# Máster Título Propio

## Gestión de Políticas de Ciberseguridad en la Empresa

MGPCE



tech universidad tecnológica



tech universidad tecnológica

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

Idioma: **Español**

Modalidad: **Online**

Duración: **12 meses**

Titulación: **TECH Universidad Tecnológica**

Horas lectivas: **1.500 h.**

Dirigido a: **Graduados, Diplomados y Licenciados universitarios que hayan realizado previamente cualquiera de las titulaciones del campo de las Ciencias Sociales y Jurídicas, Administrativas y Empresariales.**

Acceso web: **www.techtitute.com/escuela-de-negocios/master/master-gestion-politicas-ciberseguridad-empresa**

# Índice


01 Bienvenida — pág. 4

02 ¿Por qué estudiar en TECH? — pág. 6

03 ¿Por qué nuestro programa? — pág. 10

04 Objetivos — pág. 14

05 Competencias — pág. 20

06 Estructura y contenido — pág. 26

07 Metodología — pág. 38

08 Perfil de nuestros alumnos — pág. 46

09 Dirección del curso — pág. 50

10 Impacto para tu carrera — pág. 56

11 Beneficios para tu empresa — pág. 60

12 Titulación — pág. 64

02

# ¿Por qué estudiar en TECH?

TECH es la mayor escuela de negocio 100% online del mundo. Se trata de una Escuela de Negocios de élite, con un modelo de máxima exigencia académica. Un centro de alto rendimiento internacional y de entrenamiento intensivo en habilidades directivas.





*TECH es una universidad de vanguardia tecnológica, que pone todos sus recursos al alcance del alumno para ayudarlo a alcanzar el éxito empresarial”*

## En TECH Universidad Tecnológica



### Innovación

La universidad ofrece un modelo de aprendizaje en línea que combina la última tecnología educativa con el máximo rigor pedagógico. Un método único con el mayor reconocimiento internacional que aportará las claves para que el alumno pueda desarrollarse en un mundo en constante cambio, donde la innovación debe ser la apuesta esencial de todo empresario.

*"Caso de Éxito Microsoft Europa"* por incorporar en los programas un novedoso sistema de multivídeo interactivo.



### Máxima exigencia

El criterio de admisión de TECH no es económico. No se necesita realizar una gran inversión para estudiar en esta universidad. Eso sí, para titularse en TECH, se podrán a prueba los límites de inteligencia y capacidad del alumno. El listón académico de esta institución es muy alto...

**95%** | **de los alumnos de TECH finaliza sus estudios con éxito**



### Networking

En TECH participan profesionales de todos los países del mundo, de tal manera que el alumno podrá crear una gran red de contactos útil para su futuro.

**+100.000** directivos capacitados cada año

**+200** nacionalidades distintas



### Empowerment

El alumno crecerá de la mano de las mejores empresas y de profesionales de gran prestigio e influencia. TECH ha desarrollado alianzas estratégicas y una valiosa red de contactos con los principales actores económicos de los 7 continentes.

**+500** | **acuerdos de colaboración con las mejores empresas**



### Talento

Este programa es una propuesta única para sacar a la luz el talento del estudiante en el ámbito empresarial. Una oportunidad con la que podrá dar a conocer sus inquietudes y su visión de negocio.

TECH ayuda al alumno a enseñar al mundo su talento al finalizar este programa.



### Contexto Multicultural

Estudiando en TECH el alumno podrá disfrutar de una experiencia única. Estudiará en un contexto multicultural. En un programa con visión global, gracias al cual podrá conocer la forma de trabajar en diferentes lugares del mundo, recopilando la información más novedosa y que mejor se adapta a su idea de negocio.

Los alumnos de TECH provienen de más de 200 nacionalidades.



## Aprende con los mejores

El equipo docente de TECH explica en las aulas lo que le ha llevado al éxito en sus empresas, trabajando desde un contexto real, vivo y dinámico. Docentes que se implican al máximo para ofrecer una especialización de calidad que permita al alumno avanzar en su carrera y lograr destacar en el ámbito empresarial.

Profesores de 20 nacionalidades diferentes.

*En TECH tendrás acceso a los análisis de casos más rigurosos y actualizados del panorama académico"*



**TECH busca la excelencia y, para ello, cuenta con una serie de características que hacen de esta una universidad única:**

## Análisis

En TECH se explora el lado crítico del alumno, su capacidad de cuestionarse las cosas, sus competencias en resolución de problemas y sus habilidades interpersonales.

## Excelencia académica

En TECH se pone al alcance del alumno la mejor metodología de aprendizaje online. La universidad combina el método *Relearning* (metodología de aprendizaje de posgrado con mejor valoración internacional) con el Estudio de Caso. Tradición y vanguardia en un difícil equilibrio, y en el contexto del más exigente itinerario académico.

## Economía de escala

TECH es la universidad online más grande del mundo. Tiene un portfolio de más de 10.000 posgrados universitarios. Y en la nueva economía, **volumen + tecnología = precio disruptivo**. De esta manera, se asegura de que estudiar no resulte tan costoso como en otra universidad.

03

# ¿Por qué nuestro programa?

Realizar el programa de TECH supone multiplicar las posibilidades de alcanzar el éxito profesional en el ámbito de la alta dirección empresarial.

Es todo un reto que implica esfuerzo y dedicación, pero que abre las puertas a un futuro prometedor. El alumno aprenderá de la mano del mejor equipo docente y con la metodología educativa más flexible y novedosa.





*Contamos con el más prestigioso cuadro docente y el temario más completo del mercado, lo que nos permite ofrecerte una capacitación de alto nivel académico"*

**Este programa aportará multitud de ventajas laborales y personales, entre ellas las siguientes:**

01

## Dar un impulso definitivo a la carrera del alumno

Estudiando en TECH el alumno podrá tomar las riendas de su futuro y desarrollar todo su potencial. Con la realización de este programa adquirirá las competencias necesarias para lograr un cambio positivo en su carrera en poco tiempo.

