

# Máster de Formación Permanente

## Gestión de Políticas de Ciberseguridad en la Empresa

M G P C E



## Máster de Formación Permanente

### Gestión de Políticas de Ciberseguridad en la Empresa

- » Modalidad: **online**
- » Duración: **7 meses**
- » Titulación: **TECH Universidad Tecnológica**
- » Acreditación: **60 ECTS**
- » Horario: **a tu ritmo**
- » Exámenes: **online**
- » 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/gestion-politicas-ciberseguridad-empresa](http://www.techtitute.com/escuela-de-negocios/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*

# 01

# Bienvenida

Hoy en día, las pérdidas producidas por ciberataques se calculan en cifras que alcanzan y superan ampliamente los millones. Tal es la exposición a sufrir un ataque cibernético que incluso los estados pueden ser objetivo de ciberincidentes. Esto ha puesto en relieve la importancia de contar con directivos especializados en la Gestión de Políticas de Ciberseguridad, con los conocimientos adecuados en organización, implementación y herramientas de monitorización para coordinar todos los esfuerzos en seguridad cibernética. Este programa prepara al directivo para enfrentarse a escenarios inciertos con seguridad y conocimientos avanzados, aportando soluciones de calidad en materia de Seguridad de la Información. A través de un contenido teórico exhaustivo, basado en casos prácticos reales, se obtendrá una perspectiva moderna e integral de todas las funciones que debe desarrollar un responsable de ciberseguridad. Todo ello, además, en un formato 100% online libre de clases presenciales y horarios prefijados, con una flexibilidad total.



Máster de Formación Permanente en Gestión de Políticas de Ciberseguridad en la Empresa.  
TECH Universidad Tecnológica



“

*Aporta un valor incalculable a tus Políticas de Ciberseguridad conociendo todos sus matices, desde los propios sistemas de seguridad a las prácticas en análisis de amenaza que te darán las claves para posicionarte con ventaja en tu organización”*

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.



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.



### 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”*

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 de Formación Permanente 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

04

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

02

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

03

Implementar un SGSI en la empresa





05

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

06

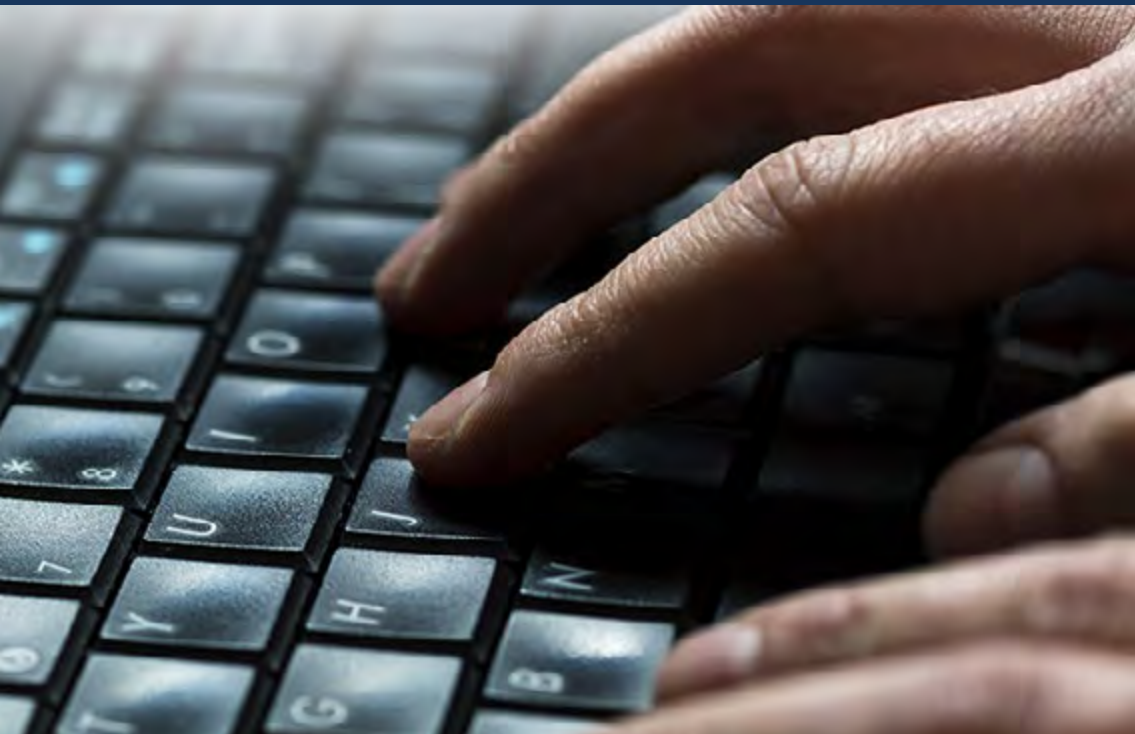
Determinar qué es la autenticación e identificación

