



## (IFCT050PO) GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA

SKU: PD7895

Horas [100](#)

### OBJETIVOS

- Gestionar la seguridad informática en la empresa.

### CONTENIDO

#### **Unidad 1: Introducción a la seguridad.**

- Introducción, modelo de ciclo de vida y principios de protección de la seguridad de la información.
  - o Modelo de ciclo de vida de la seguridad de la información.
- Políticas de seguridad.
- Tácticas de ataque.
- Concepto de hacking.
- Árbol de ataque.
- Lista de amenazas para la seguridad de la información.
- Vulnerabilidades en sistemas Windows, en aplicaciones multiplataforma y en sistemas Unix y Mac OS.
  - o Vulnerabilidades en los sistemas Windows.
- Buenas prácticas, salvaguardas y recomendaciones para la seguridad de la red.
  - o Salvaguardas para la seguridad de la red.
  - o Recomendaciones para la seguridad de una red.

Examen UA 01

### **Unidad 2: Políticas de seguridad.**

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

Examen UA 02

### **Unidad 3: Auditoría y normativa de seguridad.**

- Introducción a la auditoría de seguridad de la información y a los sistemas de gestión de seguridad de la información.
- Ciclo del sistema de gestión de seguridad de la información.
- Seguridad de la información.
- Definiciones y clasificación de los activos.
- Seguridad humana, seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de accesos.
- Gestión de continuidad del negocio.
- Conformidad y legalidad.

Examen UA 03

### **Unidad 4: Estrategias de seguridad.**

- Menor privilegio, defensa en profundidad, punto de choque y el eslabón más débil.

- o Menor privilegio.
- o Defensa en profundidad.
- o Punto en choque.
- o El eslabón más débil.
- Postura de fallo seguro, de negación establecida y de permiso establecido.
- Participación universal, diversificación de la defensa, y simplicidad.

Examen UA 04

### **Unidad 5: Exploración de las redes.**

- Exploración de la red.
- Inventario de una red. Herramientas del reconocimiento.
- NMAP y SCANLINE.
- Reconocimiento: limitar y explorar, exploración y enumerar

Examen UA 05

### **Unidad 6: Ataques remotos y locales.**

- Clasificación de los ataques.
- Ataques remotos en UNIX y ataques remotos sobre servicios inseguros en UNIX.
- o Ataques remotos en UNIX.
- Ataques locales en UNIX.
- ¿Qué podemos hacer si recibimos un ataque?

Examen UA 06

### **Unidad 7: Seguridad en redes inalámbricas.**

- Introducción a las redes inalámbricas y al estándar inalámbrico 802.11 – WIFI.
- Topologías.

- Seguridad en redes Wireless. Redes abiertas.
- WEP, Ataques WEP y otros mecanismos de cifrado.

Examen UA 07

### **Unidad 8: Criptografía y criptoanálisis.**

- Criptografía y criptoanálisis: introducción y definición.
- Cifrado y descifrado.
- Ejemplo de cifrado: relleno de una sola vez y criptografía clásica.
  - o Ejemplo de cifrado por relleno de una sola vez.
- Ejemplo de cifrado: criptografía moderna.
- Comentarios sobre claves públicas y privadas: sesiones.

Examen UA 08

### **Unidad 9: Autenticación.**

- Validación de identificación en redes y métodos de autenticación.
  - o Métodos de autenticación.
- Validación de identificación basada en clave secreta compartida: protocolo.
- Establecimiento de una clave compartida: intercambio de claves Diffie-Hellman.
- Validación de identificación usando un centro de distribución de claves y el protocolo de autenticación Kerberos.
- Validación de identificación de clave pública y protocolo de interbloqueo.

Examen UA 09

Examen final IFCT050PO