Máster Titulo Propio

Gestión de Políticas de Ciberseguridad en la Empresa

tech global university

tech global university

Máster Titulo Propio

Gestión de Políticas de Ciberseguridad en la Empresa

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Global University**
- Acreditación: **60 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: **www.techtitute.com/informatica/master/master-gestion-politicas-ciberseguridad-empresa**

Índice

01

Presentación del programa

a Gestión de Políticas de Ciberseguridad se ha convertido en un aspecto crucial para la protección de la información y los activos corporativos. Según un informe del Instituto Nacional de Ciberseguridad, el 77% de las empresas han experimentado algún tipo de ciberataque en los últimos años, lo que subraya la necesidad urgente de implementar estrategias de protección más robustas. Por lo tanto, esta oportunidad académica de TECH es una respuesta a la creciente demanda de expertos capaces de gestionar y desarrollar políticas de Ciberseguridad. Así, la metodología, basada en material didáctico actualizado y 100% online, está diseñada para ofrecer una experiencia académica flexible, permitiendo a los profesionales adaptarse rápidamente a los desafíos del sector frente a amenazas cibernéticas.

Gracias a este programa universitario 100% online, dominarás las estrategias más avanzadas en la Gestión de Políticas de Ciberseguridad"

En un entorno donde la digitalización ha transformado profundamente las dinámicas empresariales, la Gestión estratégica de la Ciberseguridad se ha convertido en una necesidad ineludible. De hecho, las organizaciones no solo deben proteger sus activos digitales, sino también garantizar la integridad, confidencialidad y disponibilidad de sus datos frente a amenazas cada vez más sofisticadas. En este contexto, la implementación de políticas robustas en materia de ciberseguridad resulta clave para prevenir vulnerabilidades, asegurar la continuidad operativa y preservar la confianza de los clientes y aliados estratégicos.

Frente a estos desafíos, TECH ha desarrollado una titulación universitaria que explorará en profundidad los componentes esenciales de la seguridad Informática. A través de un contenido riguroso, los profesionales abordarán aspectos críticos como la protección de la información, los riesgos derivados de intrusiones maliciosas y las medidas defensivas aplicadas tanto a nivel de software como de hardware. Esta mirada integral no solo contempla los aspectos técnicos, sino también las implicaciones organizativas y normativas que rigen la protección de datos en entornos empresariales.

Gracias a esta propuesta académica, los egresados adquirirán competencias para diseñar, evaluar y aplicar estrategias de Ciberseguridad adaptadas a diferentes contextos corporativos. Además, estarán preparados para anticipar amenazas emergentes, implementar soluciones efectivas y liderar procesos de mejora continua en sistemas de protección digital. Por lo tanto, esta capacitación técnica y estratégica les permitirá asumir con solvencia responsabilidades en áreas clave vinculadas a la gestión de riesgos y la seguridad Informática

Para garantizar una experiencia flexible y eficaz, TECH Universidad ha adoptado un modelo que se adapta al ritmo y disponibilidad de cada persona. Asimismo, su metodología basada en el Relearning, centrada en la revisión inteligente y constante de los contenidos, permite consolidar el conocimiento de manera progresiva. Todo esto se desarrolla en un entorno completamente online, accesible las 24 horas del día, los 7 días de la semana, desde cualquier dispositivo con conexión a internet.

Este **Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa** contiene el programa universitario más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en Gestión de Políticas de Ciberseguridad en la Empresa
- Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que están concebidos recogen una información científica y práctica sobre aquellas disciplinas indispensables para el ejercicio profesional
- Los ejercicios prácticos donde realizar el proceso de autoevaluación para mejorar el aprendizaje
- Su especial hincapié en metodologías innovadoras en la protección de los entornos digitales
- Las lecciones teóricas, preguntas al experto, foros de discusión de temas controvertidos y trabajos de reflexión individual
- La disponibilidad de acceso a los contenidos desde cualquier dispositivo fijo o portátil con conexión a internet

Ampliarás tu perspectiva sobre la complejidad y dinámica de la Ciberseguridad, integrando con claridad los desafíos tecnológicos"

Incorporarás a tu práctica diaria los componentes esenciales de la seguridad Informática para enfrentar con eficacia amenazas persistentes"

Elevarás tus competencias para gestionar con precisión la protección de la información ante escenarios de riesgo digital.

Profundizarás en los enfoques más recientes sobre medidas defensivas aplicadas tanto al software como al hardware.

Incluye en su cuadro docente a profesionales pertenecientes al ámbito de la Gestión de Políticas de Ciberseguridad en la Empresa, que vierten en este programa la experiencia de su trabajo, además de reconocidos especialistas de sociedades de referencia y universidades de prestigio.

Su contenido multimedia, elaborado con la última tecnología educativa, permitirá al profesional un aprendizaje situado y contextual, es decir, un entorno simulado que proporcionará un estudio inmersivo programado para entrenarse ante situaciones reales.

El diseño de este programa se centra en el Aprendizaje Basado en Problemas, mediante el cual el alumno deberá tratar de resolver las distintas situaciones de práctica profesional que se le planteen a lo largo del curso académico. Para ello, el profesional contará con la ayuda de un novedoso sistema de vídeo interactivo realizado por reconocidos expertos.

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.

