8.2.1. Público
- 8.2.2. Privado
- 8.2.3. Híbrido

8.3. Modelo de gestión compartida
- 8.3.1. Elementos de seguridad gestionados por proveedor
- 8.3.2. Elementos gestionados por cliente
- 8.3.3. Definición de la Estrategia para Seguridad

8.4. Mecanismos de prevención
- 8.4.1. Sistemas de gestión de autenticación
- 8.4.2. Sistema de gestión de autorización: Políticas de acceso
- 8.4.3. Sistemas de gestión de claves

8.5. Securización de Sistemas
- 8.5.1. Securización de los sistemas de almacenamiento
- 8.5.2. Protección de los sistemas de base de datos
- 8.5.3. Securización de datos en tránsito

8.6. Protección de infraestructura
- 8.6.1. Diseño e implementación de red segura
- 8.6.2. Seguridad en recursos de computación
- 8.6.3. Herramientas y recursos para protección de infraestructura

8.7. Detección de las Amenazas y Ataques
- 8.7.1. Sistemas de Auditoría y Monitorización
- 8.7.2. Sistemas de eventos y alarmas
- 8.7.3. Sistemas SIEM

8.8. Respuesta ante incidentes
- 8.8.1. Plan de respuesta a incidentes
- 8.8.2. La continuidad de negocio
- 8.8.3. Análisis forense y remediación de incidentes de la misma naturaleza

8.9. Seguridad en la nube de acceso público
- 8.9.1. Servicios de Amazon en la nube
- 8.9.2. Servicios de Microsoft en la nube
- 8.9.3. Servicios de Google en la nube
- 8.9.4. Servicios Oracle en la nube

8.10. Normativa y cumplimiento
- 8.10.1. Cumplimiento de normativas de seguridad
- 8.10.2. Gestión de riesgos
- 8.10.3. Personas y Proceso en las Organizaciones

Asignatura 9. Seguridad en comunicaciones de dispositivos de Internet de las Cosas (IoT)

9.1. Seguridad en Comunicaciones de Dispositivos provistos con internet o "IoT"
- 9.1.1. Telemetría
- 9.1.2. Conectividad Máquina a Máquina
- 9.1.3. Democratización de la Telemetría

9.2. Modelos de Referencia
- 9.2.1. Importancia
- 9.2.2. Características
- 9.2.3. Arquitectura simplificada

9.3. Vulnerabilidades de seguridad del IoT
- 9.3.1. Dispositivos IoT
- 9.3.2. Casuística de Uso
- 9.3.3. Vulnerabilidades

9.4. Conectividad del IoT
- 9.4.1. Tipos de Redes
- 9.4.2. Tecnologías inalámbricas no IoT
- 9.4.3. Tecnologías inalámbricas LPWAN

9.5. Tecnologías LPWAN
- 9.5.1. El triángulo de hierro de las redes LPWAN
- 9.5.2. Bandas de frecuencia libres vs. bandas licenciadas
- 9.5.3. Opciones de tecnologías LPWAN

9.6. Tecnología LoRaWAN
- 9.6.1. Antecedentes
- 9.6.2. Casos de uso y Ecosistema
- 9.6.3. Seguridad en LoRaWAN

9.7. Tecnología Sigfox
- 9.7.1. Antecedentes
- 9.7.2. Casos de uso y Ecosistema
- 9.7.3. Seguridad en Sigfox

9.8. Tecnología Celular IoT
- 9.8.1. Tecnología Celular IoT
- 9.8.2. Casos de uso Celular y Ecosistema
- 9.8.3. Seguridad en Celular IoT

9.9. Tecnología WiSUN
- 9.9.1. Antecedentes
- 9.9.2. Casos de uso WiSUN y Ecosistema
- 9.9.3. Seguridad

9.10. Otras tecnologías IoT
- 9.10.1. Importancia
- 9.10.2. Casos de uso y Ecosistema de otras Tecnologías IoT
- 9.10.3. Seguridad en otras tecnologías IoT

Asignatura 10. Plan de continuidad del negocio asociado a Seguridad

10.1. Plan de continuidad del negocio
- 10.1.1. Los Planes de Continuidad de Negocio
- 10.1.2. Aspectos CLAVE
- 10.1.3. Plan de valoración de la empresa

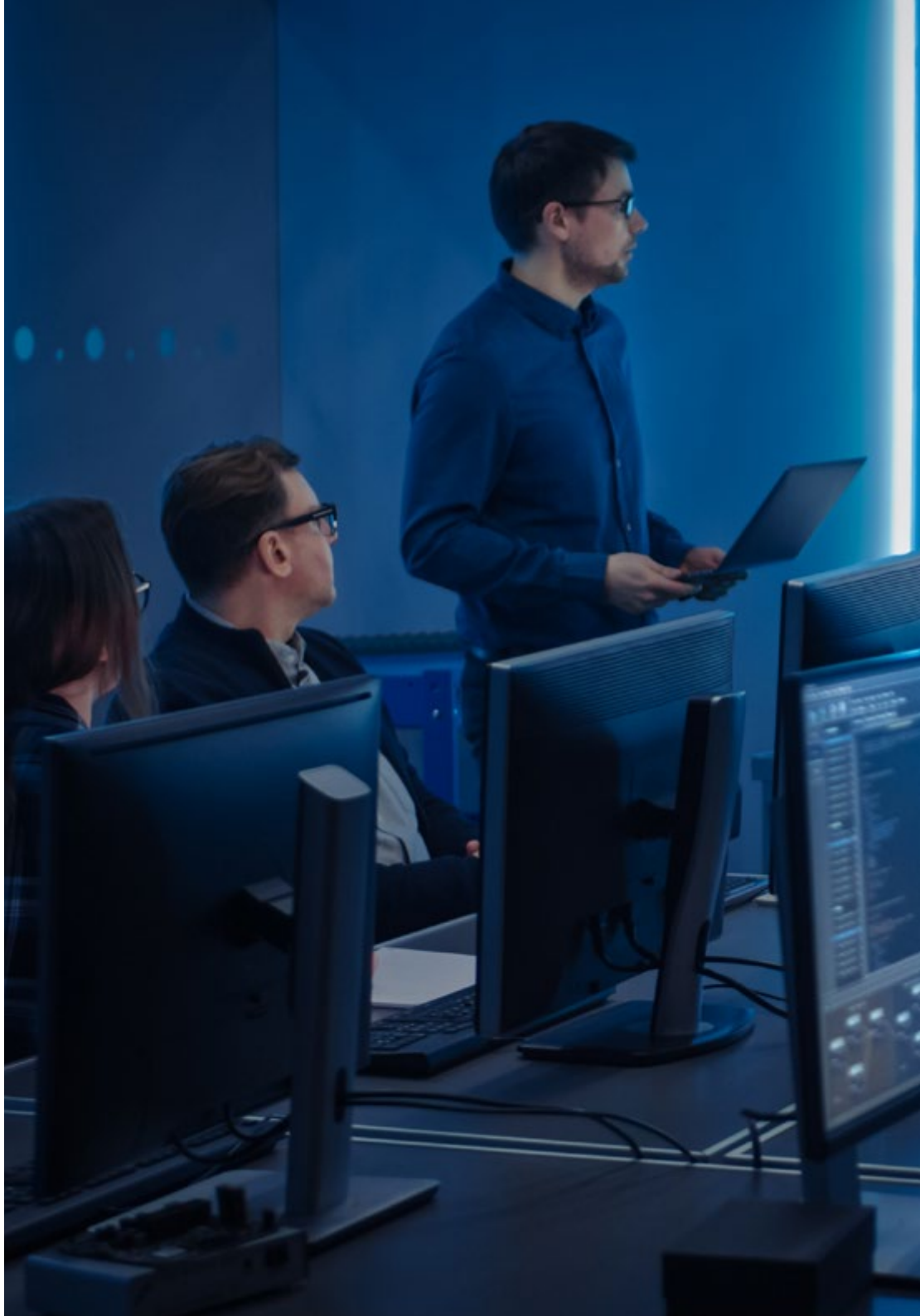
10.2. Métricas en un Plan de Continuidad de Negocio
- 10.2.1. Tiempo máximo tolerable
- 10.2.2. Niveles mínimos de Recuperación
- 10.2.3. Punto de Recuperación Objetivo