*El 70% de los participantes de esta especialización logra un cambio positivo en su carrera en menos de 2 años.*

02

## Desarrollar una visión estratégica y global de la empresa

TECH ofrece una profunda visión de dirección general para entender cómo afecta cada decisión a las distintas áreas funcionales de la empresa.

*Nuestra visión global de la empresa mejorará tu visión estratégica.*

03

## Consolidar al alumno en la alta gestión empresarial

Estudiar en TECH supone abrir las puertas de hacia panorama profesional de gran envergadura para que el alumno se posicione como directivo de alto nivel, con una amplia visión del entorno internacional.

*Trabajarás más de 100 casos reales de alta dirección.*

04

## Asumir nuevas responsabilidades

Durante el programa se muestran las últimas tendencias, avances y estrategias, para que el alumno pueda llevar a cabo su labor profesional en un entorno cambiante.

*El 45% de los alumnos consigue ascender en su puesto de trabajo por promoción interna.*

05

### Acceso a una potente red de contactos

TECH interrelaciona a sus alumnos para maximizar las oportunidades. Estudiantes con las mismas inquietudes y ganas de crecer. Así, se podrán compartir socios, clientes o proveedores.

*Encontrarás una red de contactos imprescindible para tu desarrollo profesional.*

06

### Desarrollar proyectos de empresa de una forma rigurosa

El alumno obtendrá una profunda visión estratégica que le ayudará a desarrollar su propio proyecto, teniendo en cuenta las diferentes áreas de la empresa.

*El 20% de nuestros alumnos desarrolla su propia idea de negocio.*

07

### Mejorar *soft skills* y habilidades directivas

TECH ayuda al estudiante a aplicar y desarrollar los conocimientos adquiridos y mejorar en sus habilidades interpersonales para ser un líder que marque la diferencia.

*Mejora tus habilidades de comunicación y liderazgo y da un impulso a tu profesión.*

08

### Formar parte de una comunidad exclusiva

El alumno formará parte de una comunidad de directivos de élite, grandes empresas, instituciones de renombre y profesores cualificados procedentes de las universidades más prestigiosas del mundo: la comunidad TECH Universidad Tecnológica.

*Te damos la oportunidad de especializarte con un equipo de profesores de reputación internacional.*

04

# Objetivos

Siendo la ciberseguridad un aspecto crucial en el desarrollo de cualquier empresa moderna, el objetivo del presente programa no podía ser otro sino el de ofrecer la mejor capacitación posible en materia de Gestión de Políticas de Ciberseguridad. Para ello, el grupo de docentes expertos en informática, ha recopilado un material didáctico exhaustivo y focalizado plenamente en la mejora de las habilidades, competencias y capacidades del directivo.





*Lidera la seguridad cibernética de tu organización, conociendo los entresijos de las políticas más efectivas en materia de ciberseguridad"*

## TECH hace suyos los objetivos de sus alumnos. Trabajan conjuntamente para conseguirlos.

El **Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa** capacitará al alumno para:

01 Profundizar en los conceptos clave de la seguridad de la información

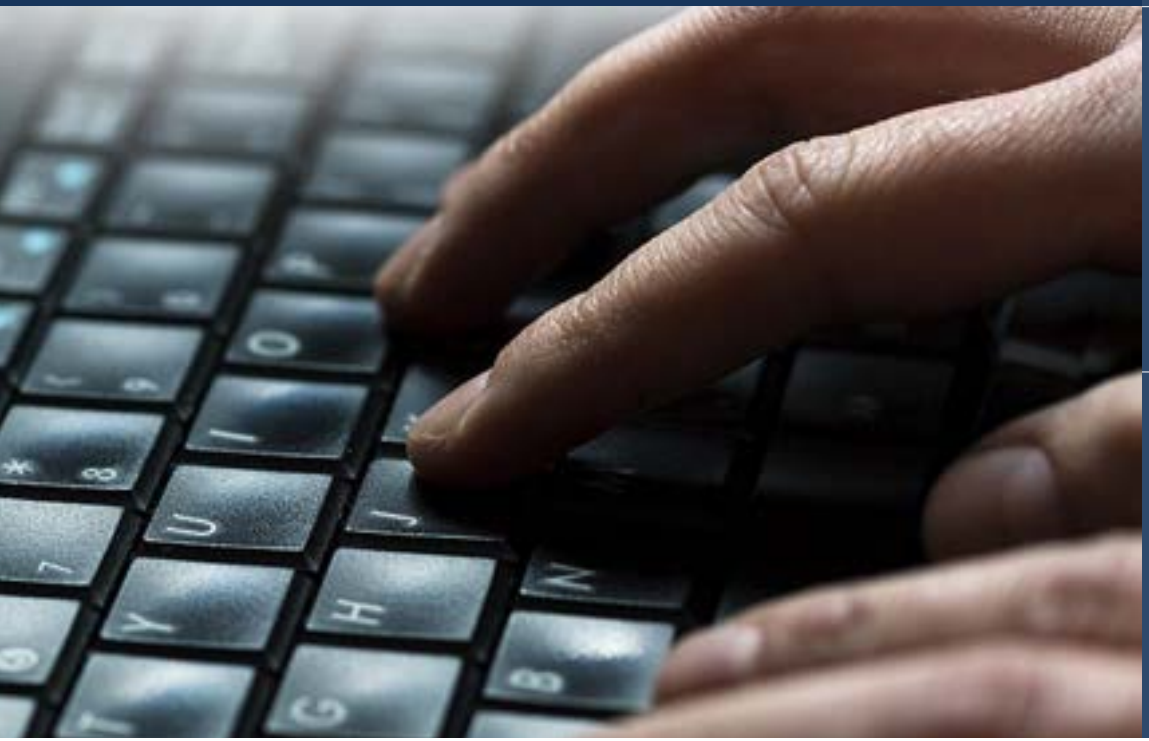
02 Analizar las normativas y estándares aplicables en la actualidad a los SGSI

