# Máster Título Propio

## Gestión de Políticas de Ciberseguridad en la Empresa

tech universidad tecnológica

tech universidad tecnológica

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

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Universidad Tecnológica**
- Horario: **a tu ritmo**
- Exámenes: **online**

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

# Índice

01

# Presentación

La mayor dependencia de muchas empresas e industrias de entornos virtuales ha provocado, a su vez, la proliferación de la ciberdelincuencia y los ataques informáticos a todo tipo de organizaciones. Independientemente del tamaño o localización, las amenazas de ciberseguridad suponen un peligro real que puede provocar numerosas pérdidas tanto de tiempo como de dinero o datos. Por ello, la figura del informático con conocimientos específicos en Gestión de Políticas de Ciberseguridad está cobrando cada vez más peso en el sector empresarial, con amplias oportunidades de crecimiento tanto profesional como personal. Esta titulación ofrece al profesional de la informática una oportunidad inmejorable para darle un impulso a la carrera, apoyándose en un equipo de profesionales con amplia experiencia en la materia. El formato 100% online de la titulación la hace, además, una opción completamente compatible con toda clase de actividades o responsabilidades.

*Inscríbete ya y accede a un contenido especializado en Políticas de Gestión de Incidencias, Seguridad en software y hardware y Recuperación Práctica de Desastres de Seguridad"*

Miles de ciberdelincuentes atacan cada día a empresas de todo el mundo, incluso a distancias de miles de kilómetros, lo que ha colocado a la ciberseguridad como una de las principales preocupaciones en el panorama empresarial moderno. Las vulnerabilidades de las organizaciones que dependen de entornos virtuales pueden ser aprovechadas por criminales de todo tipo, robando datos sensibles o impidiendo el acceso a los mismos a cambio de un rescate.

Es por ello que una correcta Gestión de Políticas de Ciberseguridad en la Empresa conlleva una gran responsabilidad, siendo este puesto de responsabilidad uno de alto prestigio y proyección económica para el informático especializado. Por ello, dar el paso y profundizar en temas como los sistemas de auditoría para localizar amenazas o los protocolos seguros de comunicación, supone un impulso directo hacia una posición clave en cualquier organización.

Para este Máster Título Propio, un grupo de docentes seleccionados minuciosamente por TECH, ha preparado un contenido didáctico de primer nivel. A lo largo de 10 módulos exhaustivos, el informático ampliará sus capacidades en materia de Implementación de Políticas de Seguridad Física y Ambiental, Sistema de Gestión de Seguridad de la Información, herramientas de monitorización y muchas más competencias que le convertirán en un activo valioso en cualquier institución.

Todo ello con la ventaja incontestable de no tener que atender clases presenciales ni horarios prefijados, pues todo el programa se imparte de manera online. El contenido didáctico está disponible para su descarga desde cualquier dispositivo con conexión a internet, sirviendo incluso de guía de referencia una vez se acabe la titulación. El informático tendrá la libertad de adaptar la carga lectiva a su propio ritmo, pudiendo compaginarla con su actividad profesional habitual o sus responsabilidades más exigentes.

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

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

*Posiciónate como un responsable de Políticas de Ciberseguridad solvente, adaptándote a toda clase de situaciones e imprevistos en materia de Seguridad Informática”*

*Incorpora a tu trabajo diario las prácticas de políticas de seguridad ante ataques más eficaces, perfeccionadas por un equipo docente especializado en el campo”*

*Accede a un temario rico en contenido multimedia, reforzado con temas específicos sobre políticas de seguridad en dirección, clasificación de riesgos informáticos e Hijacking.*

*Podrás elegir cuando, donde y como asumir toda la carga lectiva, teniendo libertad total para avanzar en el temario a tu propio ritmo.*

El programa incluye, en su cuadro docente, a profesionales del sector que vierten en esta capacitación la experiencia de su trabajo, además de reconocidos especialistas de sociedades de referencia y universidades de prestigio.

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

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

02

# Objetivos

Al ser la ciberseguridad un tema tan importante en el mundo empresarial actual, esta titulación asume el rol del informático como una parte central para lidiar con dichos problemas. Por ello, los objetivos perseguidos a lo largo de todo el temario son diversos, priorizando ofrecer un contenido teórico actualizado en base a los últimos avances en materia de seguridad informática.