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

Este exclusivo itinerario académico profundizará en aspectos clave de la Gestión de Políticas de Ciberseguridad en la Empresa. A su vez, se integrará de manera progresiva temáticas como la respuesta ante incidencias de seguridad, la protección física de los recursos tecnológicos y el control ambiental dentro de los entornos corporativos. A lo largo del desarrollo de cada módulo, se facilitará la adquisición de competencias para identificar vulnerabilidades, aplicar protocolos preventivos y diseñar entornos seguros. Además, mediante un enfoque práctico y actualizado, se analizará cómo estas medidas impactan directamente en la continuidad operativa y en la protección integral de los sistemas empresariales.

Ponte al día en las estrategias más eficaces para la protección física de los recursos tecnológicos en entornos corporativos de alta exigencia operativa"

Módulo 1. Sistema de Gestión de Seguridad de Información (SGSI)

1.1. Seguridad de la información. Aspectos clave
  1.1.1. Seguridad de la información
    1.1.1.1. Confidencialidad
    1.1.1.2. Integridad
    1.1.1.3. Disponibilidad
    1.1.1.4. 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 SGSI
  1.2.3. Niveles y controles de un 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 27.000
  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 normas ISO/IEC 27.000
1.5. Diseño e implantación de un sistema general de seguridad de información
  1.5.1. Fases de implantación de un sistema general de seguridad de la Información
  1.5.2. 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

Módulo 2. Aspectos Organizativos en Política 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. BIA- Analizando el impacto
- 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. Cumplimiento de los requisitos legales
- 2.9.2. Revisiones en la seguridad de la información

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

Módulo 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. Clasificación y flujo de información
- 3.3.2. 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. Implementación de medidas de salvaguarda
- 3.5.2. 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

Módulo 4. Implementación Práctica 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 OTP
- 4.2.2. Token USB o tarjeta inteligente PKI
- 4.2.3. La llave “Confidencial Defensa”
- 4.2.4. El RFID 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. OTP
- 4.6.3. PAP, CHAP
- 4.6.4. KERBEROS, DIAMETER, NTLM

4.7. Controles CIS para bastionado de sistemas
- 4.7.1. Controles CIS básicos
- 4.7.2. Controles CIS fundamentales
- 4.7.3. Controles CIS 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. Vulnerabilidades lógicas
- 4.10.2. Implementación de políticas de defensa

Módulo 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. Organismos CERT

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
  - 5.5.2.1. Análisis de evidencias electrónicas
  - 5.5.2.2. Recogida de evidencias electrónicas

5.6. Herramientas de Sistemas de detección y prevención de intrusiones (IDS/IPS)
- 5.6.1. *Snort*
- 5.6.2. Suricata
- 5.6.3. Solar-Winds

5.7. Herramientas centralizadoras de eventos
- 5.7.1. SIM
- 5.7.2. SEM
- 5.7.3. SIEM

5.8. Guía de seguridad CCN-STIC 817
- 5.8.1. Gestión de ciberincidentes
- 5.8.2. Métricas e Indicadores

5.9. NIST SP800 - 61
- 5.9.1. Capacidad de respuesta antes incidentes de seguridad Informática
- 5.9.2. Manejo de un incidente
- 5.9.3. Coordinación e información compartida

5.10. Norma ISO 27035
- 5.10.1. Norma ISO 27035. Principios de la gestión de incidentes
- 5.10.2. Guías para la elaboración de un plan para la gestión de incidentes
- 5.10.3. Guías de operaciones en la respuesta a incidentes

Módulo 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. Políticas de control de acceso físico
- 6.2.2. Sistemas de control físico de entrada

6.3. Vulnerabilidades de accesos físicos
- 6.3.1. Principales vulnerabilidades físicas
- 6.3.2. 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. Implementación de sistemas biométricos
- 6.6.2. Vulnerabilidades de los sistemas biométricos

6.7. Implementación de políticas en *hosts*
- 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 (EEUU)
- 6.10.3. NERC CIP - 014 - 2 (EEUU)

Módulo 7. Políticas de Comunicaciones Seguras en la Empresa

7.1. Gestión de la seguridad en las redes
- 7.1.1. Control y monitorización de red
- 7.1.2. Segregación de redes
- 7.1.3. Sistemas de seguridad en redes

7.2. Protocolos seguros de comunicación
- 7.2.1. Modelo TCP/IP
- 7.2.2. Protocolo IPSEC
- 7.2.3. Protocolo TLS

7.3. Protocolo TLS 1.3
- 7.3.1. Fases de un proceso TLS1.3
- 7.3.2. Protocolo *Handshake*
- 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. *Cipher - suites*
- 7.4.3. Algoritmos criptográficos permitidos para TLS 1.3

7.5. Funciones Digest
- 7.5.1. MD6
- 7.5.2. SHA

7.6. PKI. Infraestructura de clave pública
- 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. SSH. *Secure Shell*
- 7.8.1. SSH. Cápsula segura
- 7.8.2. Funcionamiento de SSH
- 7.8.3. Herramientas SSH

7.9. Auditoria de sistemas criptográficos
- 7.9.1. Pruebas de integridad
- 7.9.2. Testeo sistema criptográfico

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

Módulo 8. Implementación Práctica de Políticas de Seguridad Ante Ataques

8.1. *System Hacking*
- 8.1.1. Riesgos y vulnerabilidades
- 8.1.2. Contramedidas

8.2. DoS en servicios
- 8.2.1. Riesgos y vulnerabilidades
- 8.2.2. Contramedidas

8.3. *Session Hijacking*
- 8.3.1. El proceso de *Hijacking*
- 8.3.2. Contramedidas a *Hijacking*