03 Implementar un SGSI en la empresa

04 Determinar qué departamentos debe abarcar la implementación del sistema de gestión de seguridad



05 Desarrollar las medidas necesarias para garantizar buenas prácticas en materia de seguridad de la información



06 Determinar qué es la autenticación e identificación

07 Analizar los distintos métodos de autenticación que existen y su implementación práctica

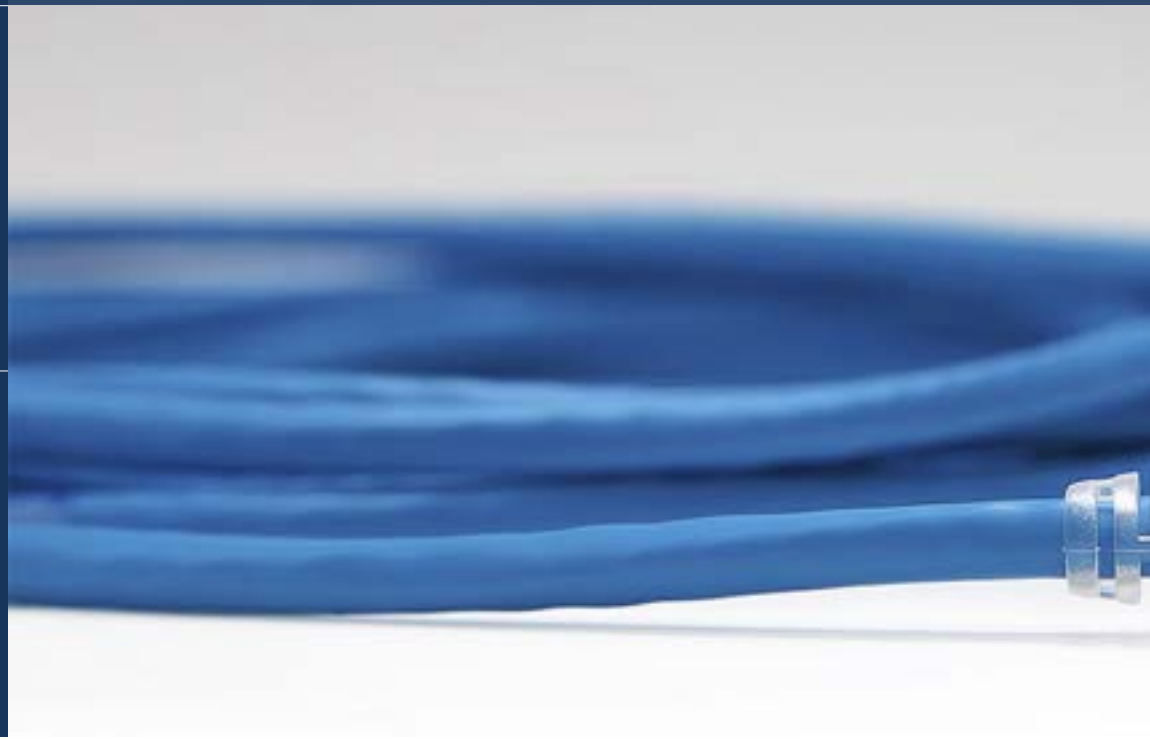
08 Implementar la política de control de accesos correcta al software y sistemas

09 Desarrollar conocimiento especializado sobre cómo gestionar incidencias causadas por eventos de seguridad informática

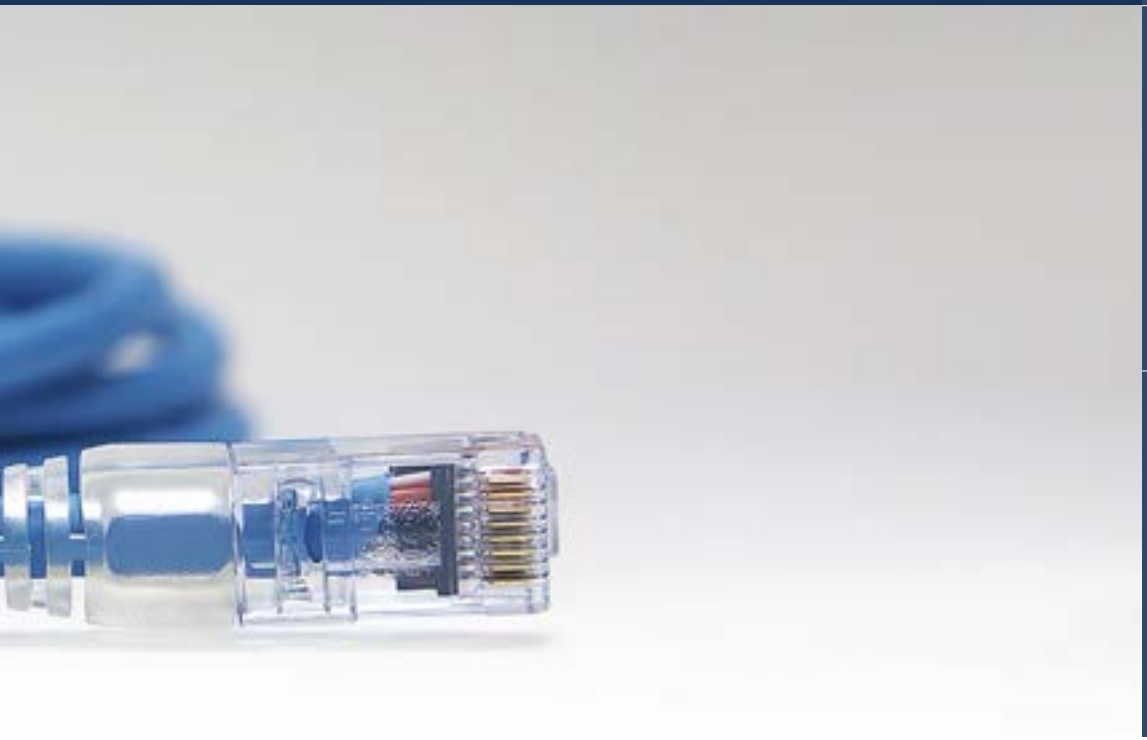
10 Analizar el término de área segura y perímetro seguro