*Tendrás a tu disposición una guía de referencia en materia de Gestión de Políticas de Ciberseguridad que te ayudará a impulsar tu carrera como informático experto en seguridad digital"*

## Objetivos generales

- Profundizar en los conceptos clave de la seguridad de la información
- Desarrollar las medidas necesarias para garantizar buenas prácticas en materia de seguridad de la información
- Desarrollar las diferentes metodologías para la realización de un análisis exhaustivo de amenazas
- Instalar y conocer las distintas herramientas utilizadas en el tratamiento y prevención de incidencias

*La metodología pedagógica de TECH te permitirá alcanzar tus objetivos más ambiciosos incluso antes de lo que esperas"*

## Objetivos específicos

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

- Analizar las normativas y estándares aplicables en la actualidad a los SGSI
- Desarrollar las fases necesarias para implementar un SGSI en una entidad
- Analizar los procedimientos de gestión de incidentes de seguridad de la información e implantación

### Módulo 2. Aspectos organizativos en Política de Seguridad de la Información

- Implementar un SGSI en la empresa
- Determinar qué departamentos debe abarcar la implementación del sistema de gestión de seguridad
- Implementar contramedidas de seguridad necesaria en la operativa

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

- Analizar el significado de amenazas
- Determinar las fases de una gestión preventiva de amenazas
- Comparar las distintas metodologías de gestión de amenazas

### Módulo 4. Implementación Práctica de Políticas de seguridad en Software y Hardware

- Determinar qué es la Autenticación e Identificación
- Analizar los distintos métodos de Autenticación que existen y su implementación práctica
- Implementar la política de control de accesos correcta al software y sistemas
- Establecer las principales tecnologías de identificación actuales
- Generar conocimiento especializado sobre las distintas metodologías que existen para el bastionado de sistemas

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

- Desarrollar conocimiento especializado sobre cómo gestionar incidencias causadas por eventos de seguridad informática
- Determinar el funcionamiento de un equipo de tratamiento de incidencias en materia de seguridad
- Analizar las distintas fases de una gestión de eventos de seguridad informática
- Examinar los protocolos estandarizados para el tratamiento de incidencias de seguridad

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

- Analizar el término de Área Segura y Perímetro Seguro
- Examinar la Biometría y sistemas biométricos
- Implementar políticas de seguridad correctas en materia de seguridad física
- Desarrollar la normativa vigente acerca de áreas seguras de sistemas informáticos

### Módulo 7. Políticas de Comunicaciones Seguras en la Empresa

- Segurizar una red de comunicaciones mediante la división de la misma
- Analizar los distintos algoritmos de cifrado utilizados en redes de comunicaciones
- Implementar diversas técnicas de cifrado en la red como TLS, VPN o SSH

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

- Determinar los distintos ataques reales a nuestro sistema de información
- Evaluar las distintas políticas de seguridad para paliar los ataques
- Implementar técnicamente las medidas para mitigar las principales amenazas

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

- Desarrollar el concepto de Monitorización e Implementación de Métricas
- Configurar los registros de auditoria en los sistemas y a monitorizar las redes
- Compilar las mejores herramientas de monitorización de sistemas existentes actualmente en el mercado

### Módulo 10. Política de Recuperación práctica de Desastres de Seguridad

- Generar conocimiento especializado sobre el concepto de Continuidad de la seguridad de la información
- Desarrollar un plan de continuidad de negocio
- Analizar un plan de continuidad TIC
- Diseñar un plan de recuperación de desastres