8.4. Evasión de IDS, *Firewalls and Honeypots*
- 8.4.1. Técnicas de evasión
- 8.4.2. Implementación de contramedidas

8.5. *Hacking Web Servers*
- 8.5.1. Ataques a servidores webs
- 8.5.2. Implementación de medidas de defensa

8.6. *Hacking Web Applications*
- 8.6.1. Ataques a aplicaciones web
- 8.6.2. Implementación de medidas de defensa

8.7. *Hacking Wireless Networks*
- 8.7.1. Vulnerabilidades redes wifi
- 8.7.2. Implementación de medidas de defensa

8.8. *Hacking Mobile Platforms*
- 8.8.1. Vulnerabilidades de plataformas móviles
- 8.8.2. Implementación de contramedidas

8.9. *Ransomware*
- 8.9.1. Vulnerabilidades causantes del *Ransomware*
- 8.9.2. Implementación de contramedidas

8.10. Ingeniera social
- 8.10.1. Tipos de ingeniería social
- 8.10.2. Contramedidas para la ingeniería social

Módulo 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 Linux

9.3. Protocolo SNMP. *Simple Network Management Protocol*
- 9.3.1. Protocolo SNMP
- 9.3.2. Funcionamiento de SNMP
- 9.3.3. Herramientas SNMP

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

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

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

9.7. Cacti. Sistema de monitorización de redes
- 9.7.1. Cacti
- 9.7.2. Funcionamiento de Cacti
- 9.7.3. Instalación de Cacti

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

9.9. *SolarWinds*. Sistema de monitorización de redes
- 9.9.1. SolarWinds
- 9.9.2. Funcionamiento de SolarWinds
- 9.9.3. Instalación de SolarWinds

9.10. Normativa sobre monitorización
- 9.10.1. Controles CIS sobre auditoria y registro
- 9.10.2. NIST 800 - 123 (EEUU)

Módulo 10. Política de Recuperación Práctica de Desastres de Seguridad

10.1. DRP. Plan de recuperación de desastres
- 10.1.1. Objetivo de un DRP
- 10.1.2. Beneficios de un DRP
- 10.1.3. Consecuencias de ausencia de un DRP y no actualizado

10.2. Guía para definir un DRP (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's que se requieren
- 10.2.7. Realización de un Plan de formación, concienciación y comunicación

10.3. Alcance y objetivos de un DRP (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 DRP (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 BCP (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 (AP)
- 10.7.2. Tiempos de recuperación ideales (TRI)
- 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 BCP
- 10.10.1. Objetivos
- 10.10.2. Términos y definiciones
- 10.10.3. Operación

Tendrás acceso a recursos especializados sobre técnicas de Session Hijacking, con material detallado y actualizado"