11 Analizar los distintos algoritmos de cifrado utilizados en redes de comunicaciones

12 Determinar los distintos ataques reales a nuestro sistema de información



13 Evaluar las distintas políticas de seguridad para paliar los ataques



14 Desarrollar el concepto de monitorización e implementación de métricas

15 Generar conocimiento especializado sobre el concepto de continuidad de la seguridad de la información

16 Determinar qué es la criptografía y tipos de criptografía

05

# Competencias

Para realizar una adecuada Gestión de Políticas de Ciberseguridad es imprescindible tener una gran capacidad de organización, además de poseer unos conocimientos y competencias superiores en materia informática y tecnológica. Es por ello que, a lo largo de todo este programa, el directivo no solo encontrará una guía de referencia útil para la gestión de seguridad informática, sino que también verá reforzadas sus capacidades de liderazgo y gestión administrativa.





*Perfeccionarás las competencias necesarias para destacar como un directivo experto en Políticas de Ciberseguridad, dándote ventaja para ocupar los puestos de dirección más importantes"*

01 Determinar la implicación de un SGSI en la organización interna de la entidad, así como su estado

02 Establecer las políticas de seguridad en la empresa

03 Determinar qué medidas tenemos que implementar con suministradores y mantenimientos de sistemas de información

04 Generar conocimiento especializado sobre el control de amenazas



05 Determinar las fases de la gestión preventiva de amenazas



06 Desarrollar las metodologías para el análisis de amenazas informáticas

07 Clasificar las amenazas por impacto y gravedad

08 Diseñar una metodología propia para el análisis y control preventivo de amenazas

09 Implementar una política correcta de control de accesos a redes y servicios

10 Analizar la importancia de un tratamiento correcto en materia de incidencias de seguridad

11 Compilar los distintos sistemas biométricos que existen

12 Examinar la Biometría y sistemas biométricos




13 Implementar las distintas políticas de seguridad física correctas y los sistemas de control de acceso físico en CPDs

14 Implementar una red segura



15 Examinar las vulnerabilidades de las plataformas móviles y de los IoT y cómo evitarlas

16 Establecer los tipos de Ingeniera social y aprender a mitigarlos

17 Analizar el concepto de monitorización e implementación de métricas

18 Determinar la necesidad de la continuidad de la seguridad de la información

06

# Estructura y contenido

TECH ha estructurado el presente programa en base a la metodología del *Relearning*, lo que quiere decir que el directivo no tendrá que emplear largas horas de estudio en adquirir todo el conocimiento propuesto. Los términos y conceptos claves en materia de Políticas de Ciberseguridad son dados de forma natural y reiterativa a lo largo de toda la titulación, lo que acaba resultando en un aprendizaje mucho más progresivo.





*Tendrás libertad para entrar al aula virtual las 24 horas del día, pudiendo elegir y adaptar el ritmo de estudios a tus propios intereses”*

## Plan de estudios

El Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa de TECH Universidad Tecnológica es un programa intensivo que prepara al alumno para los ámbitos más exigentes de la ciberseguridad empresarial.

El contenido del Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa está pensado para favorecer el desarrollo de las competencias directivas que permitan la toma de decisiones con un mayor rigor en entornos inciertos.

Este Máster Título Propio trata en profundidad el mundo digital, la seguridad en dicho entorno y la instauración del comercio electrónico en las empresas, y está diseñado para capacitar a profesionales que entiendan la Gestión de Políticas de Ciberseguridad en la Empresa desde una perspectiva estratégica, internacional e innovadora.

Este Máster Título Propio se desarrolla a lo largo de 12 meses y se divide en 10 módulos:

| | |
|---|---|
| **Módulo 1** | Sistema de Gestión de Seguridad de Información (SGSI) |
| **Módulo 2** | Aspectos organizativos en Política de Seguridad de la Información |
| **Módulo 3** | Políticas de Seguridad para el Análisis de Amenazas en Sistemas Informáticos |
| **Módulo 4** | Implementación Práctica de Políticas de seguridad en Software y Hardware |
| **Módulo 5** | Políticas de Gestión de Incidencias de Seguridad |
| **Módulo 6** | Implementación de Políticas de Seguridad Física y Ambiental en la Empresa |
| **Módulo 7** | Políticas de Comunicaciones Seguras en la Empresa |
| **Módulo 8** | Implementación Práctica de Políticas de Seguridad ante Ataques |
| **Módulo 9** | Herramientas de Monitorización en Políticas de Seguridad de los sistemas de información |
| **Módulo 10** | Política de Recuperación práctica de desastres de seguridad |



## ¿Dónde, cuándo y cómo se imparte?

TECH ofrece la posibilidad de desarrollar este Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa de manera totalmente online. Durante los 12 meses que dura la especialización, el alumno podrá acceder a todos los contenidos de este programa en cualquier momento, lo que le permitirá autogestionar su tiempo de estudio.