10.3. Proyectos de continuidad
- 10.3.1. Plan de Continuidad de Negocio
- 10.3.2. Plan de Continuidad de Tecnologías de la Información y las Comunicaciones
- 10.3.3. Plan de Recuperación ante Desastres

10.4. Gestión de Riesgos asociada al plan de continuidad
- 10.4.1. Análisis de Impacto sobre el negocio
- 10.4.2. Beneficios de la implantación de un Plan
- 10.4.3. Mentalidad basada en Riesgos

10.5. Ciclo de Vida de un Plan de Continuidad de Negocio
- 10.5.1. Fase 1: Análisis de la Organización
- 10.5.2. Fase 2: Determinación de la Estrategia de Continuidad
- 10.5.3. Fase 3: Respuesta a la Contingencia
- 10.5.4. Fase 4: Prueba, Mantenimiento y Revisión

10.6. Fase del Análisis de la Organización de un Plan de continuidad
- 10.6.1. Identificación de procesos en el alcance del Plan
- 10.6.2. Identificación de áreas críticas del negocio
- 10.6.3. Identificación de dependencias entre áreas y procesos
- 10.6.4. Determinación de la protección de dispositivos móviles adecuada
- 10.6.5. Entregables. Creación de un plan



10.7. Fase de Determinación de la Estrategia de Continuidad
- 10.7.1. Roles en la Fase de Determinación de la Estrategia
- 10.7.2. Tareas de la Fase de Determinación de la Estrategia
- 10.7.3. Entregables

10.8. Fase de Respuesta a la Contingencia
- 10.8.1. Roles en la Fase de Respuesta
- 10.8.2. Tareas en esta fase
- 10.8.3. Entregables

10.9. Fase de Pruebas, Mantenimiento y Revisión de un Plan
- 10.9.1. Roles en la Fase de Pruebas, Mantenimiento y Revisión
- 10.9.2. Tareas en la Fase de Pruebas, Mantenimiento y Revisión
- 10.9.3. Entregables

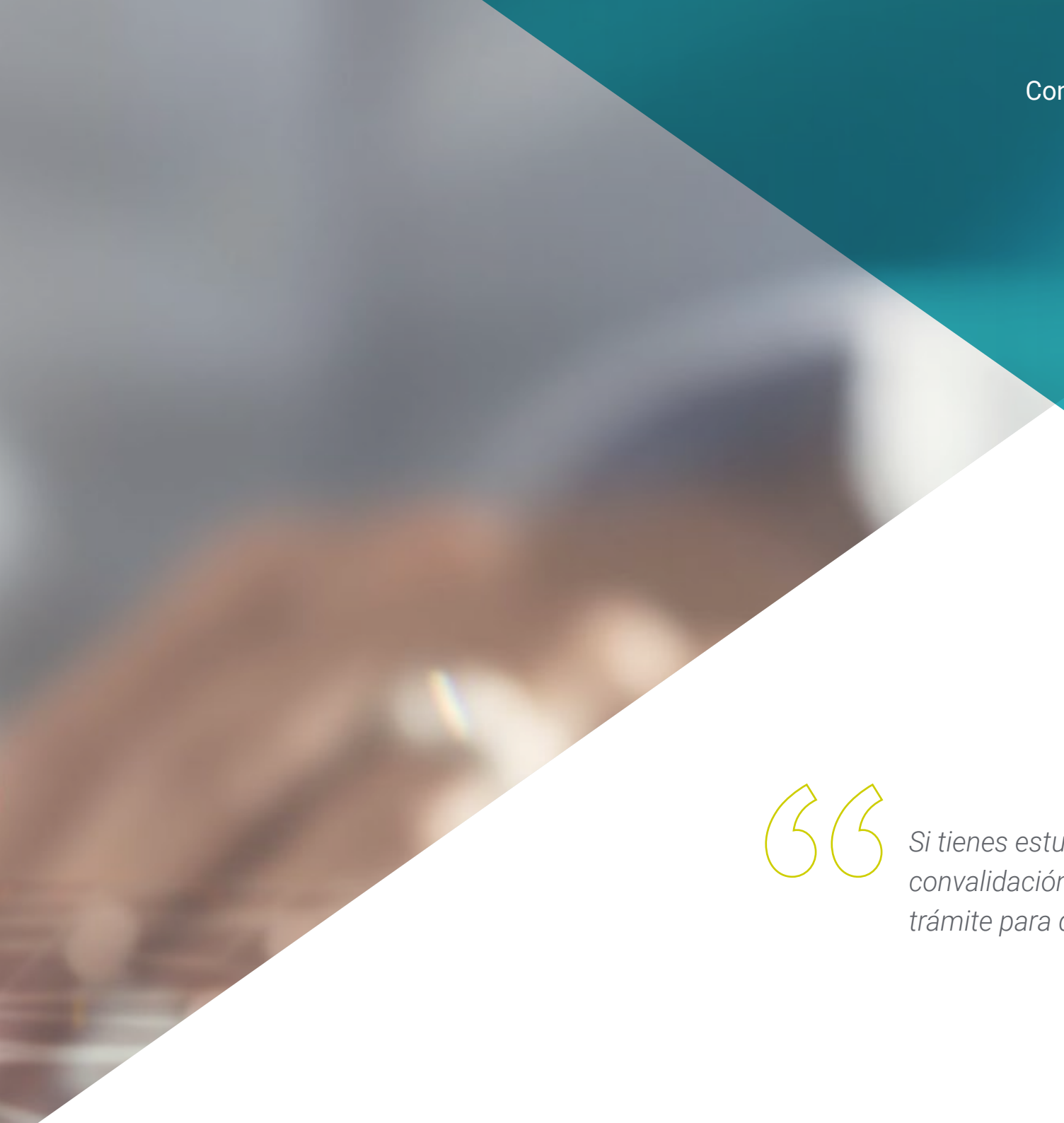
10.10. Normas ISO asociadas a los Planes de Continuidad de Negocio
- 10.10.1. Norma ISO 22301:2019
- 10.10.2. Norma ISO 22313:2020
- 10.10.3. Otras normas ISO e internacionales relacionadas

¿Buscas desarrollar competencias de liderazgo para dirigir equipos de trabajo multidisciplinares y gestionar proyectos relacionados con la Seguridad Informática? Lógralo con esta titulación universitaria en solo 20 meses"

04

Convalidación de asignaturas

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



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

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

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

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

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

¿Qué es la convalidación de estudios?