04

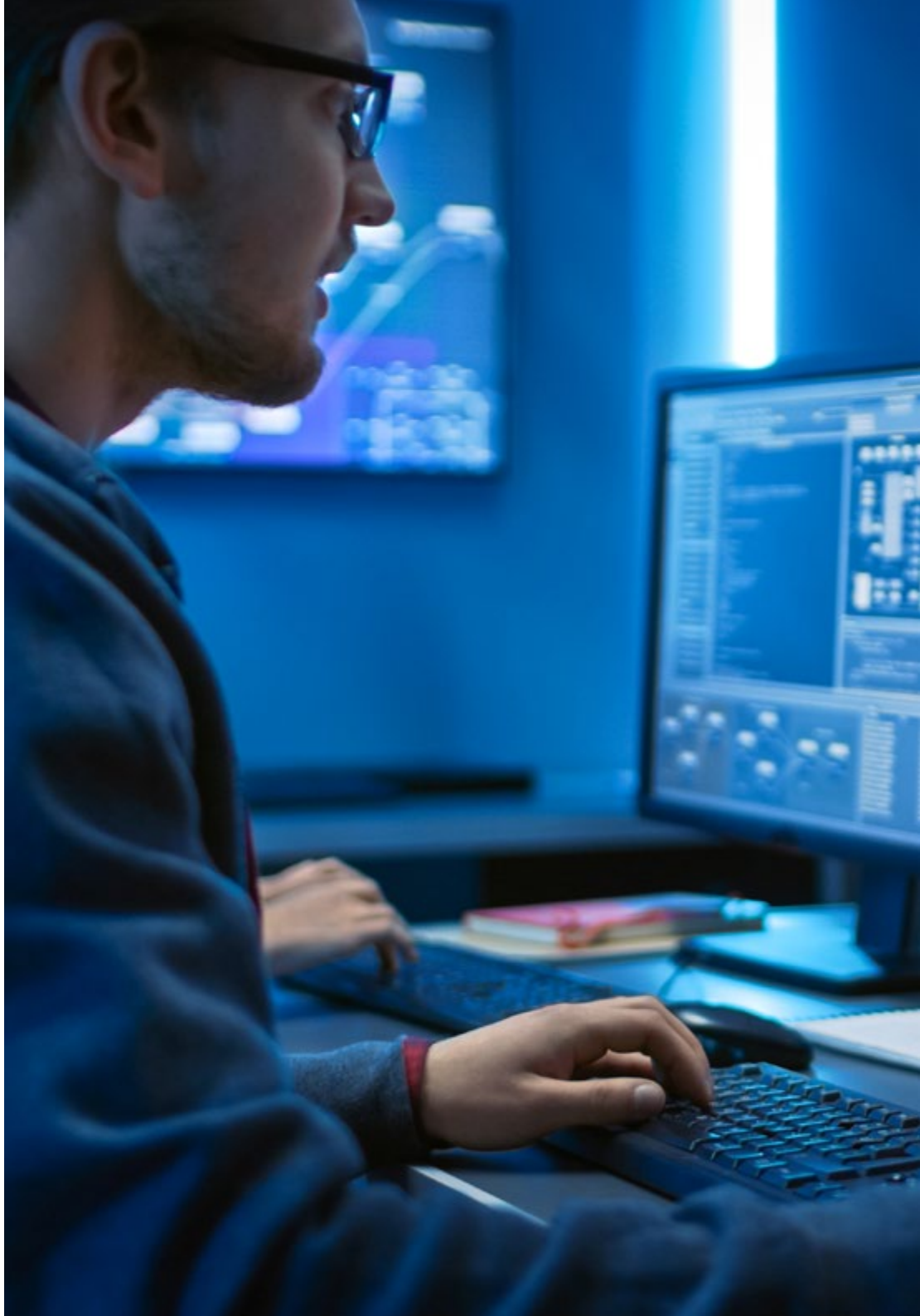
Objetivos docentes

Este Máster Título Propio tiene como finalidad capacitar a los profesionales en la Gestión avanzada de la seguridad de la información, enfocándose en la implementación de estándares internacionales y la protección de infraestructuras digitales. A lo largo del programa universitario, se desarrollarán competencias esenciales para identificar, prevenir y responder eficazmente ante amenazas, garantizando la integridad y disponibilidad de los sistemas. A su vez, el alumnado aplicará estrategias de protección robustas, gestionar incidentes de seguridad y optimizar la resiliencia organizacional, contribuyendo así a la continuidad operativa y la protección integral de los activos digitales dentro de sus entornos empresariales.

¿Quieres ser un experto en la protección de infraestructuras digitales? Este programa universitario te brindará las herramientas necesarias para innovar en la defensa de sistemas"

Objetivos generales

- Desarrollar competencias en la implementación de un Sistema de Gestión de Seguridad de la Información eficaz
- Fortalecer la capacidad de diseñar políticas organizativas en seguridad de la información adaptadas a contextos específicos
- Capacitar en el análisis y desarrollo de políticas de seguridad ante amenazas en sistemas informáticos
- Adquirir habilidades en la implementación práctica de políticas de seguridad para proteger software y hardware empresarial
- Brindar herramientas para la gestión de incidencias de seguridad y su resolución efectiva
- Preparar para la implementación de políticas de seguridad física y ambiental en entornos corporativos
- Proporcionar conocimientos sobre el diseño y gestión de comunicaciones seguras dentro de la empresa
- Desarrollar competencias en la recuperación de desastres de seguridad mediante políticas eficaces y procedimientos prácticos



Objetivos específicos

Módulo 1. Sistema de Gestión de Seguridad de Información (SGSI)

- Desarrollar la capacidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a los estándares internacionales
- Analizar y aplicar las normas ISO/IEC 27.000 para la certificación y acreditación en seguridad de la información
- Identificar y gestionar los riesgos, amenazas y activos en la planificación de un sistema de seguridad de la información
- Establecer políticas de seguridad eficaces para la gestión y categorización de incidentes en sistemas de información

Módulo 2. Aspectos Organizativos en Política de Seguridad de la Información

- Desarrollar habilidades para asignar responsabilidades y garantizar la segregación de tareas en la gestión de la seguridad de la información
- Adquirir competencias en la clasificación de activos, manejo de soportes de almacenamiento y gestión de la seguridad en los procesos de negocio
- Implementar políticas de seguridad vinculadas a los recursos humanos y gestionar la seguridad con proveedores y en la cadena de suministro
- Aplicar directrices de seguridad en la dirección de la empresa y asegurar la continuidad de la información mediante planes de recuperación y redundancias

Módulo 3. Políticas de Seguridad para el Análisis de Amenazas en Sistemas Informáticos

- Gestionar riesgos e implementar metodologías para identificar y analizar amenazas en sistemas informáticos
- Clasificar riesgos, calcular probabilidades de amenazas y gestionar el riesgo residual en seguridad de la información
- Aplicar enfoques prácticos para el control de amenazas utilizando catálogos de medidas de control
- Implementar procedimientos continuos de gestión de riesgos con métricas de seguridad y normas ISO 27005s

Módulo 4. Implementación Práctica de Políticas de Seguridad en Software y Hardware

- Implementar políticas de seguridad en software y hardware, enfocándose en identificación, autorización y medidas técnicas
- Aplicar tecnologías de acceso seguro, como identificadores OTP, tarjetas inteligentes y sistemas RFID activos
- Gestionar el control de accesos a sistemas y aplicaciones mediante la segregación de roles y el establecimiento de políticas de contraseñas
- Aplicar prácticas de seguridad operativa, incluyendo protección contra código malicioso y gestión de vulnerabilidades técnicas