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

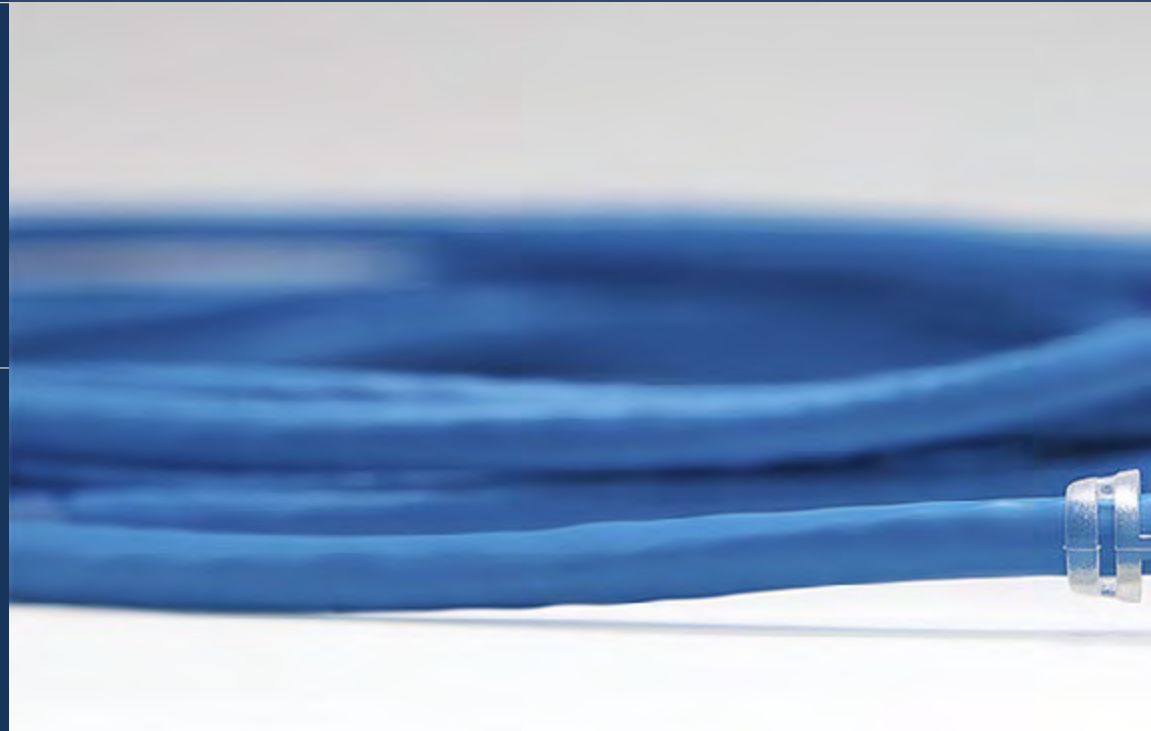
Analizar el término de área segura y perímetro seguro

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 proveedores 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

12

Examinar la Biometría y sistemas biométricos

10

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

11

Compilar los distintos sistemas biométricos que existen

13

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





14

Implementar una red segura

16

Establecer los tipos de Ingeniería social y aprender a mitigarlos



15

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

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 de Formación Permanente 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 de Formación Permanente 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 de Formación Permanente 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 de Formación Permanente se desarrolla a lo largo de 7 meses y se divide en 10 módulos:

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



### ¿Dónde, cuándo y cómo se imparte?

TECH ofrece la posibilidad de desarrollar este Máster de Formación Permanente en Gestión de Políticas de Ciberseguridad en la Empresa de manera totalmente online. Durante los 7 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 (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 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. 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

<b>3.1. La gestión de amenazas en las políticas de seguridad</b> 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	<b>3.2. Fases de la gestión de amenazas</b> 3.2.1. Identificación 3.2.2. Análisis 3.2.3. Localización 3.2.4. Medidas de salvaguarda	<b>3.3. Sistemas de auditoria para localización de amenazas</b> 3.3.1. Clasificación y flujo de información 3.3.2. Análisis de los procesos vulnerable	<b>3.4. Clasificación del riesgo</b> 3.4.1. Tipos de riesgo 3.4.2. Cálculo de la probabilidad de amenaza 3.4.3. Riesgo residual
<b>3.5. Tratamiento del riesgo</b> 3.5.1. Implementación de medidas de salvaguarda 3.5.2. Transferir o asumir	<b>3.6. Control de riesgo</b> 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	<b>3.7. Metodologías prácticas para el análisis y control de amenazas</b> 3.7.1. Catálogo de amenazas 3.7.2. Catálogo de medidas de control 3.7.3. Catálogo de salvaguardas	<b>3.8. Norma ISO 27005</b> 3.8.1. Identificación del riesgo 3.8.2. Análisis del riesgo 3.8.3. Evaluación del riesgo
<b>3.9. Matriz de riesgo, impacto y amenazas</b> 3.9.1. Datos, sistemas y personal 3.9.2. Probabilidad de amenaza 3.9.3. Magnitud del daño	<b>3.10. Diseño de fases y procesos en el análisis de amenazas</b> 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

<b>4.1. Implementación práctica de políticas de seguridad en software y hardware</b> 4.1.1. Implementación de identificación y autorización 4.1.2. Implementación de técnicas de identificación 4.1.3. Medidas técnicas de autorización	<b>4.2. Tecnologías de identificación y autorización</b> 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	<b>4.3. Políticas de seguridad en el acceso a software y sistemas</b> 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	<b>4.4. Gestión de acceso a usuarios</b> 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
<b>4.5. Control de acceso a sistemas y aplicaciones</b> 4.5.1. Norma del mínimo acceso 4.5.2. Tecnologías seguras de inicios de sesión 4.5.3. Políticas de seguridad en contraseñas	<b>4.6. Tecnologías de sistemas de identificación</b> 4.6.1. Directorio activo 4.6.2. OTP 4.6.3. PAP, CHAP 4.6.4. KERBEROS, DIAMETER, NTLM	<b>4.7. Controles CIS para bastionado de sistemas</b> 4.7.1. Controles CIS básicos 4.7.2. Controles CIS fundamentales 4.7.3. Controles CIS organizacionales	<b>4.8. Seguridad en la operativa</b> 4.8.1. Protección contra código malicioso 4.8.2. Copias de seguridad 4.8.3. Registro de actividad y supervisión
<b>4.9. Gestión de las vulnerabilidades técnicas</b> 4.9.1. Vulnerabilidades técnicas 4.9.2. Gestión de vulnerabilidades técnicas 4.9.3. Restricciones en la instalación de software	<b>4.10. Implementación de prácticas de políticas de seguridad</b> 4.10.1. Vulnerabilidades lógicas 4.10.2. Implementación de políticas de defensa		