*Una experiencia educativa única, clave y decisiva para impulsar tu desarrollo profesional y dar el salto definitivo.*

## **Módulo 1.** Sistema de gestión de seguridad de información

### 1.1. Seguridad de la información. Aspectos clave
1.1.1. Seguridad de la información
1.1.1.1. 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. Diseño e implantación de un sistema general de seguridad de información
1.5.2. Fases de implantación de un sistema general de seguridad de la información
1.5.3. Plan de continuidad de negocio

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

### 1.7. Fase II: preparación
1.7.1. Contexto de la organización
1.7.2. Análisis de normativas de seguridad aplicables
1.7.3. Alcance del sistema general de seguridad de información
1.7.4. Política del sistema general de seguridad de información
1.7.5. Objetivos del sistema general de seguridad de información

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

### 1.9. Fase IV: implantación y seguimiento
1.9.1. Análisis de resultados
1.9.2. Asignación de responsabilidades
1.9.3. Temporalización del plan de acción
1.9.4. Seguimiento y auditorías

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

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

**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. Sistemas de auditoría para la localización de amenazas
3.3.2. Clasificación y flujo de información
3.3.3. Análisis de los procesos vulnerable

### 3.4. Clasificación del riesgo
3.4.1. Tipos de riesgo
3.4.2. Calculo de la probabilidad de amenaza
3.4.3. Riesgo residual

### 3.5. Tratamiento del riesgo
3.5.1. Tratamiento del riesgo
3.5.2. Implementación de medidas de salvaguarda
3.5.3. Transferir o asumir

### 3.6. Control de riesgo
3.6.1. Proceso continuo de gestión de riesgo
3.6.2. Implementación de métricas de seguridad
3.6.3. Modelo estratégico de métricas en seguridad de la información

### 3.7. Metodologías prácticas para el análisis y control de amenazas
3.7.1. Catálogo de amenazas
3.7.2. Catálogo de medidas de control
3.7.3. Catálogo de salvaguardas

### 3.8. Norma ISO 27005
3.8.1. Identificación del riesgo
3.8.2. Análisis del riesgo
3.8.3. Evaluación del riesgo

### 3.9. Matriz de riesgo, impacto y amenazas
3.9.1. Datos, sistemas y personal
3.9.2. Probabilidad de amenaza
3.9.3. Magnitud del daño

### 3.10. Diseño de fases y procesos en el análisis de amenazas
3.10.1. Identificación elementos críticos de la organización
3.10.2. Determinación de amenazas e impactos
3.10.3. Análisis del impacto y riesgo
3.10.4. Metodologías

**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. Implementación de prácticas de políticas de seguridad
4.10.2. Vulnerabilidades lógicas
4.10.3. 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. Guía de seguridad CCN-STIC 817
5.8.2. Gestión de ciberincidentes
5.8.3. 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. Controles físicos de entrada
6.2.2. Políticas de control de acceso físico
6.2.3. Sistemas de control físico de entrada

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

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

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

### 6.6. Gestión de riesgos en Biometría
6.6.1. Gestión de riesgos en Biometría
6.6.2. Implementación de sistemas Biométricos
6.6.3. Vulnerabilidades de los sistemas Biométricos

### 6.7. Implementación de políticas en *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. Funciones Digest
7.5.2. MD6
7.5.3. 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. Auditoría de sistemas criptográficos
7.9.2. Pruebas de integridad
7.9.3. Testeo sistema criptográfico

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

## **Módulo 8.** Implementación Práctica de Políticas de Seguridad ante Ataques

### 8.1. *System Hacking*
8.1.1. *System Hacking*
8.1.2. Riesgos y vulnerabilidades
8.1.3. Contramedidas

### 8.2. DoS en servicios
8.2.1. DoS en Servicios
8.2.2. Riesgos y vulnerabilidades
8.2.3. Contramedidas

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

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

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

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

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

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

### 8.9. *Ramsonware*
8.9.1. *Ramsonware*
8.9.2. Vulnerabilidades causantes del *Ramsonware*
8.9.3. Implementación de contramedidas

### 8.10. Ingeniera social
8.10.1. Ingeniería social
8.10.2. Tipos de ingeniería social
8.10.3. 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 Windows
9.2.3. 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. Monitorización de redes
9.4.2. La monitorización de red en sistemas de control
9.4.3. Herramientas de monitorización para sistemas de control

### 9.5. 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. Normativa sobre monitorización
9.10.2. Controles CIS sobre auditoria y registro
9.10.3. NIST 800-123 (EE.UU)

## **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 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

08

# Perfil de nuestros alumnos

El Máster Título Propio está dirigido a Graduados, Diplomados y Licenciados universitarios que hayan realizado previamente cualquiera de las siguientes titulaciones en el campo de las Ciencias Sociales y Jurídicas, Administrativas y Económicas.

La diversidad de participantes con diferentes perfiles académicos y procedentes de múltiples nacionalidades conforma el enfoque multidisciplinar de este programa.

También podrán realizar el Máster Título Propio los profesionales que, siendo titulados universitarios en cualquier área, cuenten con una experiencia laboral de dos años en el campo de la Gestión de Políticas de Ciberseguridad.



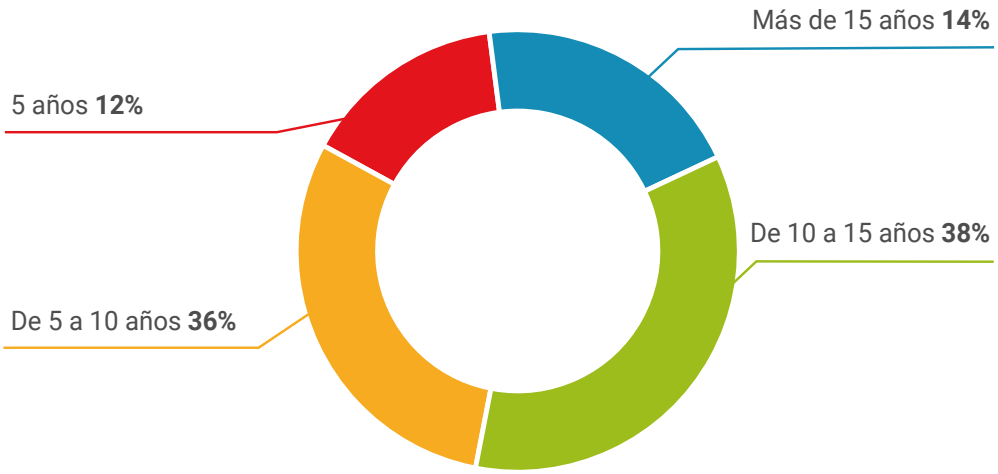


*Si buscas impulsar tu trayectoria profesional con un conocimiento de calidad, basado en la realidad más actual de la ciberseguridad, inscríbete ya en este programa"*