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

¿Qué es la Opinión Técnica de Convalidación de Asignaturas?

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

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

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

¿Qué documentación necesitará incluir en la solicitud?

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

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

¿En qué plazo se resolverá la solicitud?

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

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

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

Procedimiento paso a paso

05

Matriculación

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

Duración:
20 min

06

Carga de la opinión técnica en campus

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

Duración:
20 min

07

Consolidación del expediente

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

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

05

Objetivos docentes

Esta Maestría Oficial Universitaria está diseñada para profesionales que desean profundizar en las últimas tendencias protección y defensa de la información digital. Tras finalizar el programa, los alumnos dispondrán de un conocimiento integral relativo a la protección de arquitecturas digitales, lo que les permitirá proteger los sistemas frente a amenazas o vulnerabilidades sofisticadas. Así pues, los especialistas obtendrán habilidades estratégicas avanzadas para identificar, evaluar y mitigar riesgos asociados con la Seguridad Informática. De este modo, podrán crear políticas efectivas de prevención ante peligros como inyecciones SQL, ataques DDoS o programas maliciosos.

Diseñarás nuevas metodologías de gestión de riesgos basadas en el enfoque Agile Risk Management, lo que te permitirá adaptarte rápidamente a cambios inesperados"

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
- Diferenciar 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)
- Examinar el Modelo de Gestión de Riesgos basado en la ISO 31.000
- Ahondar en la ciencia de la criptología y la relación con sus ramas: criptografía, criptoanálisis, esteganografía y estegoanálisis
- Abordar los certificados digitales, la Infraestructura de Clave Pública (PKI) y desarrollar el concepto de gestión de identidades
- Dominar diferentes métodos de autenticación, generando conocimiento especializado sobre el ecosistema de seguridad informática
- Detallar los ámbitos de seguridad en Cloud, los servicios y herramientas en cada uno de los ámbitos de seguridad
- Desarrollar las especificaciones de seguridad de cada tecnología LPWAN, analizando de forma comparativa la seguridad de cada una de ellas

Objetivos específicos

Asignatura 1. Seguridad en el diseño y desarrollo de sistemas

- Analizar los elementos más destacados de un Sistema de Información, sus componentes, actividades y ciclo de vida
- Examinar todos los aspectos clave que garantizan la eficiencia en su diseño y desarrollo, centrando la seguridad como uno de los aspectos básicos a tener en cuenta
- Delimitar las principales amenazas de seguridad en el acceso a los datos y redes de un Sistema de Información
- Identificar las implicaciones legales y los procedimientos que hacen seguros los sistemas, con el propósito de salvaguardar todo tipo de información y datos críticos en las empresas

Asignatura 2. Arquitecturas y modelos de seguridad de la información

- Diferenciar las características y componentes más importantes implicados en la Arquitectura y Modelos de Seguridad de la Información
- Evaluar la gestión de riesgos, la administración de recursos, las métricas, los cuadros de mando asociados, y el marco normativo y legislación a aplicar

Asignatura 3. Gestión de la seguridad en tecnologías de la información

- Dominar el empleo de las técnicas más actuales, considerando todas las dimensiones de la seguridad, sin descuidar ningún aspecto
- Implementar medidas de protección técnicas y diversos procedimientos para evitar posibles peligros, amenazas y ataques sufridos por los sistemas de información de muchas organizaciones

Asignatura 4. Análisis de riesgos y entorno de seguridad en tecnología de la información

- Ahondar en los elementos más importantes relacionados con las últimas tendencias en Gestión Inteligente de Riesgos
- Analizar el diseño y la aplicación de nuevas metodologías de gestión de riesgos propias, basadas en el concepto Ágile

Asignatura 5. Criptografía en tecnología de la información

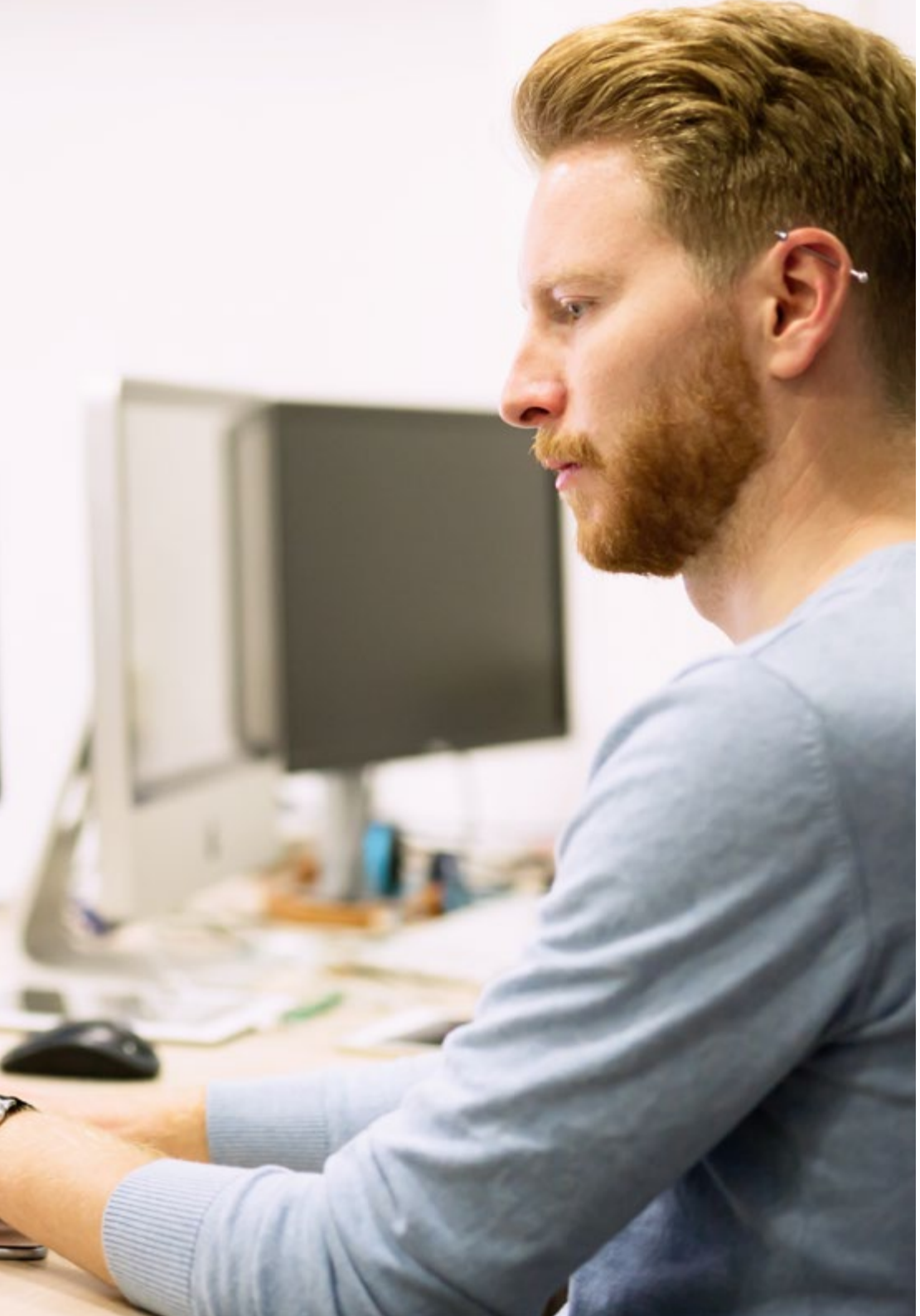
- Emplear las técnicas más importantes para la protección de la información, a través del estudio de los distintos algoritmos criptográficos
- Manejar las herramientas matemáticas en las que se basan la mayoría de las técnicas y algoritmos