**Módulo 5. Políticas de Gestión de Incidencias de Seguridad**

<p><b>5.1. Políticas de gestión de incidencias de seguridad de la información y mejoras</b></p> <ul style="list-style-type: none"> <li>5.1.1. Gestión de incidencias</li> <li>5.1.2. Responsabilidades y procedimientos</li> <li>5.1.3. Notificación de eventos</li> </ul>	<p><b>5.2. Sistemas de detección y prevención de intrusiones (IDS/IPS)</b></p> <ul style="list-style-type: none"> <li>5.2.1. Datos de funcionamiento del sistema</li> <li>5.2.2. Tipos de sistemas de detección de intrusos</li> <li>5.2.3. Criterios para la ubicación de los IDS/IPS</li> </ul>	<p><b>5.3. Respuesta ante incidentes de seguridad</b></p> <ul style="list-style-type: none"> <li>5.3.1. Procedimiento de recolección de información</li> <li>5.3.2. Proceso de verificación de intrusión</li> <li>5.3.3. Organismos CERT</li> </ul>	<p><b>5.4. Proceso de notificación y gestión de intentos de intrusión</b></p> <ul style="list-style-type: none"> <li>5.4.1. Responsabilidades en el proceso de notificación</li> <li>5.4.2. Clasificación de los incidentes</li> <li>5.4.3. Proceso de resolución y recuperación</li> </ul>
<p><b>5.5. Análisis forense como política de seguridad</b></p> <ul style="list-style-type: none"> <li>5.5.1. Evidencias volátiles y no volátiles</li> <li>5.5.2. Análisis y recogida de evidencias electrónicas                             <ul style="list-style-type: none"> <li>5.5.2.1. Análisis de evidencias electrónicas</li> <li>5.5.2.2. Recogida de evidencias electrónicas</li> </ul> </li> </ul>	<p><b>5.6. Herramientas de Sistemas de detección y Prevención de Intrusiones (IDS/IPS)</b></p> <ul style="list-style-type: none"> <li>5.6.1. Snort</li> <li>5.6.2. Suricata</li> <li>5.6.3. Solar-Winds</li> </ul>	<p><b>5.7. Herramientas centralizadoras de eventos</b></p> <ul style="list-style-type: none"> <li>5.7.1. SIM</li> <li>5.7.2. SEM</li> <li>5.7.3. SIEM</li> </ul>	<p><b>5.8. Guía de seguridad CCN-STIC 817</b></p> <ul style="list-style-type: none"> <li>5.8.1. Guía de seguridad CCN-STIC 817</li> <li>5.8.2. Gestión de ciberincidentes</li> <li>5.8.3. Métricas e Indicadores</li> </ul>
<p><b>5.9. NIST SP800-61</b></p> <ul style="list-style-type: none"> <li>5.9.1. Capacidad de respuesta antes incidentes de seguridad informática</li> <li>5.9.2. Manejo de un incidente</li> <li>5.9.3. Coordinación e información compartida</li> </ul>	<p><b>5.10. Norma ISO 27035</b></p> <ul style="list-style-type: none"> <li>5.10.1. Norma ISO 27035. Principios de la gestión de incidentes</li> <li>5.10.2. Guías para la elaboración de un plan para la gestión de incidentes</li> <li>5.10.3. Guías de operaciones en la respuesta a incidentes</li> </ul>		

## 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. 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. 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

<p><b>8.1. System Hacking</b>                  8.1.1. Riesgos y vulnerabilidades                  8.1.2. Contramedidas</p>	<p><b>8.2. DoS en servicios</b>                  8.2.1. Riesgos y vulnerabilidades                  8.2.2. Contramedidas</p>	<p><b>8.3. Session Hijacking</b>                  8.3.1. El proceso de <i>Hijacking</i>                  8.3.2. Contramedidas a <i>Hijacking</i></p>	<p><b>8.4. Evasión de IDS, Firewalls and Honeypots</b>                  8.4.1. Técnicas de evasión                  8.4.2. Implementación de contramedidas</p>
<p><b>8.5. Hacking Web Servers</b>                  8.5.1. Ataques a servidores webs                  8.5.2. Implementación de medidas de defensa</p>	<p><b>8.6. Hacking Web Applications</b>                  8.6.1. Ataques a aplicaciones web                  8.6.2. Implementación de medidas de defensa</p>	<p><b>8.7. Hacking Wireless Networks</b>                  8.7.1. Vulnerabilidades redes wifi                  8.7.2. Implementación de medidas de defensa</p>	<p><b>8.8. Hacking Mobile Platforms</b>                  8.8.1. Vulnerabilidades de plataformas móviles                  8.8.2. Implementación de contramedidas</p>
<p><b>8.9. Ramsonware</b>                  8.9.1. Vulnerabilidades causantes del <i>Ramsonware</i>                  8.9.2. Implementación de contramedidas</p>	<p><b>8.10. Ingeniería social</b>                  8.10.1. Tipos de ingeniería social                  8.10.2. Contramedidas para la ingeniería social</p>		