Módulo 5. Políticas de Gestión de Incidencias de Seguridad

- Gestionar incidencias de seguridad de la información, asegurando la implementación de procedimientos y la notificación adecuada de eventos
- Implementar y administrar sistemas de detección y prevención de intrusiones (IDS/IPS), optimizando la ubicación y el funcionamiento de los mismos
- Desarrollar procedimientos de respuesta ante incidentes de seguridad, incluyendo recolección de información y verificación de intrusiones
- Aplicar análisis forense en la gestión de incidencias, enfocándose en la recogida y análisis de evidencias electrónicas para la resolución de incidentes

Módulo 6. Implementación de Políticas de Seguridad Física y Ambiental en la Empresa

- Implementar políticas de seguridad física en áreas clave de la empresa, como oficinas y recursos, estableciendo perímetros de seguridad adecuados
- Establecer controles de acceso físico, utilizando sistemas de seguridad para regular entradas y salidas en las instalaciones
- Gestionar riesgos asociados a sistemas biométricos, evaluando vulnerabilidades y aplicando medidas de protección
- Adoptar políticas de seguridad para equipos informáticos, asegurando su correcta instalación, protección y manejo, así como su disposición fuera de las dependencias

Módulo 7. Políticas de Comunicaciones Seguras en la Empresa

- Establecer controles para la gestión de la seguridad en redes, incluyendo la monitorización y segregación de las mismas
- Aplicar protocolos seguros de comunicación, como TCP/IP, IPSEC y TLS, para proteger la integridad de los datos en tránsito
- Implementar el protocolo TLS 1.3, asegurando su correcta ejecución a través de las fases del proceso y las diferencias clave con su versión anterior
- Utilizar algoritmos criptográficos adecuados, como Cipher - suites y funciones Digest, para garantizar la seguridad de las comunicaciones

Módulo 8. Implementación Práctica de Políticas de Seguridad Ante Ataques

- Identificar riesgos y vulnerabilidades en ataques de *System Hacking* y aplicar contramedidas adecuadas
- Gestionar los riesgos asociados a los ataques de DoS y poner en marcha estrategias de protección eficaces
- Analizar el proceso de *Session Hijacking*, implementando contramedidas para mitigar este tipo de ataque
- Desarrollar técnicas para la evasión de IDS, *firewalls* y *honeypots*, implementando contramedidas adecuadas para su protección

Módulo 9. Herramientas de Monitorización en Políticas de Seguridad de los Sistemas de Información

- Establecer políticas de monitorización de sistemas, incluyendo el uso de métricas para evaluar el rendimiento
- Implementar auditorías y registros en sistemas, adaptados a entornos Windows y Linux
- Gestionar el uso del protocolo SNMP para la monitorización de redes y su integración con herramientas especializadas
- Configurar y mantener herramientas de monitorización como Nagios, Zabbix, Cacti y Pandora para la gestión eficiente de redes

Módulo 10. Política de Recuperación Práctica de Desastres de Seguridad

- Establecer los objetivos y beneficios de un DRP, así como las consecuencias de no contar con uno actualizado
- Definir la guía para la creación de un DRP, incluyendo el alcance, los objetivos, roles y responsabilidades, además de un inventario de recursos necesarios
- Diseñar la estrategia de recuperación de desastres, considerando el presupuesto, los recursos humanos y físicos, y la tecnología requerida para su implementación
- Desarrollar un Plan de Continuidad Empresarial (BCP), identificando los procesos más críticos y estableciendo estrategias de recuperación y supervivencia

05

Salidas profesionales

Este programa universitario destaca por brindar las herramientas necesarias para que los egresados sobresalgan en el ámbito de la seguridad Informática. De este modo, los profesionales podrán acceder a roles clave como analistas de Ciberseguridad, consultores en protección de datos o responsables de gestión de riesgos, desempeñándose en empresas de tecnología, consultoras o instituciones gubernamentales. Con un enfoque práctico y actualizado, se abrirán nuevas oportunidades para gestionar y proteger infraestructuras críticas en un entorno digital cada vez más complejo. Así, se asegurará una integración exitosa en el dinámico mundo de la ciberseguridad.

Asumirás roles especializados como analista de Ciberseguridad, dominando técnicas avanzadas para identificar mitigar riesgos en entornos tecnológicos”

Perfil del egresado

El egresado contará con una comprensión profunda de los sistemas de información, capaz de identificar vulnerabilidades y desarrollar soluciones efectivas para protegerlos. Asimismo, se destacará por su capacidad para implementar protocolos de seguridad robustos y gestionar incidentes tecnológicos de manera eficiente. Además, podrá liderar proyectos complejos, colaborar con equipos multidisciplinarios y aplicar conocimientos técnicos avanzados para garantizar la integridad de los datos y la continuidad operativa. Su enfoque estará orientado a las soluciones innovadoras, con una visión estratégica para enfrentar los desafíos emergentes en el mundo digital.

Gracias a las herramientas avanzadas de este programa universitario, podrás tomar decisiones clave en la Gestión de Políticas de Seguridad en la Empresa.

- **Pensamiento creativo:** evaluar y analizar situaciones complejas para tomar decisiones informadas en la gestión de políticas de seguridad.
- **Gestión estratégica:** expresar de manera clara y concisa los riesgos y estrategias de seguridad a diferentes niveles dentro de la organización.
- **Adaptación tecnológica:** colaborar con diversos departamentos para implementar y gestionar políticas de seguridad de manera eficiente.
- **Conciencia medioambiental:** aplicar los cambios en las normativas de seguridad y en las amenazas digitales para mantener la protección de la empresa.