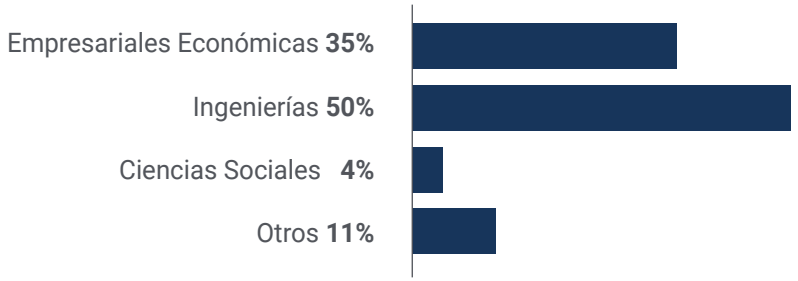
## Edad media

Entre **35** y **45** años

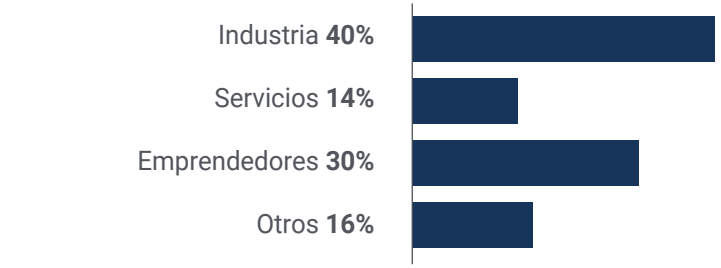
## Años de experiencia



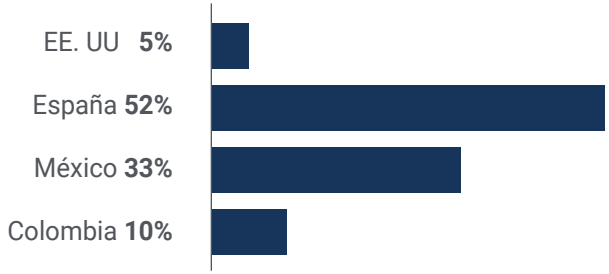

## Formación




## Perfil académico



## Distribución geográfica






# Gabriel Gutiérrez Gómez

**Responsable de Ciberseguridad**

*"Tras sufrir un ataque informático severo en nuestra organización, pusimos más énfasis en proteger nuestras bases de datos y dedicar un pequeño departamento a ello. Gracias a este programa, pude liderar ese esfuerzo, diseñando e implementando las políticas de ciberseguridad que seguimos usando hoy en día"*

09

# Dirección del curso

Para lograr la mayor calidad posible de todo el contenido didáctico, TECH ha seleccionado a un grupo de docentes expertos en las diferentes áreas que abarca la ciberseguridad. Así, el directivo tendrá acceso a un temario redactado por profesionales con amplia experiencia en la Gestión de Políticas de Ciberseguridad, que han aportado a toda la teoría su distintiva visión práctica para cada uno de los temas tratados.





*Apóyate en un cuadro docente con experiencia en la alta dirección y gestión de seguridad informática compleja, con temas dedicados al mantenimiento de sistemas de la información, análisis forense y Hijacking"*

## Dirección



### Dña. Fernández Sapena, Sonia

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

## Profesores

### D. Solana Villarias, Fabián

- Consultor de Tecnologías de la Información
- Creador y administrador de servicios de encuestas en Investigación, Planificación y Desarrollo, S.A.
- 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 de 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