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

<p><b>9.1. Políticas de monitorización de sistemas de la información</b>                  9.1.1. Monitorización de sistemas                  9.1.2. Métricas                  9.1.3. Tipos de métricas</p>	<p><b>9.2. Auditoría y registro en sistemas</b>                  9.2.1. Auditoría y Registro en sistemas                  9.2.2. Auditoría y registro en Windows                  9.2.3. Auditoría y registro en Linux</p>	<p><b>9.3. Protocolo SNMP. Simple Network Management Protocol</b>                  9.3.1. Protocolo SNMP                  9.3.2. Funcionamiento de SNMP                  9.3.3. Herramientas SNMP</p>	<p><b>9.4. Monitorización de redes</b>                  9.4.1. La monitorización de red en sistemas de control                  9.4.2. Herramientas de monitorización para sistemas de control</p>
<p><b>9.5. Nagios. Sistema de monitorización de redes</b>                  9.5.1. Nagios                  9.5.2. Funcionamiento de Nagios                  9.5.3. Instalación de Nagios</p>	<p><b>9.6. Zabbix. Sistema de monitorización de redes</b>                  9.6.1. Zabbix                  9.6.2. Funcionamiento de Zabbix                  9.6.3. Instalación de Zabbix</p>	<p><b>9.7. Cacti. Sistema de monitorización de redes</b>                  9.7.1. Cacti                  9.7.2. Funcionamiento de Cacti                  9.7.3. Instalación de Cacti</p>	<p><b>9.8. Pandora. Sistema de monitorización de redes</b>                  9.8.1. Pandora                  9.8.2. Funcionamiento de Pandora                  9.8.3. Instalación de Pandora</p>
<p><b>9.9. SolarWinds. Sistema de monitorización de redes</b>                  9.9.1. SolarWinds                  9.9.2. Funcionamiento de SolarWinds                  9.9.3. Instalación de SolarWinds</p>	<p><b>9.10. Normativa sobre monitorización</b>                  9.10.1. Controles CIS sobre auditoría y registro                  9.10.2. NIST 800-123 (EE.UU)</p>		

**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

main.cpp

```
42 cout<<"Registration Name: ";
43 cout<<"Course: ";
44 cout<<"GPA: ";
45
46 file.read((char*)obj.name);
47 }
48 file.close();
49
50 getch();
51 }
52
53 void search()
54 {
55     // done!
56     float user;
57     cout<<"Enter GPA: ";
58     cin>>user;
59     file.open("database.txt", ios::in);
60     file.read((char*)obj.name);
61     while (file.eof() == false)
62     {
63         if (obj.gpa == user)
64         {
65             cout<<"Name: ";
66             cout<<"Registration Name: ";
67             cout<<"Course: ";
68             cout<<"GPA: ";
69         }
70         file.read((char*)obj.name);
71     }
72     file.close();
73
74     getch();
75 }
76
77 void edit()
78 {
79     // done!
80     char user[100];
81     cout<<"Enter registration name: ";
82     cin>>user;
83 }
```

07

# Metodología

Este programa de capacitación ofrece una forma diferente de aprender. Nuestra metodología se desarrolla a través de un modo de aprendizaje de forma cíclica: ***el Relearning***.

Este sistema de enseñanza es utilizado, por ejemplo, en las facultades de medicina más prestigiosas del mundo y se ha considerado uno de los más eficaces por publicaciones de gran relevancia como el ***New England Journal of Medicine***.





“

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

## TECH Business School emplea el Estudio de Caso para contextualizar todo el contenido

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

“

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



*Este programa te prepara para afrontar retos empresariales en entornos inciertos y lograr el éxito de tu negocio.*





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

## Un método de aprendizaje innovador y diferente

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

“

*Aprenderás, mediante actividades colaborativas y casos reales, la resolución de situaciones complejas en entornos empresariales reales”*

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de negocios del mundo desde que éstas existen. Desarrollado en 1912 para que los estudiantes de Derecho no solo aprendiesen las leyes a base de contenidos teóricos, el método del caso consistió en presentarles situaciones complejas reales para que tomaran decisiones y emitieran juicios de valor fundamentados sobre cómo resolverlas.