Asignatura 6. Gestión de identidad y accesos en seguridad de las tecnologías de la información y las comunicaciones

- Valorar la importancia de la confidencialidad, así como la Gestión de la Identidad y Accesos en la Seguridad de las Tecnologías de la Información y las Comunicaciones
- Asegurar que la información confidencial de una compañía no llegue a las personas equivocadas, no autorizadas

Asignatura 7. Seguridad en comunicaciones y operación software

- Abordar los elementos más importantes relacionados con el Ecosistema de Seguridad Informática en el contexto de un mundo hiperconectado
- Determinar los riesgos que supone para las compañías no tener un entorno de Seguridad Informática, con el propósito de establecer las bases de un centro de operaciones en materia de ciberseguridad



Asignatura 8. Seguridad en entornos de la nube

- Interpretar el modelo de responsabilidad compartida que rige los despliegues en la nube de acceso público, así como los mecanismos de seguridad disponibles
- Delimitar los mecanismos como los procesos a implementar; considerando los servicios y herramientas en cada uno de los ámbitos de seguridad, con el propósito de poner en marcha cualquier proyecto de implantación en la nube

Asignatura 9. Seguridad en comunicaciones de dispositivos de Internet de las Cosas (IoT)

- Identificar la tecnología de conectividad, la lógica en el intercambio de información y el diseño de un sitio web, considerando la capa de transmisión de datos
- Establecer las mejores opciones de conectividad para afrontar un proyecto, con especial énfasis en tecnologías de transmisión inalámbrica

Asignatura 10. Plan de continuidad del negocio asociado a seguridad

- Analizar elementos clave que conforman un plan de continuidad asociada seguridad, a través del estudio de las fases del mismo y las prácticas que se deben adoptar para la minimización, o eliminación total de los riesgos
- Dominar como la guía ISO-22301, con el propósito de lograr la integración de todos los elementos dentro de la Gestión de Riesgos global de la compañía

Un programa de alta intensidad creado para impulsar tu trayectoria como Informático y colocarte en primera línea de competitividad en el sector"

06

Salidas profesionales

Esta Maestría Oficial Universitaria en Seguridad Informática Avanzada abre un amplio abanico de salidas profesionales en el ámbito de la Ciberseguridad. Su temario integral y actualizado capacita a los egresados en técnicas avanzadas de protección de datos, detección de vulnerabilidades y prevención de ciberataques. Gracias a esto, los expertos estarán altamente preparados para asumir roles estratégicos de mayor relevancia en cualquier organización, desde la gestión de riesgos hasta la implementación de estrategias de defensa de sistemas digitales. Así, el alumnado dispondrá de las competencias requeridas para superar los desafíos más exigentes en un entorno laboral cada vez más tecnológico.

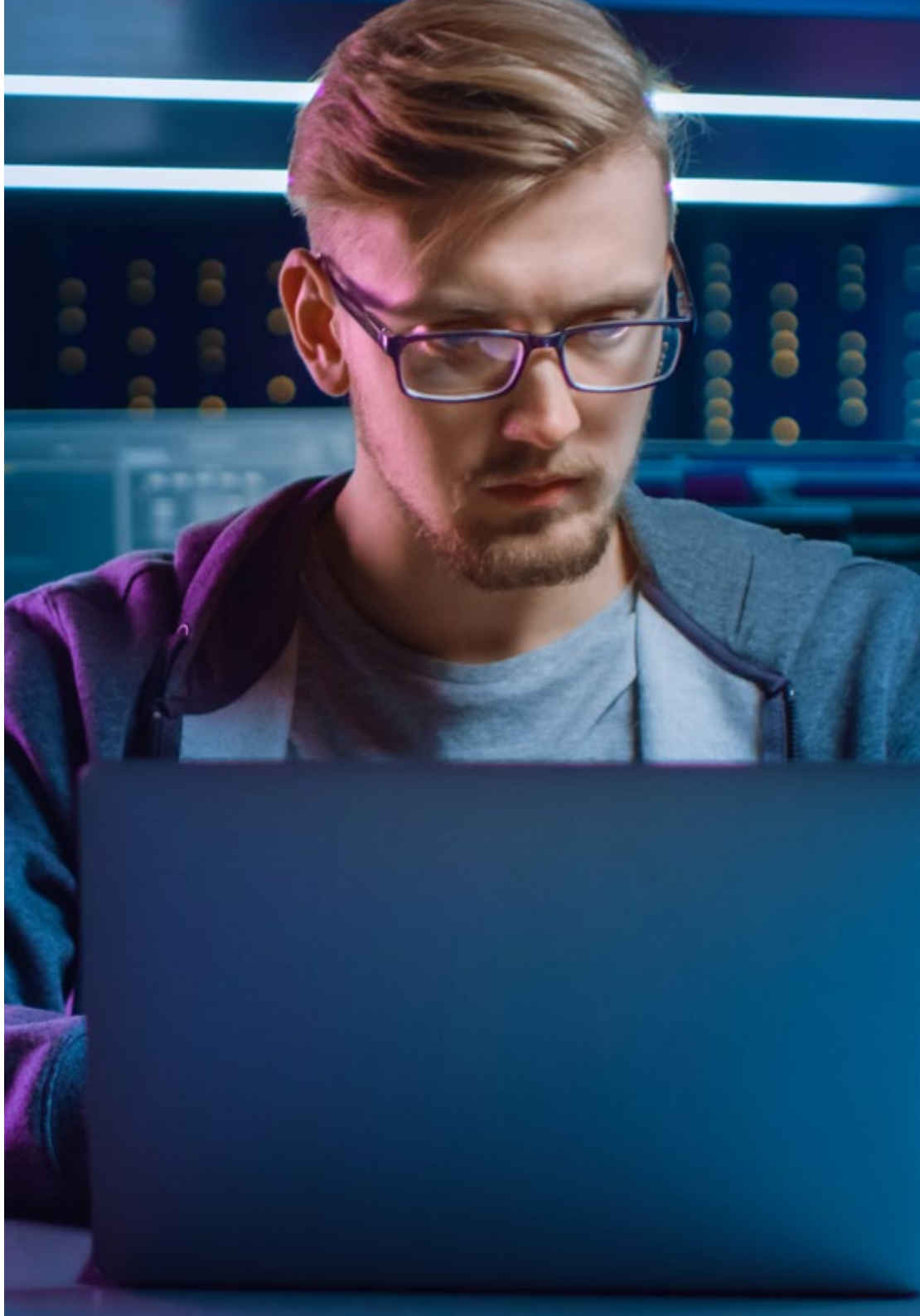
Diseñarás las políticas de Seguridad Informática más innovadoras para defender las infraestructuras digitales de las instituciones de forma óptima"

Perfil del egresado

Este completísimo programa universitario de TECH garantiza a los especialistas de la Ciberseguridad el dominio de las herramientas más modernas para detectar amenazas digitales. Con estos conocimientos integrales, los informáticos podrán anticipar una amplia gama de riesgos cibernéticos entre las que se incluyen las suplantaciones de identidad. De este modo, los alumnos se convertirán en auténticos expertos en la implementación de mecanismos de contención que salvaguarden la privacidad de los datos sensibles de las empresas.