03

# Competencias

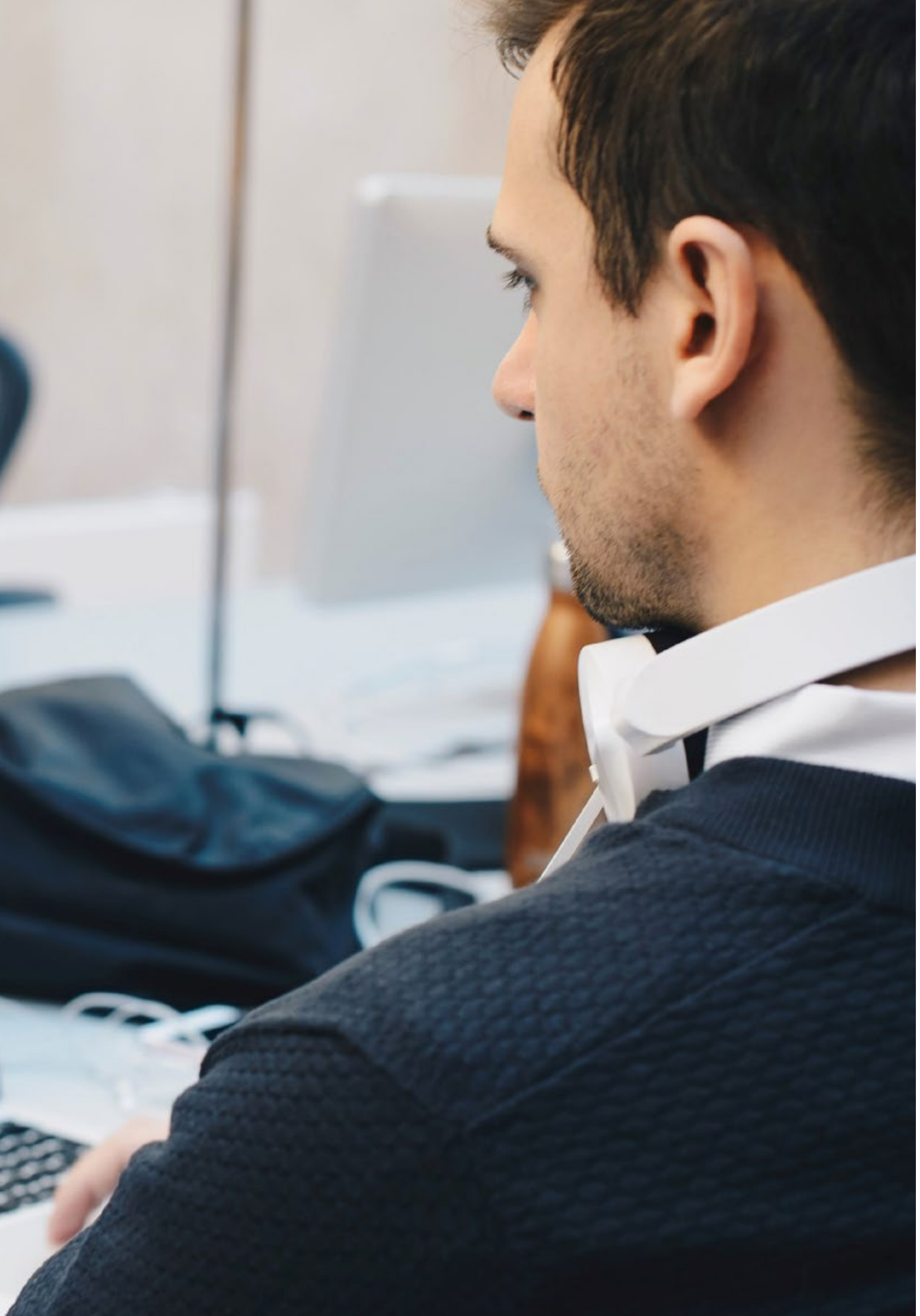
Para desarrollar las competencias perfeccionadas y especializadas que debe poseer un informático experto en Políticas de Ciberseguridad, TECH ha recurrido a un personal docente excepcional. Gracias a una combinación práctica de su experiencia profesional y los desarrollos más recientes en materia de seguridad digital, el informático obtendrá una contextualización mucho mayor de cada tema tratado, con amplios ejemplos y recursos multimedia para ello.

*Obtendrás un set de habilidades que resaltarán tu importancia clave en cualquier plan de estrategia cibernética en tu organización”*

## Competencias generales

- Implementar y desarrollar un Plan de Continuidad de Negocio acorde a cada tipología de entidad y sus necesidades
- Desarrollar un Análisis de Proceso de Negocio
- Analizar las metodologías de auditoria
- Valorar la necesidad de un Análisis Forense Informático para el estudio en profundidad de las incidencias registradas

*Conseguirás aumentar tu proyección laboral y salarial gracias a una especialización en el tema que más preocupa actualmente, la ciberseguridad"*