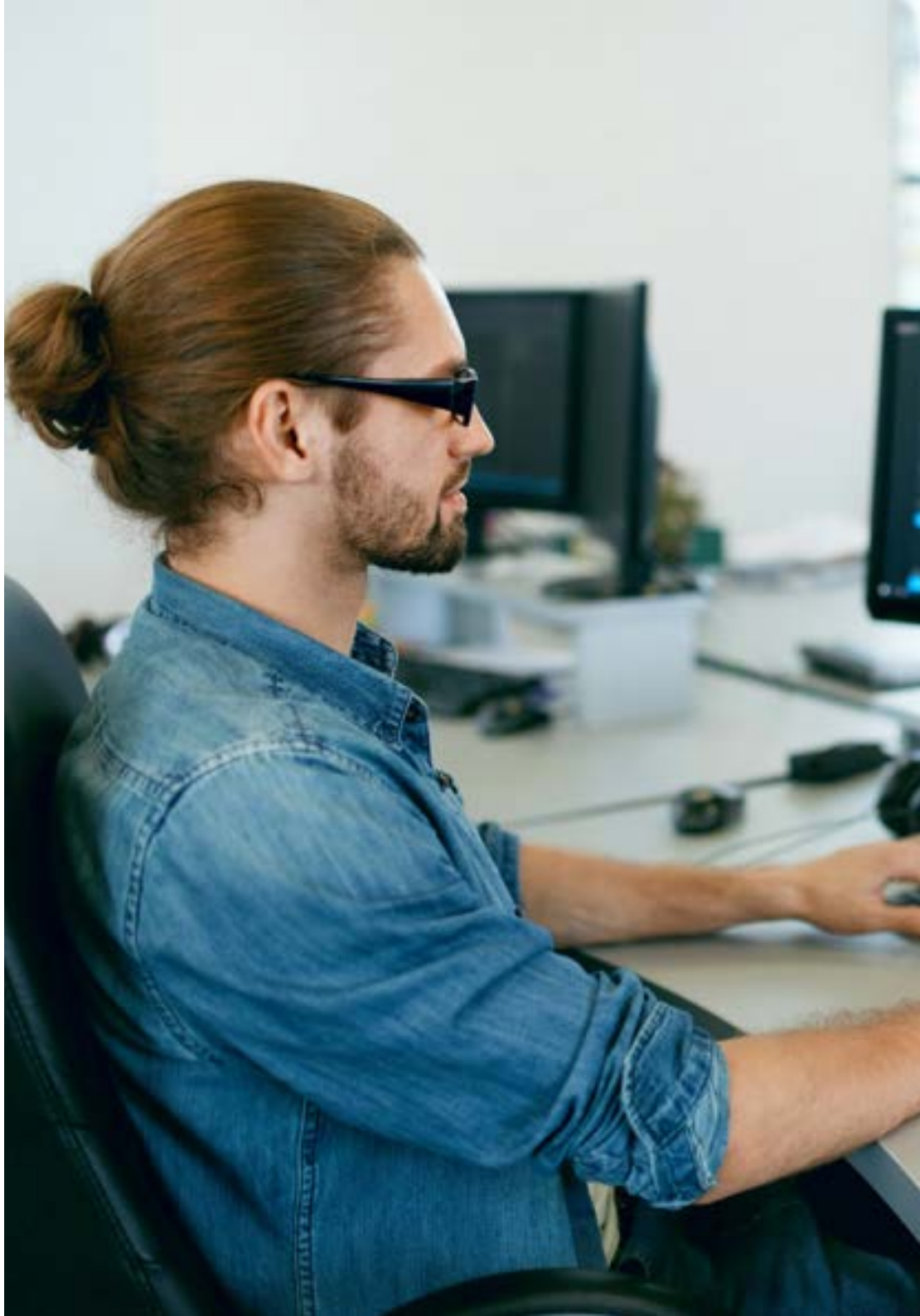
- Ingeniero informático
- Técnico en Microinformática, Redes y Seguridad en Cas-Training
- Desarrollador de servicios web, CMS, e-Commerce, UI y UX en Fersa Reparaciones
- Gestor de servicios web, contenidos, correo y DNS en Oropesia Web & Network
- Diseñador gráfico y de aplicaciones web en Xarxa Sakai Projectes
- Diplomado en Informática de Sistemas por la Universidad de Alcalá de Henares
- Master 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 seguridad (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 de Henares
- Máster para el 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 senior - Protección de Datos y Ciberseguridad. Altia
- Abogado / Asesor jurídico. Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Asesor jurídico / Pasante. Despacho de profesional: Oscar Padura
- Grado en Derecho. Universidad Pública del País Vasco
- Máster en Delegado de Protección de Datos. EIS Innovative School
- Máster Universitario en Abogacía. Universidad Pública del País Vasco
- Máster Especialista en Práctica Procesal Civil. Universidad Internacional Isabel I de Castilla
- Docente en Máster en Protección de Datos Personales, Ciberseguridad y Derecho de las TIC





*TECH ha seleccionado cuidadosamente al equipo docente de este programa para que puedas aprender de los mejores especialistas de la actualidad”*

10

# Impacto para tu carrera

TECH es consciente del esfuerzo que debe realizar el directivo para asumir una titulación de estas características, por lo que dedica especial esfuerzo a que todos los contenidos y material didáctico proporcionado cumplan los estándares de calidad más exigentes. Así, la biblioteca multimedia a la que se gana acceso sirve de un referente excepcional en el área de ciberseguridad, pudiendo incluso descargarse en su totalidad para seguir usándola una vez finalice la titulación.





*Conseguirás la proyección económica y profesional que buscas gracias al apoyo constante de un equipo docente y técnico comprometido con llevarte al cénit de la dirección en Políticas de Ciberseguridad"*

## ¿Preparado para dar el salto?
## Una excelente mejora profesional espera

El Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa de TECH es un programa intensivo que prepara al estudiante para afrontar retos y decisiones empresariales en el ámbito de la ciberseguridad. Su objetivo principal es favorecer tu crecimiento personal y profesional y ayudarle a conseguir el éxito.

Si el estudiante quiere superarse a sí mismo, conseguir un cambio positivo a nivel profesional y relacionarse con los mejores, este es su sitio.

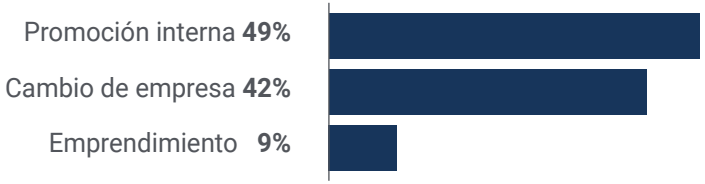
*Conseguirás la mejora laboral que persigues en menos tiempo del que imaginas gracias a la metodología pedagógica de TECH.*

*Matricúlate ya en este Máster Título Propio y no esperes más a conseguir un cambio positivo en tu entorno.*

### Momento del cambio

| Durante el programa el | Durante el primer año el | Dos años después el |
|---|---|---|
| **11%** | **63%** | **26%** |

### Tipo de cambio



## Mejora salarial

La realización de este programa supone para nuestros alumnos un incremento salarial de más del **25,22%**

| Salario previo | Incremento salarial del | Salario posterior |
|---|---|---|
| **57.900€** | **25,22%** | **72.500€** |

11

# Beneficios para tu empresa

El Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa contribuye a elevar el talento de la organización a su máximo potencial mediante la instrucción de líderes de alto nivel.

Participar en este Máster Título Propio supone una oportunidad única para acceder a una red de contactos potente en la que encontrar futuros socios profesionales, clientes o proveedores.





*Las amenazas cibernéticas suponen una de las mayores vulnerabilidades a las que están expuestas empresas de todo tipo y tamaño. Especialízate en el área con mayor proyección futura"*

**Desarrollar y retener el talento en las empresas es la mejor inversión a largo plazo.**

01

### Crecimiento del talento y del capital intelectual

El profesional aportará a la empresa nuevos conceptos, estrategias y perspectivas que pueden provocar cambios relevantes en la organización.