Adquirirás un enfoque crítico para detectar y evaluar amenazas cibernéticas, lo que te permitirá mejorar la toma de decisiones informadas.

- **Análisis de Riesgos y Vulnerabilidades:** Los egresados desarrollan habilidades para identificar, analizar y evaluar riesgos y vulnerabilidades en sistemas informáticos; aplicando metodologías avanzadas para garantizar la protección de infraestructuras digitales
- **Tecnologías de Ciberseguridad:** En un entorno digital cada vez más complejo, los expertos dominan herramientas tecnológicas innovadoras como sistemas de detección de intrusos o criptografía hasta análisis forense digital
- **Gestión de Incidentes de Seguridad:** Los profesionales son capaces de gestionar de manera eficiente los incidentes de Seguridad, desde su identificación hasta la implementación de soluciones preventivas para mitigar futuros riesgos
- **Pensamiento Crítico en Ciberseguridad:** El alumnado aplica el pensamiento crítico para evaluar amenazas cibernéticas, tomar decisiones informadas y desarrollar estrategias innovadoras de defensa frente a ataques sofisticados



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

1. **Especialista en Seguridad Informática Avanzada:** Se encarga de diseñar, implementar y evaluar sistemas de protección en infraestructuras digitales, abordando riesgos cibernéticos en entornos tecnológicos complejos.
   Responsabilidades: Identificar vulnerabilidades digitales, aplicar medidas preventivas y desarrollar estrategias de mitigación de riesgos.
2. **Director de Ciberseguridad:** Liderara proyectos y equipos de Seguridad Informática dentro de organizaciones. Este rol incluye la planificación, ejecución y supervisión de políticas de protección.
   Responsabilidades: Dirigir equipos de Seguridad Informática, supervisar las operaciones diarias en este ámbito y diseñar planes de contingencia ante incidentes.
3. **Analista de Riesgos Cibernéticos:** Su labor se centra en la evaluación y gestión de riesgos asociados con la infraestructura digital de una entidad, aplicando las mejores prácticas para reducir vulnerabilidades.
   Responsabilidades: Evaluar riesgos potenciales, realizar auditorías de Seguridad, implementar herramientas de protección y analizar informes sobre situaciones de crisis.
4. **Consultor en Ciberseguridad Avanzada:** Brinda asesoría holística a organizaciones para optimizar su infraestructura tecnológica, prevenir ciberataques y optimizar los sistemas de protección digital.
   Responsabilidades: Ofrecer recomendaciones personalizadas sobre medidas de seguridad, realizar auditorías de sistemas informáticos y desarrollar planes de acción ante posibles amenazas.
5. **Investigador en Ciberseguridad:** Realizan análisis exhaustivos para mejorar las técnicas de protección contra amenazas informáticas, crear soluciones innovadoras de Seguridad y desarrollar tecnologías de defensa vanguardistas.
   Responsabilidades: Llevar a cabo investigaciones sobre ciberamenazas emergentes y desarrollar propuestas sofisticadas para mitigarlas.

> *Liderarás proyectos de investigación minuciosos sobre áreas como las tendencias emergentes en cibercriminalidad, facilitando la creación de nuevos algoritmos criptográficos"*

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 Oficial Universitaria, podrá aprender idiomas de un modo sencillo y práctico.

Acredita tu competencia lingüística

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

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

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

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

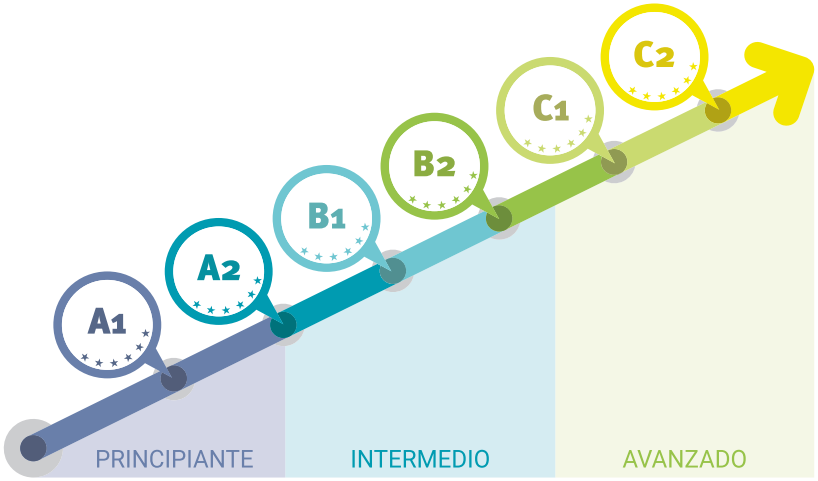
El estudiante aprenderá, mediante actividades en contextos reales, la resolución de situaciones cotidianas de comunicación en entornos simulados de aprendizaje y se enfrentará a simulacros de examen para la preparación de la prueba de certificación de nivel.

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

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

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

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



08
Metodología de estudio

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

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

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

El alumno: la prioridad de todos los programas de TECH

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

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

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

Los planes de estudios más exhaustivos a nivel internacional

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

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

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

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

Case studies o Método del caso

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

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

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

Método *Relearning*

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

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

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

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

Un Campus Virtual 100% online con los mejores recursos didácticos

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

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

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

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

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

La eficacia del método se justifica con cuatro logros fundamentales:

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

La metodología universitaria mejor valorada por sus alumnos

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

La valoración de los estudiantes sobre la calidad docente, calidad de los materiales, estructura del curso y sus objetivos es excelente. No en valde, la institución se convirtió en la universidad mejor valorada por sus alumnos según el índice global score, 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.