## Competencias específicas

- Determinar la implicación de un SGSI en la organización interna de la entidad, así como su estado
- Establecer las políticas de seguridad en la empresa
- Determinar qué medidas tenemos que implementar con suministradores y mantenimientos de sistemas de información
- Generar un conocimiento especializado sobre el control de amenazas
- Determinar las fases de la gestión preventiva de amenazas
- Desarrollar las metodologías para el análisis de amenazas informáticas
- Clasificar las amenazas por impacto y gravedad
- Diseñar una metodología propia para el análisis y control preventivo de amenazas
- Implementar una política correcta de control de accesos a redes y servicios
- Analizar la importancia de un tratamiento correcto en materia de incidencias de seguridad
- Compilar los distintos sistemas biométricos que existen
- Examinar la Biometría y sistemas biométricos
- Implementar las distintas políticas de seguridad física correctas y los sistemas de control de acceso físico en CPDs
- Implementar una red segura
- Examinar las vulnerabilidades de las plataformas móviles y de los IoT y cómo evitarlas
- Establecer los tipos de Ingeniera Social y aprender a mitigarlos
- Analizar el concepto de Monitorización e Implementación de Métricas
- Determinar la necesidad de la continuidad de la seguridad de la información

04

# Dirección del curso

Todos los profesionales que ha seleccionado TECH para la realización de este Máster Título Propio, poseen una amplia experiencia en el ámbito de la gestión de servicios informáticos, siempre con el foco puesto en la ciberseguridad y correcta ejecución de protocolos. Precisamente, es esta experiencia la que confiere un cariz de mayor calidad a todo el temario, pues su naturaleza eminentemente práctica, hace que el informático pueda adoptar todos los nuevos conocimientos de forma inmediata, mejorando sus capacidades incluso antes de finalizar la titulación.

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

## Dirección

### Dña. Fernández Sapena, Sonia

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

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

05

# Estructura y contenido

TECH ha empleado la metodología *Relearning* para elaborar todos los contenidos de este programa. Esto quiere decir que las claves y conceptos más destacados en materia de Gestión de Políticas de Ciberseguridad son dados de forma progresiva a lo largo de todo el temario, resultando en una enseñanza mucho más efectiva y rápida. El informático tendrá acceso a numerosos vídeos en detalle, ejercicios de autoconocimiento y lecturas complementarias realizadas y seleccionadas específicamente para cada tema del programa.


*Todo el material multimedia que contiene este Máster Título Propio te ayudará a especializarte de forma mucho más profunda, rápida y exhaustiva"*

## **Módulo 1.** Sistema de gestión de seguridad de información (SGSI)

1.1. Seguridad de la información. Aspectos clave
- 1.1.1. Seguridad de la información
  - 1.1.1.1. Confidencialidad
  - 1.1.1.2. Integridad
  - 1.1.1.3. Disponibilidad
  - 1.1.1.4. Medidas de seguridad de la Información

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

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

1.4. Normas ISO/IEC 27.000
- 1.4.1. Objeto y ámbito de aplicación
- 1.4.2. Estructura de la norma
- 1.4.3. Certificación
- 1.4.4. Fases de acreditación
- 1.4.5. Beneficios normas ISO/IEC 27.000

1.5. Diseño e implantación de un Sistema General de Seguridad de Información
- 1.5.1. Fases de implantación de un sistema General de Seguridad de la Información
- 1.5.2. Plan de continuidad de negocio

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

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

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

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

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

## **Módulo 2.** Aspectos organizativos en Política de Seguridad de la Información

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

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

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

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

2.5. Políticas de seguridad en dirección
- 2.5.1. Directrices de la dirección en seguridad de la información
- 2.5.2. BIA- analizando el impacto
- 2.5.3. Plan de recuperación como política de seguridad

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## **Módulo 4.** Implementación Práctica de Políticas de seguridad en Software y Hardware

4.1. Implementación práctica de políticas de seguridad en software y hardware
- 4.1.1. Implementación de identificación y autorización
- 4.1.2. Implementación de técnicas de identificación
- 4.1.3. Medidas técnicas de autorización

4.2. Tecnologías de identificación y autorización
- 4.2.1. Identificador y OTP
- 4.2.2. *Token USB* o tarjeta inteligente PKI
- 4.2.3. La llave "Confidencial Defensa"
- 4.2.4. El RFID Activo

4.3. Políticas de seguridad en el acceso a software y sistemas
- 4.3.1. Implementación de políticas de control de accesos
- 4.3.2. Implementación de políticas de acceso a comunicaciones
- 4.3.3. Tipos de herramientas de seguridad para control de acceso