Después de realizar el programa universitario, podrás desempeñar tus conocimientos y habilidades en los siguientes cargos

1. **Analista de seguridad Informática:** responsable de identificar vulnerabilidades y gestionar riesgos en los sistemas de información, implementando medidas de seguridad y asegurando la protección ante amenaza
2. **Administrador de sistemas:** encargado de gestionar la infraestructura tecnológica de la empresa, asegurando el funcionamiento óptimo de los servidores y sistemas, implementando políticas de seguridad y respaldo
3. **Consultor de ciberseguridad:** dedicado en brindar asesoría a las empresas en la creación e implementación de políticas y medidas de seguridad, analizando riesgos y proponiendo soluciones adecuadas para proteger los activos digitales
4. **Jefe de seguridad de la información:** encargado de la protección de los activos informáticos, establece políticas de seguridad, gestiona equipos de trabajo y coordina la respuesta ante incidentes de seguridad
5. **Director de tecnología:** responsable de la estrategia tecnológica de la empresa, asegurando que todas las iniciativas tecnológicas sean seguras, eficientes y alineadas con los objetivos empresariales
6. **Ingeniero de redes:** dedicado al diseño, implementación y mantenimiento de las redes de comunicación de la empresa, asegurando la protección de los datos transmitidos y la correcta operación de la infraestructura tecnológica
7. **Especialista en respuesta a incidentes:** encargado de investigar y mitigar incidentes de seguridad, como brechas de datos o ataques cibernéticos, coordinando las respuestas para minimizar el impacto
8. **Arquitecto de seguridad:** responsable de diseñar y planificar infraestructuras de seguridad robustas para la protección de los sistemas informáticos, implementando soluciones de seguridad que se adapten a las necesidades específicas de la empresa
9. **Auditor de seguridad Informática:** dedicado a la realización de auditorías periódicas de los sistemas de información para identificar vulnerabilidades, asegurando que las políticas de seguridad sean cumplidas y recomendando mejoras
10. **Gestor de riesgos de TI: r**esponsable de identificar, evaluar y gestionar los riesgos tecnológicos dentro de la empresa, implementando estrategias para mitigar amenazas y asegurando la continuidad del negocio en caso de incidentes.

Te posicionarás como un referente en seguridad informática dominando la gestión de riesgos, detección de amenazas y protección de sistemas digitales”

06

Licencias de software incluidas

TECH es referencia en el mundo universitario por combinar la última tecnología con las metodologías docentes para potencial el proceso de enseñanza-aprendizaje. Para ello, ha establecido una red de alianzas que le permite tener acceso a las herramientas de software más avanzadas del mundo profesional.

Al matricularte recibirás, de forma completamente gratuita, las credenciales de uso académico de las siguientes aplicaciones de software profesional”

TECH ha establecido una red de alianzas profesionales en la que se encuentran los principales proveedores de software aplicado a las diferentes áreas profesionales. Estas alianzas permiten a TECH tener acceso al uso de centenares de aplicaciones informáticas y licencias de software para acercarlas a sus estudiantes.

Las licencias de software para uno académico permitirán a los estudiantes utilizar las aplicaciones informáticas más avanzadas en su área profesional, de modo que podrán conocerlas y aprender su dominio sin tener que incurrir en costes. TECH se hará cargo del procedimiento de contratación para que los alumnos puedan utilizarlas de modo ilimitado durante el tiempo que estén estudiando el programa de Máster de Formación Permanente en Gestión de Políticas de Ciberseguridad en la Empresa, y además lo podrán hacer de forma completamente gratuita.

TECH te dará acceso gratuito al uso de las siguientes aplicaciones de software:

Google Career Launchpad

Google Career Launchpad es una solución para desarrollar habilidades digitales en tecnología y análisis de datos. Con un valor estimado de **5.000 dólares**, se incluye de forma **gratuita** en el programa universitario de TECH, brindando acceso a laboratorios interactivos y certificaciones reconocidas en el sector.

Esta plataforma combina capacitación técnica con casos prácticos, usando tecnologías como BigQuery y Google AI. Ofrece entornos simulados para experimentar con datos reales, junto a una red de expertos para orientación personalizada.

Funcionalidades destacadas:

- **Cursos especializados:** contenido actualizado en cloud computing, machine learning y análisis de datos
- **Laboratorios en vivo:** prácticas con herramientas reales de Google Cloud sin configuración adicional
- **Certificaciones integradas:** preparación para exámenes oficiales con validez internacional
- **Mentorías profesionales:** sesiones con expertos de Google y partners tecnológicos
- **Proyectos colaborativos:** retos basados en problemas reales de empresas líderes

En conclusión, **Google Career Launchpad** conecta a los usuarios con las últimas tecnologías del mercado, facilitando su inserción en áreas como inteligencia artificial y ciencia de datos con credenciales respaldadas por la industria.

Gracias a TECH podrás utilizar gratuitamente las mejores aplicaciones de software de tu área profesional”

07

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.