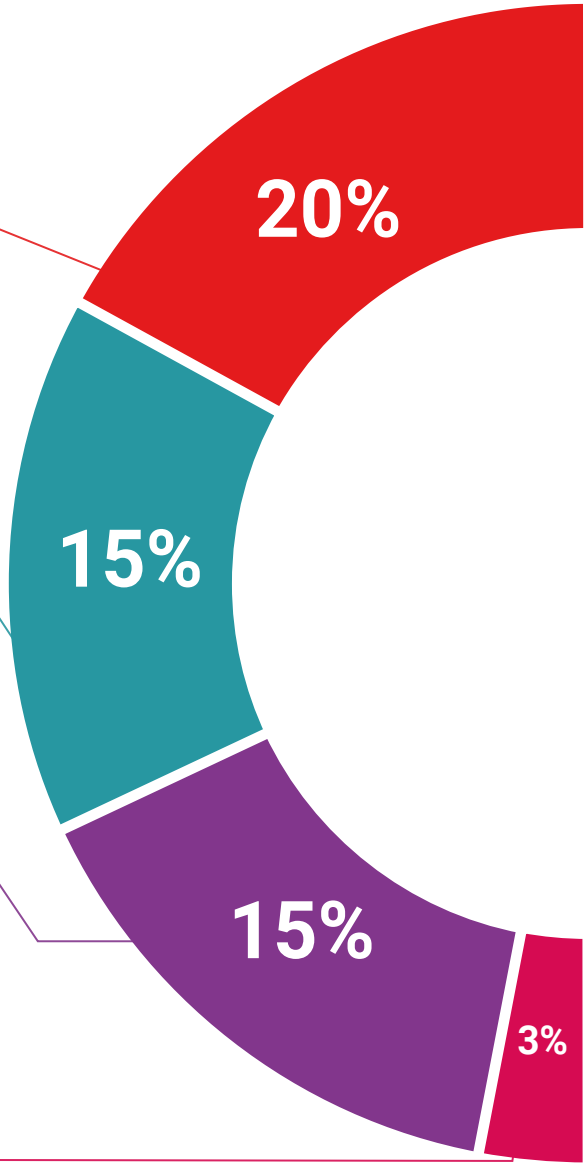
Resúmenes interactivos

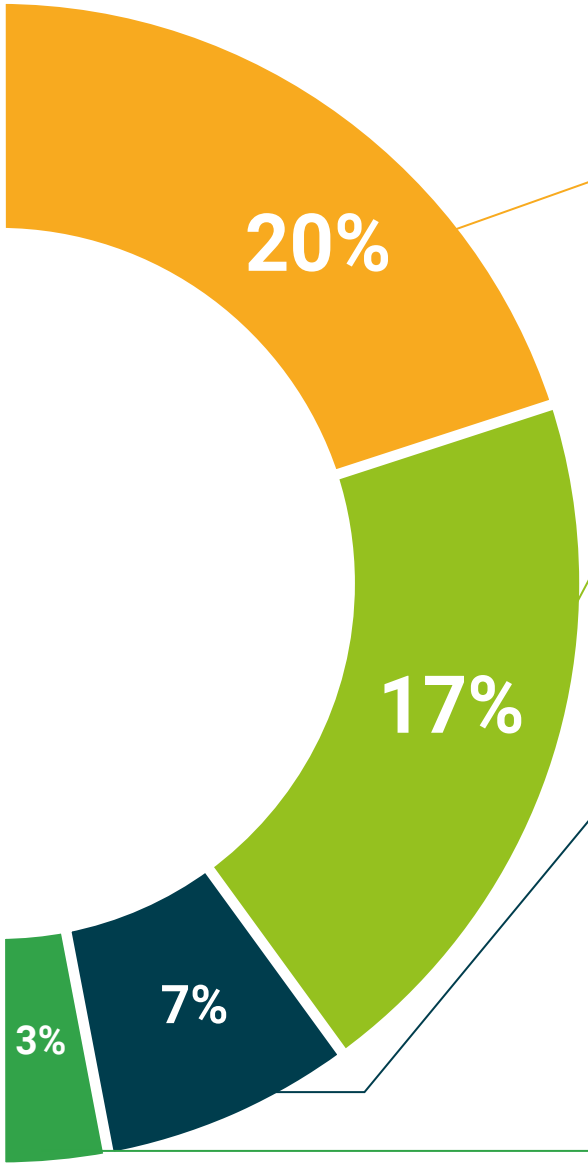
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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

TECH ha conformado para este temario un claustro de primer nivel. Sus miembros son grandes expertos en Ciberseguridad que trabajan, de modo activo, en diferentes empresas ofreciendo competencias avanzadas contra diferentes tipos de ataques. Sus experiencias y las herramientas con que trabajan han sido englobadas en este temario. Así, la titulación se distingue por ser una opción académica de primer nivel, acorde con las demandas y desafíos más retadores del panorama digital actual.

Un experimentado equipo docente especializado en Seguridad Informática Avanzada te guiará durante el transcurso del itinerario académico, resolviendo cualquier duda que te surja"

Dirección

D. Olalla Bonal, Martín

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

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. 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. Nogales Ávila, Javier

- Enterprise Cloud y Sourcing Senior Consultant en Quint
- Cloud y 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

Dr. Gómez Rodríguez, Antonio

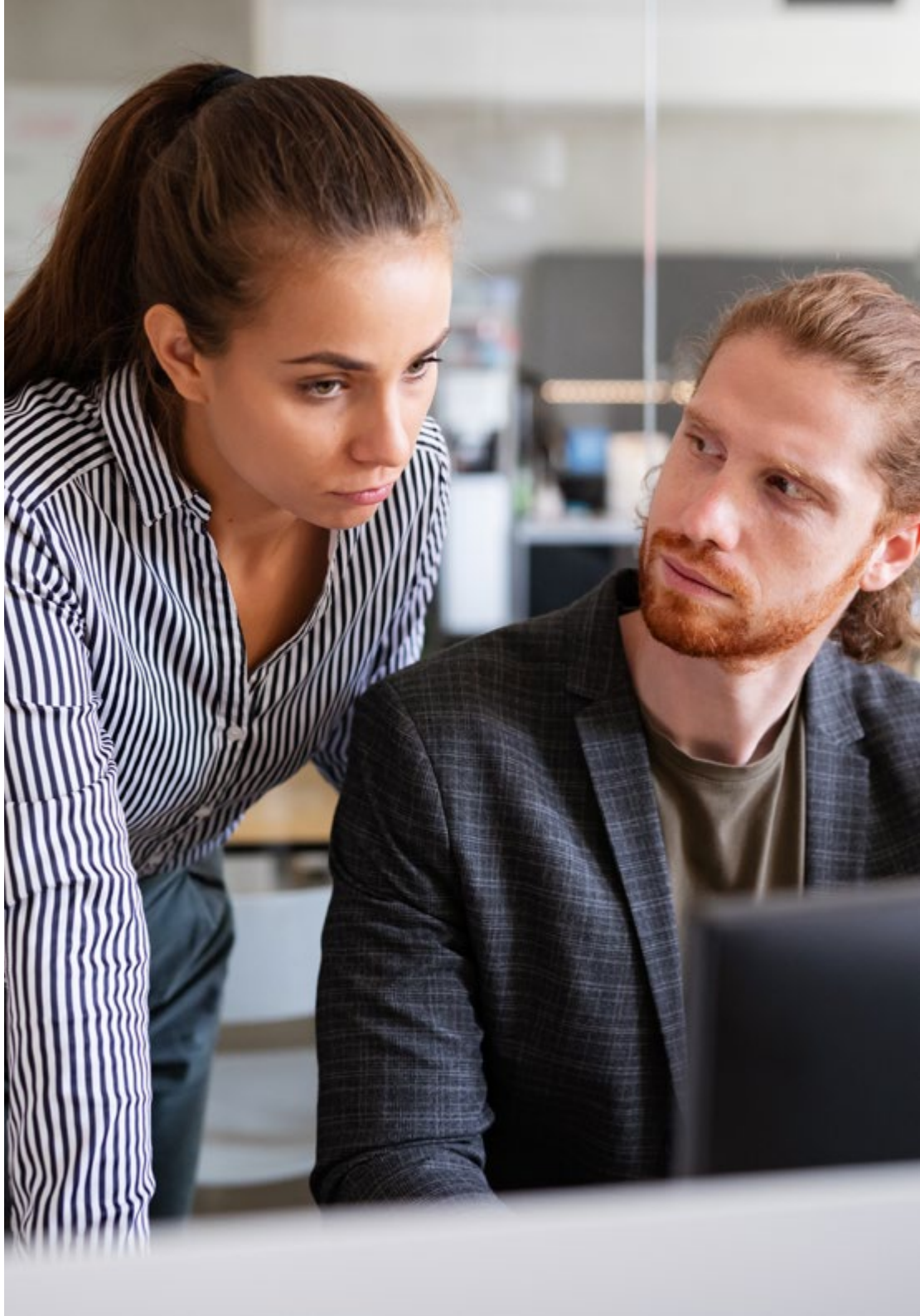
- Ingeniero Principal de Soluciones Cloud para Oracle
- Coorganizador de Málaga Developer Meetup
- Consultor Especialista para Sopra Group y Everis
- Líder de equipos en System Dynamics
- Desarrollador de Softwares en SGO Software
- Máster en E-Business por la Escuela de Negocios de La Salle
- Postgrado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