4.4. Gestión de acceso a usuarios
- 4.4.1. Gestión de los derechos de acceso
- 4.4.2. Segregación de roles y funciones de acceso
- 4.4.3. Implementación derechos de acceso en sistemas

4.5. Control de acceso a sistemas y aplicaciones
- 4.5.1. Norma del mínimo acceso
- 4.5.2. Tecnologías seguras de inicios de sesión
- 4.5.3. Políticas de seguridad en contraseñas

4.6. Tecnologías de sistemas de identificación
- 4.6.1. Directorio activo
- 4.6.2. OTP
- 4.6.3. PAP, CHAP
- 4.6.4. KERBEROS, DIAMETER, NTLM

4.7. Controles CIS para bastionado de sistemas
- 4.7.1. Controles CIS básicos
- 4.7.2. Controles CIS fundamentales
- 4.7.3. Controles CIS organizacionales

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

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

4.10. Implementación de prácticas de políticas de seguridad
- 4.10.1. Vulnerabilidades lógicas
- 4.10.2. Implementación de políticas de defensa

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

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

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

5.3. Respuesta ante incidentes de seguridad
- 5.3.1. Procedimiento de recolección de información
- 5.3.2. Proceso de verificación de intrusión
- 5.3.3. Organismos CERT

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

5.5. Análisis forense como política de seguridad
- 5.5.1. Evidencias volátiles y no volátiles
- 5.5.2. Análisis y recogida de evidencias electrónicas
  - 5.5.2.1. Análisis de evidencias electrónicas
  - 5.5.2.2. Recogida de evidencias electrónicas

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## **Módulo 7.** Políticas de Comunicaciones Seguras en la Empresa

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

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

7.3. Protocolo TLS 1.3
- 7.3.1. Fases de un proceso TLS1.3
- 7.3.2. Protocolo *Handshake*
- 7.3.3. Protocolo de registro
- 7.3.4. Diferencias con TLS 1.2

7.4. Algoritmos criptográficos
- 7.4.1. Algoritmos criptográficos usados en comunicaciones
- 7.4.2. *Cipher-suites*
- 7.4.3. Algoritmos criptográficos permitidos para TLS 1.3

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

7.6. PKI. Infraestructura de clave pública
- 7.6.1. PKI y sus entidades
- 7.6.2. Certificado digital
- 7.6.3. Tipos de certificados digital

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

7.8. SSH. *Secure Shell*
- 7.8.1. SSH. Cápsula segura
- 7.8.2. Funcionamiento de SSH
- 7.8.3. Herramientas SSH

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9.2. Auditoria y registro en Sistemas
- 9.2.1. Auditoría y Registro en Sistemas
- 9.2.2. Auditoria y registro en 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. La monitorización de red en sistemas de control
- 9.4.2. Herramientas de monitorización para sistemas de control

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

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

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

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

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

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

## **Módulo 10.** Política de Recuperación práctica de Desastres de Seguridad

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

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

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

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

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


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

10.7. Implementación de los procesos garantizados de negocio
- 10.7.1. Actividades Prioritarias (AP)
- 10.7.2. Tiempos de Recuperación Ideales (TRI)
- 10.7.3. Estrategias de supervivencia

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

10.9. Respuesta a la contingencia
- 10.9.1. Plan de crisis
- 10.9.2. Planes operativos de recuperación de entornos
- 10.9.3. Procedimientos técnicos de trabajo o de incidentes

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

06

# 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"*

## 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"*


*Accederás a un sistema de aprendizaje basado en la reiteración, con una enseñanza natural y progresiva a lo largo de todo el temario.*

*El alumno aprenderá, mediante actividades colaborativas y casos reales, la resolución de situaciones complejas en entornos empresariales reales.*

## Un método de aprendizaje innovador y diferente

El presente programa de TECH es una enseñanza intensiva, creada desde 0, que propone los retos y decisiones más exigentes en este campo, 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 profesional más vigente.

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

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de Informática 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 tomasen decisiones y emitiesen 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 te enfrentamos en el método del caso, un método de aprendizaje orientado a la acción. A lo largo del curso, los estudiantes se enfrentarán a múltiples casos reales. Deberán integrar todos sus conocimientos, investigar, argumentar y defender sus ideas y decisiones.