02

### Retención de directivos de alto potencial evitando la fuga de talentos

Este programa refuerza el vínculo de la empresa con el profesional y abre nuevas vías de crecimiento profesional dentro de la misma.

03

### Construcción de agentes de cambio

Será capaz de tomar decisiones en momentos de incertidumbre y crisis, ayudando a la organización a superar los obstáculos.

04

### Incremento de las posibilidades de expansión internacional

Gracias a este programa, la empresa entrará en contacto con los principales mercados de la economía mundial.



05

### Desarrollo de proyectos propios

El profesional puede trabajar en un proyecto real o desarrollar nuevos proyectos en el ámbito de I+D o Desarrollo de Negocio de su compañía.

06

### Aumento de la competitividad

Este Máster Título Propio dotará a sus profesionales de competencias para asumir los nuevos desafíos e impulsar así la organización.

12

# 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 Universidad Tecnológica.





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

Este **Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa** contiene el programa más completo y actualizado del mercado.

Tras la superación de la evaluación, el alumno recibirá por correo postal* con acuse de recibo su correspondiente título de **Máster Propio** emitido por **TECH Universidad Tecnológica.**

El título expedido por **TECH Universidad Tecnológica** expresará la calificación que haya obtenido en el Máster Título Propio, y reunirá los requisitos comúnmente exigidos por las bolsas de trabajo, oposiciones y comités evaluadores de carreras profesionales.

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

N.º Horas Oficiales: **1.500 h.**


tech universidad tecnológica

Otorga la presente

**CONSTANCIA**

a

C. _____, con documento de identificación nº_____

Por haber superado con éxito y acreditado el programa de

**MÁSTER TÍTULO PROPIO**

en

Gestión de Políticas de Ciberseguridad en la Empresa

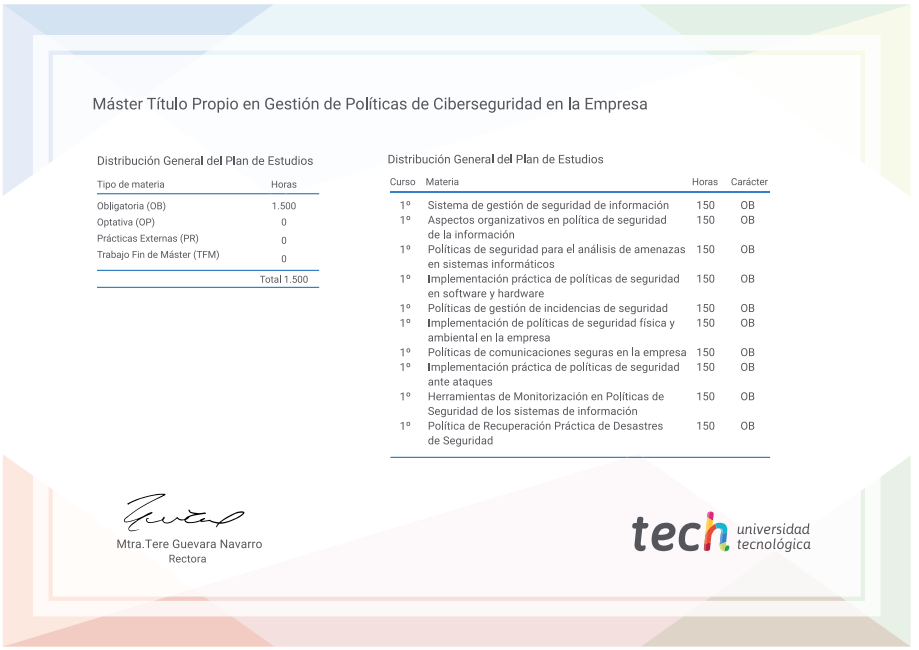
Se trata de un título propio de esta Universidad con una duración de 1.500 horas, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH es una Institución Particular de Educación Superior reconocida por la Secretaría de Educación Pública a partir del 28 de junio de 2018.

A 17 de junio de 2020

Mtra.Tere Guevara Navarro
Rectora

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 | Horas |
|---|---|
| Obligatoria (OB) | 1.500 |
| Optativa (OP) | 0 |
| Prácticas Externas (PR) | 0 |
| Trabajo Fin de Máster (TFM) | 0 |
| | Total 1.500 |

Distribución General del Plan de Estudios

| Curso | Materia | Horas | Carácter |
|---|---|---|---|
| 1º | Sistema de gestión de seguridad de información | 150 | OB |
| 1º | Aspectos organizativos en política de seguridad de la información | 150 | OB |
| 1º | Políticas de seguridad para el análisis de amenazas en sistemas informáticos | 150 | OB |
| 1º | Implementación práctica de políticas de seguridad en software y hardware | 150 | OB |
| 1º | Políticas de gestión de incidencias de seguridad | 150 | OB |
| 1º | Implementación de políticas de seguridad física y ambiental en la empresa | 150 | OB |
| 1º | Políticas de comunicaciones seguras en la empresa | 150 | OB |
| 1º | Implementación práctica de políticas de seguridad ante ataques | 150 | OB |
| 1º | Herramientas de Monitorización en Políticas de Seguridad de los sistemas de información | 150 | OB |
| 1º | Política de Recuperación Práctica de Desastres de Seguridad | 150 | OB |

Mtra.Tere Guevara Navarro
Rectora

tech universidad tecnológica

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

tech universidad tecnológica

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

Idioma: **Español**
Modalidad: **Online**
Duración: **12 meses**
Titulación: **TECH Universidad Tecnológica**
Horas lectivas: **1.500 h.**

# Máster Título Propio

## Gestión de Políticas de Ciberseguridad en la Empresa



tech universidad tecnológica