En 1924 se estableció como método estándar de enseñanza en Harvard.

Ante una determinada situación, ¿qué debería hacer un profesional? Esta es la pregunta a la que nos enfrentamos en el método del caso, un método de aprendizaje orientado a la acción. A lo largo del programa, los estudiantes se enfrentarán a múltiples casos reales.

Deberán integrar todos sus conocimientos, investigar, argumentar y defender sus ideas y decisiones.

## Relearning Methodology

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

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

*Nuestro sistema online te permitirá organizar tu tiempo y tu ritmo de aprendizaje, adaptándolo a tus horarios. Podrás acceder a los contenidos desde cualquier dispositivo fijo o móvil con conexión a internet.*

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

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



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

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

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

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



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



#### Material de estudio

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

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



#### Clases magistrales

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

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



#### Prácticas de habilidades directivas

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



#### Lecturas complementarias

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





#### Case studies

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



#### Resúmenes interactivos

El equipo de TECH presenta los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audios, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento. Este exclusivo sistema educativo para la presentación de contenidos multimedia fue premiado por Microsoft como "Caso de éxito en Europa".



#### Testing & Retesting

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



08

# Perfil de nuestros alumnos

El Máster de Formación Permanente 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 de Formación Permanente 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.





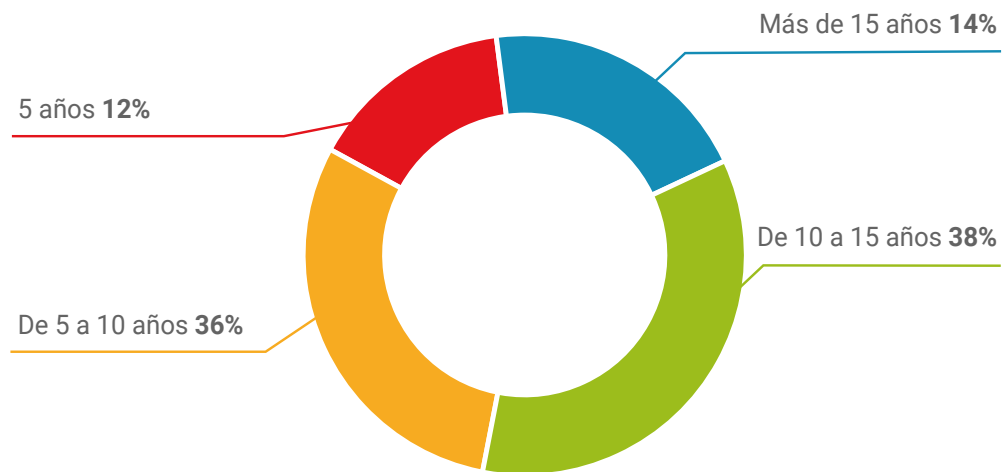
“

*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”*

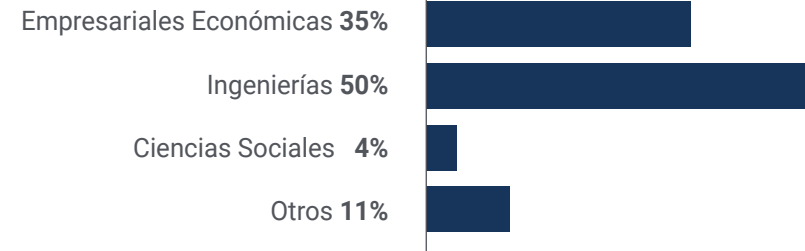
### Edad media

Entre **35** y **45** años

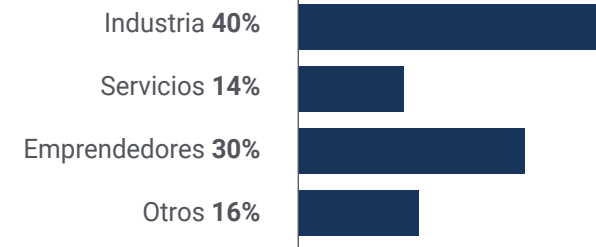
### Años de experiencia



### Formación



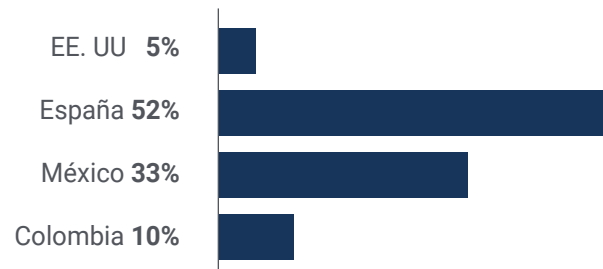
### Perfil académico





## 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 Technologies. 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 de Formación Permanente 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 ayudarte 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.

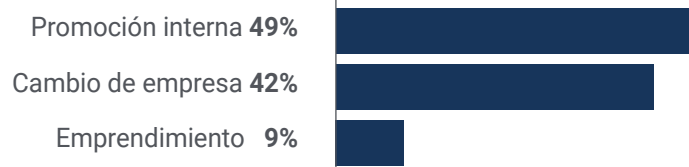
*Conseguirás la mejora laboral que persigues en menos tiempo del que imaginas gracias a la metodología pedagógica de TECH.*

*Matricúlate ya en este Máster de Formación Permanente y no esperes más a conseguir un cambio positivo en tu entorno.*