## Relearning Methodology

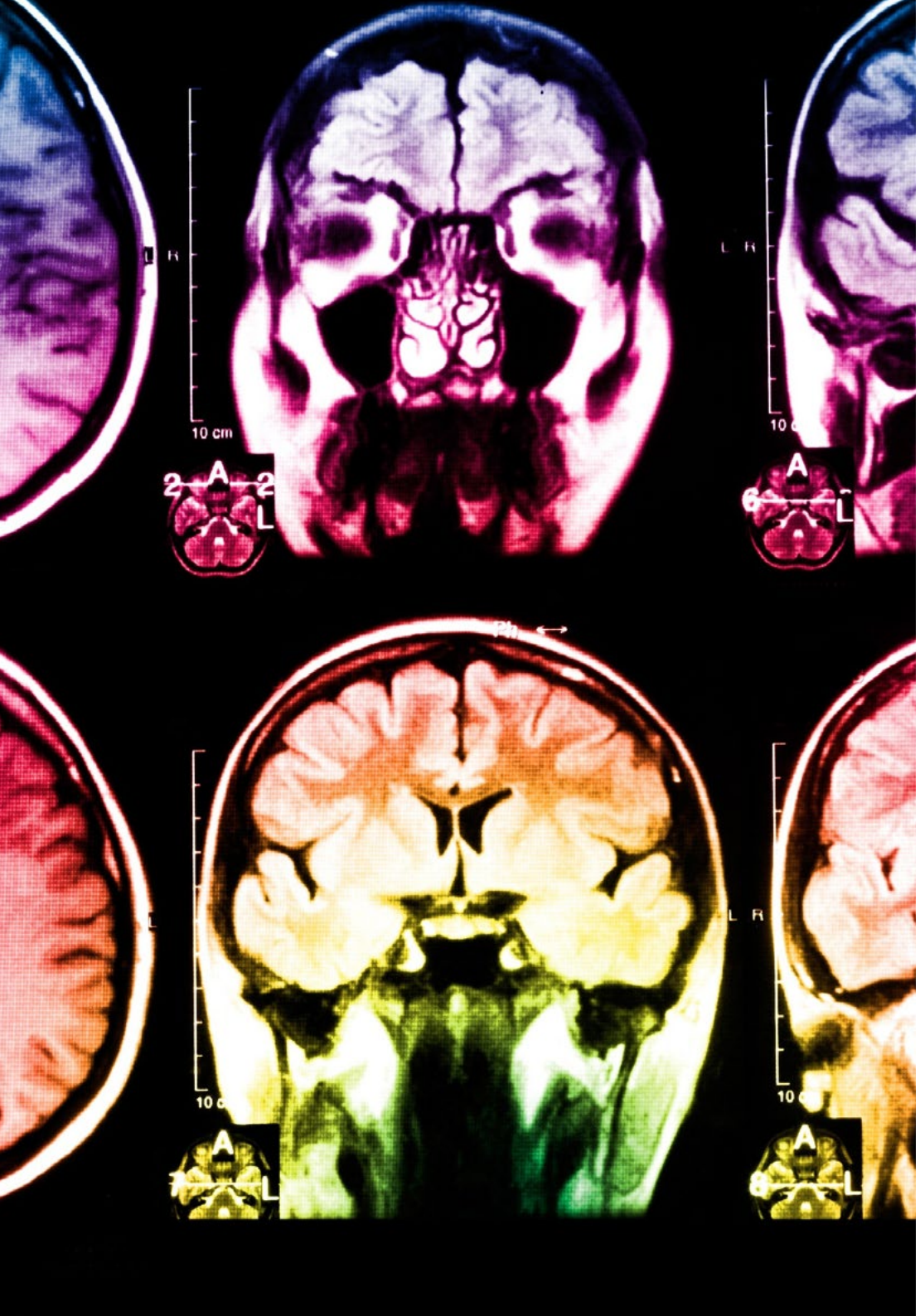
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

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

*En 2019 obtuvimos los mejores resultados de aprendizaje de todas las universidades online en español en el mundo.*

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 universidad 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, se combinan 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 capacitación, 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.