D. Del Valle Arias, Jorge

- Ingeniero de Telecomunicaciones experto en Desarrollo de Negocios
- 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) en el Grupo Pascual
- Cybersecurity Manager en KPMG. España
- Consultor de Procesos TI y Control y Gestión de Proyectos de Infraestructura en Bankia
- Ingeniero de Herramientas de Explotación en Dalkia
- Desarrollador en el Grupo Banco Popular
- Desarrollador de Aplicaciones por la Universidad Politécnica de Madrid
- Graduada en Ingeniería Informática por la Universidad Alfonso X el Sabio
- Ingeniero Técnico en Informática de Gestión por la Universidad Politécnica de Madrid
- Certified Data Privacy Solutions Engineer (CDPSE) por ISACA

D. Ortega Esteban, Octavio

- Especialista en Marketing y Desarrollo Web
- Programador de Aplicaciones Informáticas y Desarrollador Web *Freelance*
- *Chief Operating Officer* en Smallsquid SL
- Administrador e-commerce de Ortega y Serrano
- Docente en cursos de Certificados de Profesionalidad en Informática y Comunicaciones
- Docente de cursos de Seguridad Informática
- Licenciado en Psicología por la Universidad Abierta de Cataluña
- Técnico Superior Universitario en Análisis, Diseño y Soluciones de *Software*
- Técnico Superior Universitario en Programación Avanzada

D. Embid Ruiz, Mario

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

D. Rodrigo Estébanez, Juan Manuel

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

10

Titulación

La Maestría Oficial Universitaria en Seguridad Informática Avanzada 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 con validez internacional y da un paso adelante en tu carrera profesional”

La **Maestría en Seguridad Informática Avanzada** es un programa con reconocimiento oficial. El plan de estudios se encuentra incorporado a la Secretaría de Educación Pública y al Sistema Educativo Nacional mexicano, mediante número de RVOE **20231900**, de fecha **06/07/2023**, modalidad no escolarizada. Otorgado por la Dirección de Instituciones Particulares de Educación Superior (DIPES).

Además de obtener el título de Maestría Oficial Universitaria, con el que poder alcanzar una posición bien remunerada y de responsabilidad, servirá para acceder al nivel académico de doctorado y progresar en la carrera universitaria. Con TECH el egresado eleva su estatus académico, personal y profesional.

Este programa tiene reconocimiento en los Estados Unidos de América, gracias a la evaluación positiva de la National Association of Credential Evaluation Services de USA (*NACES*), como equivalente al **Master of Science in Cybersecurity** earned by distance education.

Supera con éxito este programa y recibe tu título de Maestría Oficial Universitaria en Seguridad Informática Avanzada con el que podrás desarrollar tu carrera académica"

TECH Universidad ofrece esta Maestría Oficial Universitaria con reconocimiento oficial RVOE de Educación Superior, cuyo título emitirá la Dirección General de Acreditacion, Incorporación y Revalidación (DGAIR) de la Secretaría de Educación Pública (SEP).

Se puede acceder al documento oficial de RVOE expedido por la Secretaría de Educación Pública (SEP), que acredita el reconocimiento oficial internacional de este programa.

Para solicitar más información puede dirigirse a su asesor académico o directamente al departamento de atención al alumno, a través de este correo electrónico: *informacion@techtitute.com*.

RVOE
EDUCACIÓN SUPERIOR

Ver documento RVOE

Título: **Maestría en Seguridad Informática Avanzada**
Título equivalente en USA: **Master of Science in Cybersecurity**
N° de RVOE: **20231900**
Fecha acuerdo RVOE: **06/07/2023**
Modalidad: **100% en línea**
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.

Clave Única de Registro de Población

Folio Digital

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

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

Datos del profesionista

Nombre(s)	Primer Apellido	Segundo Apellido

MAESTRÍA EN SEGURIDAD INFORMÁTICA AVANZADA

Nombre del perfil o carrera	Clave del perfil o carrera

Datos de la institución

TECH MÉXICO UNIVERSIDAD TECNOLÓGICA

Nombre

20231900

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: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

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

Reconocimiento en USA

En **TECH Universidad**, te ofrecemos más que una educación de excelencia, este es un **título con reconocimiento en los Estados Unidos de América (USA)**.

Nuestros programas han sido evaluados por Josef Silny & Associates, Inc., agencia miembro de la **National Association of Credential Evaluation Services de USA** (*NACES*), la principal organización de validación de credenciales académicas en USA.

Obtén un título con reconocimiento en USA y expande tu futuro internacional"

Estudia este programa y obtendrás:

- **Equivalencia en USA:** este título será considerado equivalente a un Master of Science en los Estados Unidos de América, lo que te permitirá ampliar tus oportunidades educativas y profesionales. Esto significa que tu formación será reconocida bajo los estándares académicos norteamericanos, brindándote acceso a oportunidades profesionales sin necesidad de revalidaciones.
- **Ventaja competitiva en el mercado laboral:** empresas globales valoran profesionales con credenciales que cumplen con estándares internacionales. Contar con un título reconocido en USA te brinda mayor confianza ante los empleadores, facilitando la inserción en compañías multinacionales, instituciones académicas y organizaciones con operaciones en varios países.
- **Puertas abiertas para estudios de posgrado en USA:** si deseas continuar con una segunda licenciatura, una maestría o un doctorado en una universidad de USA, este reconocimiento facilita tu admisión. Gracias a la equivalencia de tu título, podrás postularte a universidades en USA sin necesidad de cursar estudios adicionales de validación académica.
- **Certificación respaldada por una agencia reconocida:** Josef Silny & Associates, Inc. es una institución acreditada en USA, que es miembro de la National Association of Credential Evaluation Services de USA (NACES), la organización más prestigiosa en la validación de credenciales internacionales. Su evaluación otorga confianza y validez a tu formación académica ante universidades y empleadores en USA.
- **Mejorar tus ingresos económicos:** tener un título con equivalencia en USA no solo amplía tus oportunidades de empleo, sino que también puede traducirse en mejores salarios. Según estudios de mercado, los profesionales con títulos reconocidos internacionalmente tienen mayor facilidad para acceder a puestos **mejor remunerados** en empresas globales y multinacionales.