### Momento del cambio



### Tipo de cambio



## Mejora salarial

---

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



11

# Beneficios para tu empresa

El Máster de Formación Permanente 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 de Formación Permanente 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 de Formación Permanente dotará a sus profesionales de competencias para asumir los nuevos desafíos e impulsar así la organización.



12

# Titulación

Este programa 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 de Formación Permanente expedido por TECH Universidad Tecnológica.





“

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

Este programa te permitirá obtener el título de **Máster de Formación Permanente en Gestión de Políticas de Ciberseguridad en la Empresa** emitido por TECH Universidad Tecnológica.

TECH Universidad Tecnológica, es una Universidad española oficial, que forma parte del Espacio Europeo de Educación Superior (EEES). Con un enfoque centrado en la excelencia académica y la calidad universitaria a través de la tecnología.

Este título propio contribuye de forma relevante al desarrollo de la educación continua y actualización del profesional, garantizándole la adquisición de las competencias en su área de conocimiento y aportándole un alto valor curricular universitario a su formación. Es 100% válido en todas las Oposiciones, Carrera Profesional y Bolsas de Trabajo de cualquier Comunidad Autónoma española.

Además, el riguroso sistema de garantía de calidad de TECH asegura que cada título otorgado cumpla con los más altos estándares académicos, brindándole al egresado la confianza y la credibilidad que necesita para destacarse en su carrera profesional.

Título: **Máster de Formación Permanente en Gestión de Políticas de Ciberseguridad en la Empresa**

Modalidad: **online**

Duración: **7 meses**

Créditos: **60 ECTS**



**tech** universidad tecnológica

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

**Máster de Formación Permanente en Gestión de Políticas de Ciberseguridad en la Empresa**

Se trata de un título propio de 1.500 horas de duración equivalente a 60 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH Universidad Tecnológica es una universidad oficial española que pertenece al Espacio Europeo de Educación Superior (EEES).

En San Cristóbal de la Laguna, a 28 de febrero de 2024

  
 Dr. Pedro Navarro Illana  
 Rector

código único TECH: AFWOR23S techtitulador.com/titulos



**Máster de Formación Permanente en Gestión de Políticas de Ciberseguridad en la Empresa**

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

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** 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.



## Máster de Formación Permanente

Gestión de Políticas  
de Ciberseguridad  
en la Empresa

- » Modalidad: **online**
- » Duración: **7 meses**
- » Titulación: **TECH Universidad Tecnológica**
- » Acreditación: **60 ECTS**
- » Horario: **a tu ritmo**
- » Exámenes: **online**

# Máster de Formación Permanente

## Gestión de Políticas de Ciberseguridad en la Empresa