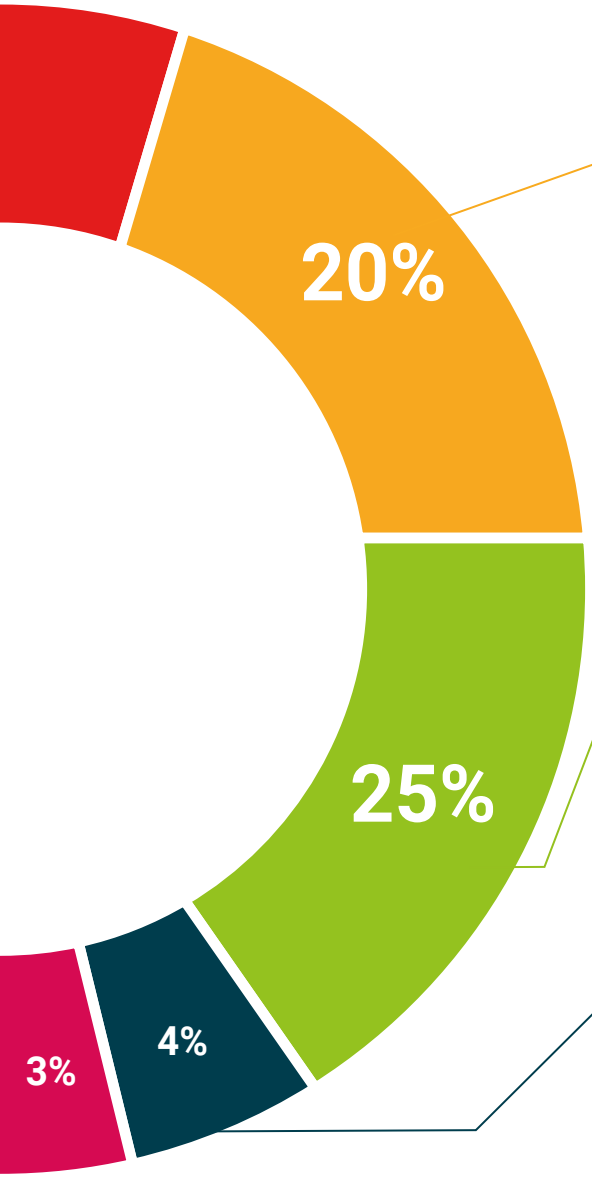
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

### Prácticas de habilidades y competencias

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

### 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 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.

07

# 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

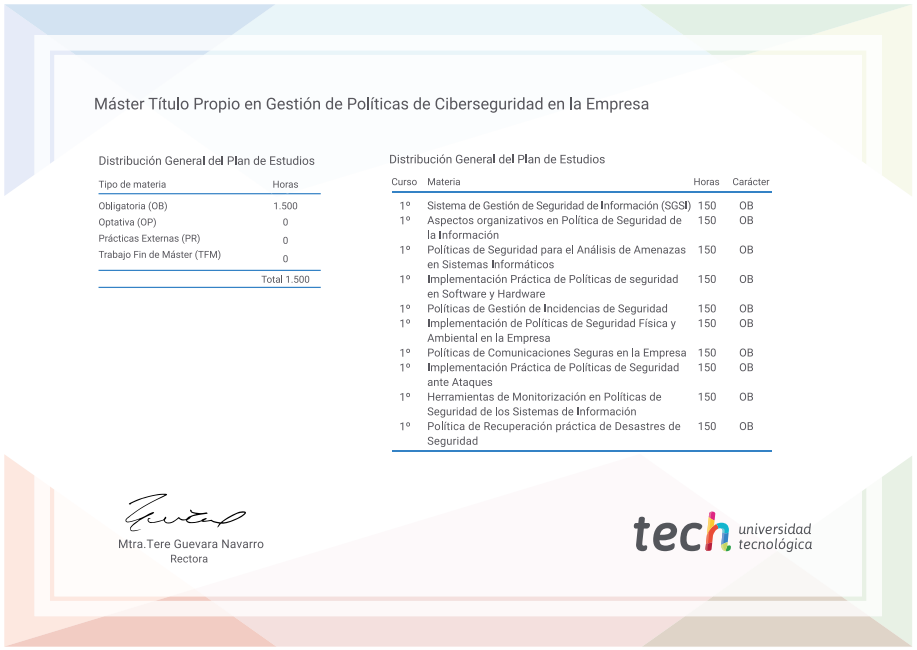
Se trata de un título propio de esta Universidad con una duración de 1.500 horas, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

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 (SGSI) | 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

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Universidad Tecnológica**
- Horario: **a tu ritmo**
- Exámenes: **online**

# Máster Título Propio

## Gestión de Políticas de Ciberseguridad en la Empresa

tech universidad tecnológica