- **Postularte a las Fuerzas Armadas de USA:** si eres residente en EE.UU. (Green Card Holder) y deseas unirte a las Fuerzas Armadas de los Estados Unidos de América, este título universitario cumple con los requisitos **educativos mínimos** exigidos, sin necesidad de estudios adicionales. Esto te permitirá avanzar en el proceso de selección y optar a una carrera militar con mayores beneficios y posibilidades de ascenso.
- **Realizar trámites migratorios o certificación laboral:** si planeas solicitar una visa de trabajo, una certificación profesional o iniciar un trámite migratorio en USA, tener un título con equivalencia oficial puede facilitar el proceso. Muchas categorías de visa y programas de residencia requieren demostrar formación académica reconocida, y este reconocimiento te da una base sólida para cumplir con dichos requisitos.

Tras la evaluación realizada por la agencia de acreditación miembro de la **National Association of Credential Evaluation Services de USA** (*NACES*), este programa obtendrá una equivalencia por el:

Master of Science in Cybersecurity

Tramita tu equivalencia

Una vez obtengas el título, podrás tramitar tu equivalencia a través de TECH sin necesidad de ir a Estados Unidos y sin moverte de tu casa.

TECH realizará todas las gestiones necesarias para la obtención del informe de equivalencia de grado académico que reconoce, en los Estados Unidos de América, los estudios realizados en TECH Universidad.

12

Homologación del título

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

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

Cualquier estudiante interesado en tramitar el reconocimiento oficial del título de **Maestría Oficial Universitaria en Seguridad Informática Avanzada** 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"

13

Requisitos de acceso

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

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

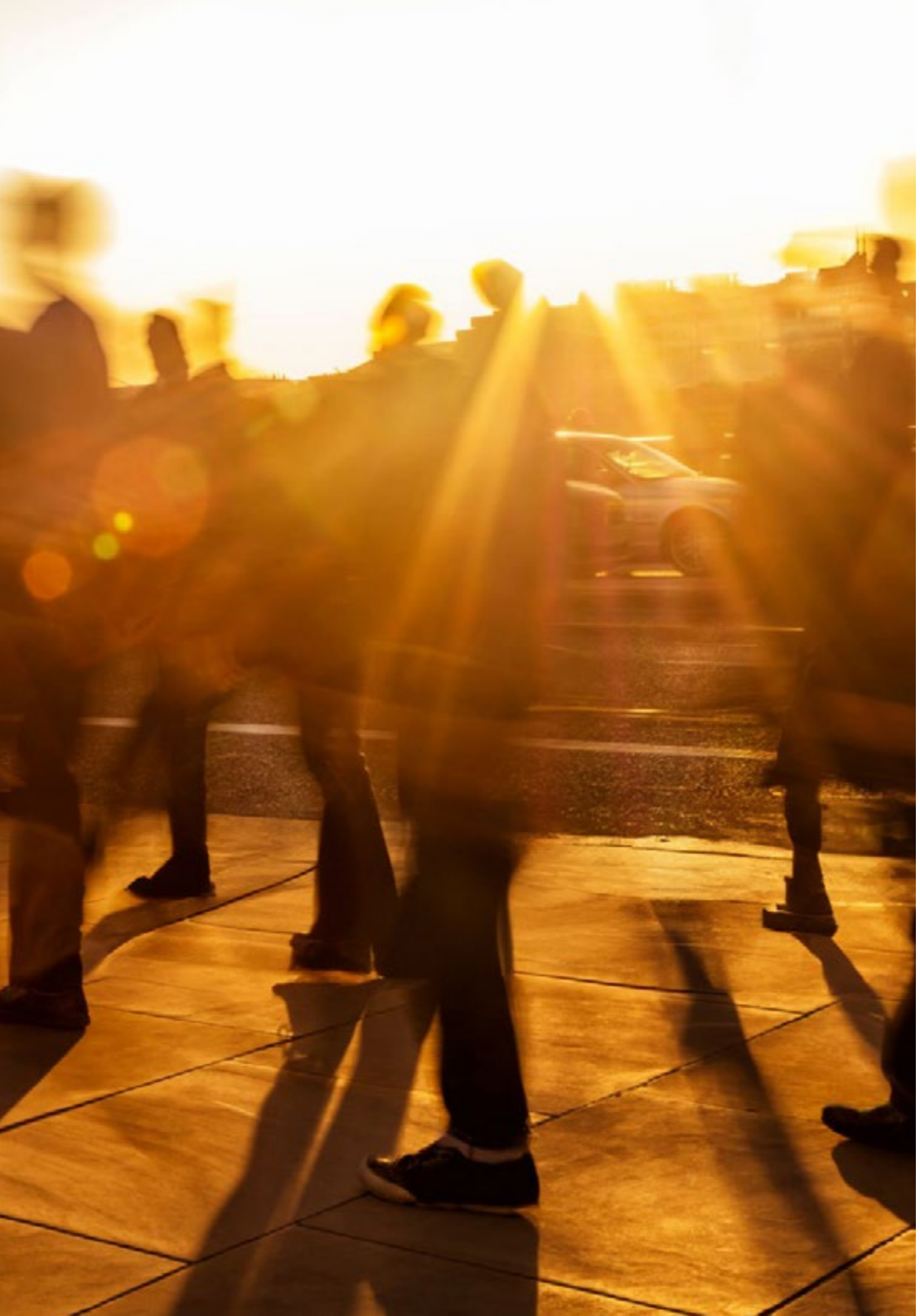
La norma establece que para inscribirse en la **Maestría Oficial Universitaria en Seguridad Informática Avanzada** con Registro de Validez Oficial de Estudios (RVOE), es imprescindible cumplir con un perfil académico de ingreso específico.

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"

14

Proceso de admisión

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

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

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

Los pasos para la admisión son simples:

1. Facilitar los datos personales al asesor académico para realizar la inscripción.
2. Recibir un email en el correo electrónico en el que se accederá a la página segura de TECH y aceptar las políticas de privacidad y las condiciones de contratación e introducir los datos de tarjeta bancaria.
3. Recibir un nuevo email de confirmación y las credenciales de acceso al campus virtual.
4. Comenzar el programa en la fecha de inicio oficial.

De esta manera, el estudiante podrá incorporarse al curso académico sin esperas. Posteriormente, se le informará del momento en el que se podrán ir enviando los documentos, a través del campus virtual, de manera muy práctica, cómoda y rápida. Sólo se deberán subir en el sistema para considerarse enviados, sin traslados ni pérdidas de tiempo.

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

Los documentos necesarios que deberán tenerse preparados con calidad suficiente para cargarlos en el campus virtual son:

- Copia digitalizada del documento que ampare la identidad legal del alumno (documento de identificación oficial, pasaporte, acta de nacimiento, carta de naturalización, acta de reconocimiento o acta de adopción)
- Copia digitalizada de Certificado de Estudios Totales de Bachillerato legalizado

Para resolver cualquier duda que surja, el estudiante podrá realizar sus consultas a través del correo: *procesodeadmision@techtitute.com*.

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

tech universidad

Nº de RVOE: 20231900

Maestría Oficial Universitaria
Seguridad Informática Avanzada

Idioma: **Español**

Modalidad: **100% en línea**

Duración: **20 meses**

Fecha acuerdo RVOE: **06/07/2023**

Maestría Oficial Universitaria
Seguridad Informática Avanzada

Nº de RVOE: 20231900

RVOE
EDUCACIÓN SUPERIOR

Título reconocido en USA

tech universidad