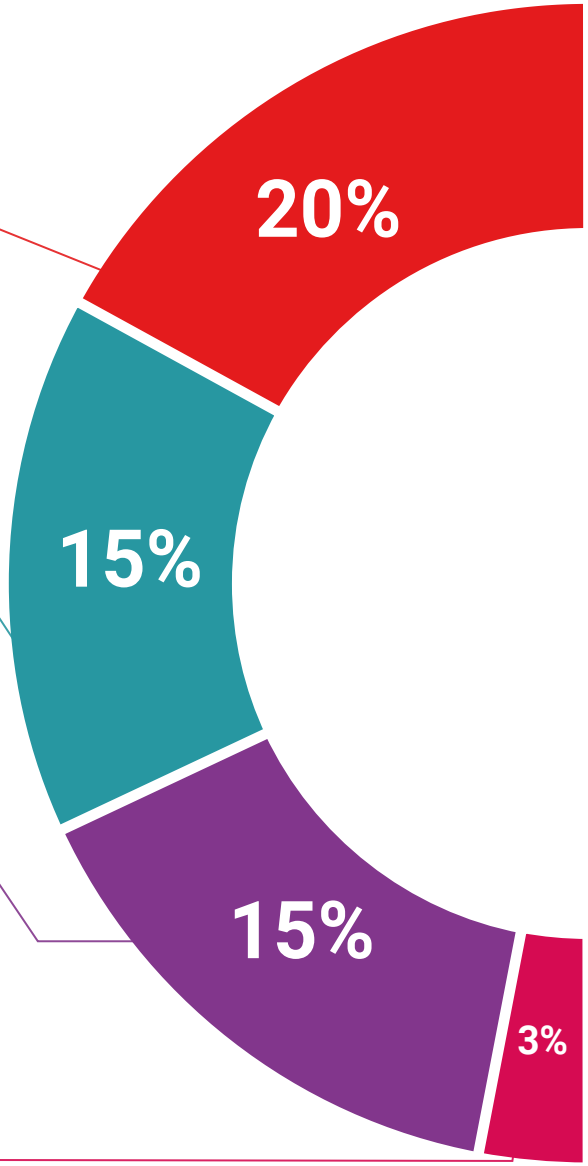
Resúmenes interactivos

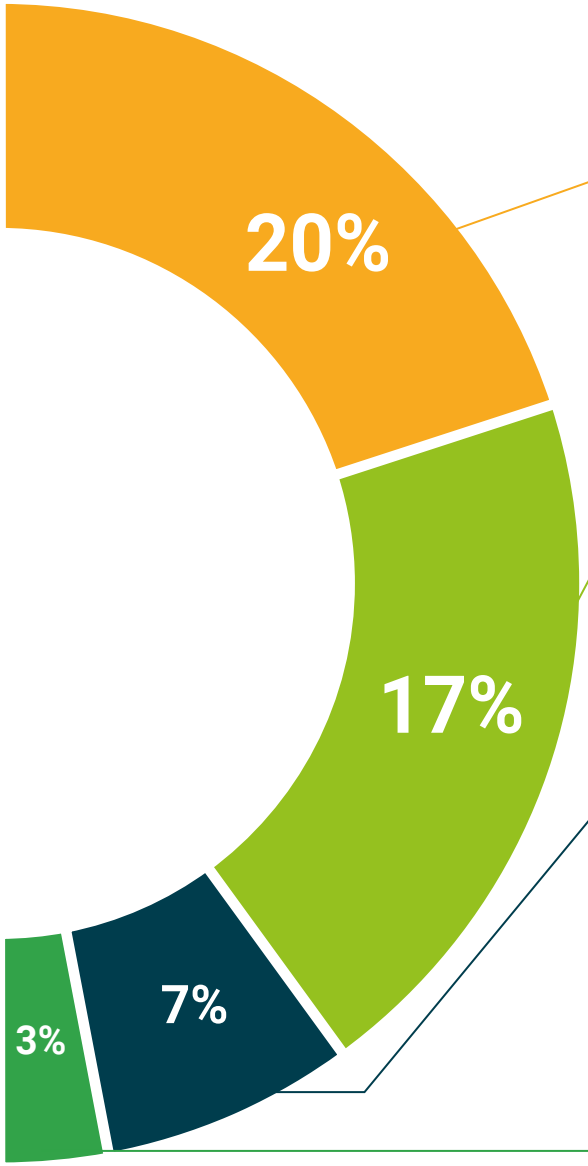
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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.

07

Cuadro docente

El equipo docente seleccionado por TECH se distingue por su sólida trayectoria en la gestión de servicios informáticos, con un enfoque preciso en la seguridad digital y la implementación eficaz de protocolos. Esta experiencia, aplicada directamente a cada módulo, transformará la capacitación en una experiencia práctica y útil desde el primer día. Gracias a esta metodología, el egresado no solo interioriza conceptos clave, sino que también los aplica en contextos reales, potenciando sus competencias incluso antes de finalizar el programa universitario. Así, se garantizará una preparación alineada con las exigencias actuales del entorno tecnológico y empresarial.

Tendrás el apoyo y ayuda de un grupo docente comprometido al máximo en tu mejora profesional hacia la Gestión de Políticas de Ciberseguridad"

Dirección

Dña. Fernández Sapena, Sonia

- Formadora de Seguridad Informática y Hacking Ético en el Centro de Referencia Nacional en Informática y Telecomunicaciones
- 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. 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

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. 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. 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

Aprovecha la oportunidad para conocer los últimos avances en esta materia para aplicarla a tu práctica diaria”

09

Titulación

El Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Máster Propio expedido por TECH Global University.

