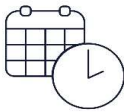
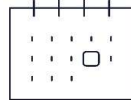


MEJORA TUS COMPETENCIAS PROFESIONALES Y DIGITALES. FORMACIÓN 100% GRATUITA



**Duración**  
100 horas



**Fecha**  
Consultar



**Horario**  
Consultar



**Modalidad**  
Aula virtual  
con Instructor



**Alcance**  
Estatal

## GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA

### OBJETIVO GENERAL

Gestionar la seguridad informática en la empresa.

### CONTENIDO FORMATIVO

Página 1 de 3

#### 1. INTRODUCCIÓN A LA SEGURIDAD

- 1.1. Introducción a la seguridad de información.
- 1.2. Modelo de ciclo de vida de la seguridad de la información.
- 1.3. Confidencialidad, integridad y disponibilidad. Principios de protección de la seguridad de la información.
- 1.4. Políticas de seguridad.
- 1.5. Tácticas de ataque.
- 1.6. Concepto de hacking.
- 1.7. Árbol de ataque.
- 1.8. Lista de amenazas para la seguridad de la información.
- 1.9. Vulnerabilidades.
- 1.10. Vulnerabilidades en sistemas Windows.
- 1.11. Vulnerabilidades en aplicaciones multiplataforma.
- 1.12. Vulnerabilidades en sistemas Unix y Mac OS.
- 1.13. Buenas prácticas y salvaguardas para la seguridad de la red.
- 1.14. Recomendaciones para la seguridad de su red.

#### 2. POLÍTICAS DE SEGURIDAD.

- 2.1. Introducción a las políticas de seguridad.
- 2.2. ¿Por qué son importantes las políticas?
- 2.3. Qué debe de contener una política de seguridad.
- 2.4. Lo que no debe contener una política de seguridad.
- 2.5. Cómo conformar una política de seguridad informática.
- 2.6. Hacer que se cumplan las decisiones sobre estrategia y políticas.

+ Información e inscripciones: [es.comercial@skillsoft.com](mailto:es.comercial@skillsoft.com)

Programa  
financiado por:



**UNIÓN EUROPEA**  
Fondo Social Europeo  
El FSE invierte en tu futuro



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE TRABAJO  
Y ECONOMÍA SOCIAL

SERVICIO PÚBLICO  
DE EMPLEO ESTATAL  
**SEPE**

## GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA

### CONTENIDO FORMATIVO

Continuación

Página 2 de 3

#### 3. AUDITORIA Y NORMATIVA DE SEGURIDAD.

- 3.1. Introducción a la auditoría de seguridad de la información y a los sistemas de gestión de seguridad de la información.
- 3.2. Ciclo del sistema de gestión de seguridad de la información.
- 3.3. Seguridad de la información.
- 3.4. Definiciones y clasificación de los activos.
- 3.5. Seguridad humana, seguridad física y del entorno.
- 3.6. Gestión de comunicaciones y operaciones.
- 3.7. Control de accesos.
- 3.8. Gestión de continuidad del negocio.
- 3.9. Conformidad y legalidad.

#### 4. ESTRATEGIAS DE SEGURIDAD.

- 4.1. Menor privilegio.
- 4.2. Defensa en profundidad.
- 4.3. Punto de choque.
- 4.4. El eslabón más débil.
- 4.5. Postura de fallo seguro.
- 4.6. Postura de negación establecida: lo que no está prohibido.
- 4.7. Postura de permiso establecido: lo que no está permitido.
- 4.8. Participación universal.
- 4.9. Diversificación de la defensa.
- 4.10. Simplicidad.

#### 5. EXPLORACIÓN DE LAS REDES.

- 5.1. Exploración de la red.
- 5.2. Inventario de una red. Herramientas del reconocimiento.
- 5.3. NMAP Y SCANLINE.
- 5.4. Reconocimiento. Limitar y explorar.
- 5.5. Reconocimiento. Exploración.
- 5.6. Reconocimiento. Enumerar.

#### 6. ATAQUES REMOTOS Y LOCALES.

- 6.1. Clasificación de los ataques.
- 6.2. Ataques remotos en UNIX.
- 6.3. Ataques remotos sobre servicios inseguros en UNIX.
- 6.4. Ataques locales en UNIX.
- 6.5. ¿Qué hacer si recibimos un ataque?

+ Información e inscripciones: [es.comercial@skillsoft.com](mailto:es.comercial@skillsoft.com)

Programa  
financiado por:



**UNIÓN EUROPEA**  
Fondo Social Europeo  
El FSE invierte en tu futuro



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE TRABAJO  
Y ECONOMÍA SOCIAL

SERVICIO PÚBLICO  
DE EMPLEO ESTATAL  
**SEPE**

## GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA

### CONTENIDO FORMATIVO

Continuación

Página 3 de 3

#### 7. SEGURIDAD EN REDES ILANÁMBRICAS

- 7.1. Introducción.
- 7.2. Introducción al estándar inalámbrico 802.11 – WIFI
- 7.3. Topologías.
- 7.4. Seguridad en redes Wireless. Redes abiertas.
- 7.5. WEP.
- 7.6. WEP. Ataques.
- 7.7. Otros mecanismos de cifrado.

#### 8. CRIPTOGRAFÍA Y CRIPTOANÁLISIS.

- 8.1. Criptografía y criptoanálisis: introducción y definición.
- 8.2. Cifrado y descifrado.
- 8.3. Ejemplo de cifrado: relleno de una sola vez y criptografía clásica.
- 8.4. Ejemplo de cifrado: criptografía moderna.
- 8.5. Comentarios sobre claves públicas y privadas: sesiones.

#### 9. AUTENTICACIÓN.

- 9.1. Validación de identificación en redes.
- 9.2. Validación de identificación en redes: métodos de autenticación.
- 9.3. Validación de identificación basada en clave secreta compartida: protocolo.
- 9.4. Establecimiento de una clave compartida: intercambio de claves Diffie-Hellman.
- 9.5. Validación de identificación usando un centro de distribución de claves.
- 9.6. Protocolo de autenticación Kerberos.
- 9.7. Validación de identificación de clave pública.
- 9.8. Validación de identificación de clave pública: protocolo de interbloqueo.

### REQUISITOS

- Estar registrado como empleado activo en la Seguridad Social, ya sea como trabajador por cuenta propia o ajena, o como solicitante de empleo en el Servicio Público de Empleo Estatal (SEPE).
- Para cada curso al que el alumno quiera asistir, recopilar y devolver al centro de formación la documentación que se le solicitará.
- Atender al menos a un 75% de la extensión del curso para poder recibir el diploma de asistencia correspondiente.
- Contar con las habilidades necesarias para utilizar la plataforma virtual WEBEX, que se emplea en la formación.

+ Información e inscripciones: [es.comercial@skillsoft.com](mailto:es.comercial@skillsoft.com)

Programa  
financiado por:



**UNIÓN EUROPEA**  
Fondo Social Europeo  
El FSE invierte en tu futuro



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE TRABAJO  
Y ECONOMÍA SOCIAL

SERVICIO PÚBLICO  
DE EMPLEO ESTATAL  
**SEPE**