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

Este programa te permitirá obtener el título propio de **Máster en Gestión de Políticas de Ciberseguridad en la Empresa** avalado por **TECH Global University**, la mayor Universidad digital del mundo.

TECH Global University, es una Universidad Oficial Europea reconocida públicamente por el Gobierno de Andorra (***boletín oficial***). Andorra forma parte del Espacio Europeo de Educación Superior (EEES) desde 2003. El EEES es una iniciativa promovida por la Unión Europea que tiene como objetivo organizar el marco formativo internacional y armonizar los sistemas de educación superior de los países miembros de este espacio. El proyecto promueve unos valores comunes, la implementación de herramientas conjuntas y fortaleciendo sus mecanismos de garantía de calidad para potenciar la colaboración y movilidad entre estudiantes, investigadores y académicos.

Este título propio de **TECH Global University**, es un programa europeo de formación continua y actualización profesional que garantiza la adquisición de las competencias en su área de conocimiento, confiriendo un alto valor curricular al estudiante que supere el programa.

Título: **Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa**

Modalidad: **online**

Duración: **12 meses**

Acreditación: **60 ECTS**

tech global university

D/Dña _____, con documento de identificación _____ ha superado con éxito y obtenido el título de:

Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa

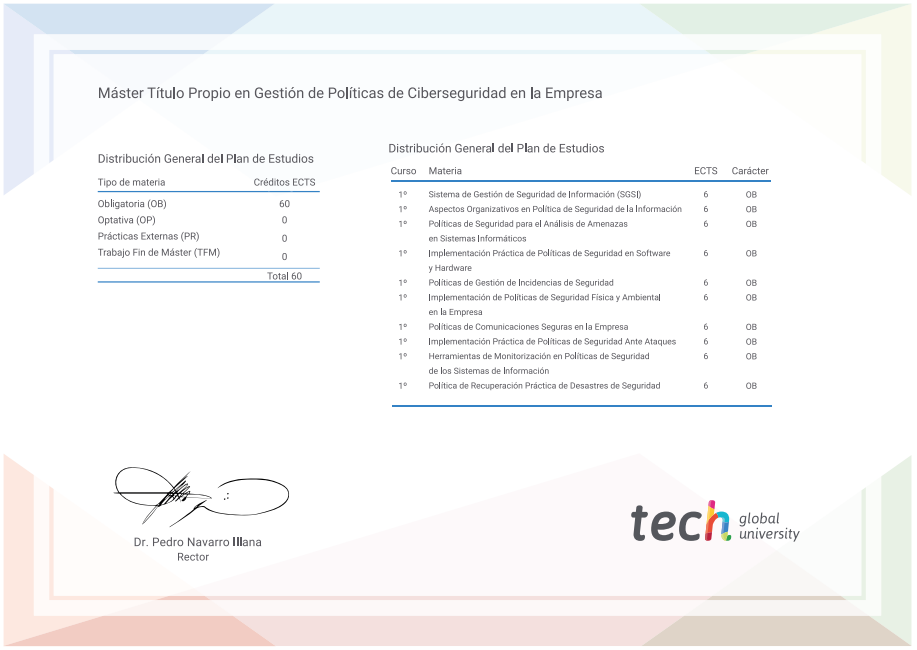
Se trata de un título propio de 1.800 horas de duración equivalente a 60 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH Global University es una universidad reconocida oficialmente por el Gobierno de Andorra el 31 de enero de 2024, que pertenece al Espacio Europeo de Educación Superior (EEES).

En Andorra la Vella, a 28 de febrero de 2024

Dr. Pedro Navarro Illana
Rector

código único TECH: AFWOR23S techtitute.com/titulos



Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa

Distribución General del Plan de Estudios

Tipo de materia	Créditos ECTS
Obligatoria (OB)	60
Optativa (OP)	0
Prácticas Externas (PR)	0
Trabajo Fin de Máster (TFM)	0
	Total 60

Distribución General del Plan de Estudios

Curso	Materia	ECTS	Carácter
1º	Sistema de Gestión de Seguridad de Información (SGSI)	6	OB
1º	Aspectos Organizativos en Política de Seguridad de la Información	6	OB
1º	Políticas de Seguridad para el Análisis de Amenazas en Sistemas Informáticos	6	OB
1º	Implementación Práctica de Políticas de Seguridad en Software y Hardware	6	OB
1º	Políticas de Gestión de Incidencias de Seguridad	6	OB
1º	Implementación de Políticas de Seguridad Física y Ambiental en la Empresa	6	OB
1º	Políticas de Comunicaciones Seguras en la Empresa	6	OB
1º	Implementación Práctica de Políticas de Seguridad Ante Ataques	6	OB
1º	Herramientas de Monitorización en Políticas de Seguridad de los Sistemas de Información	6	OB
1º	Política de Recuperación Práctica de Desastres de Seguridad	6	OB

Dr. Pedro Navarro Illana
Rector

tech global university

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

tech global university

Máster Titulo Propio

Gestión de Políticas de Ciberseguridad en la Empresa

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Global University**
- Acreditación: **60 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Máster Titulo Propio

Gestión de Políticas de Ciberseguridad en la Empresa

tech global university