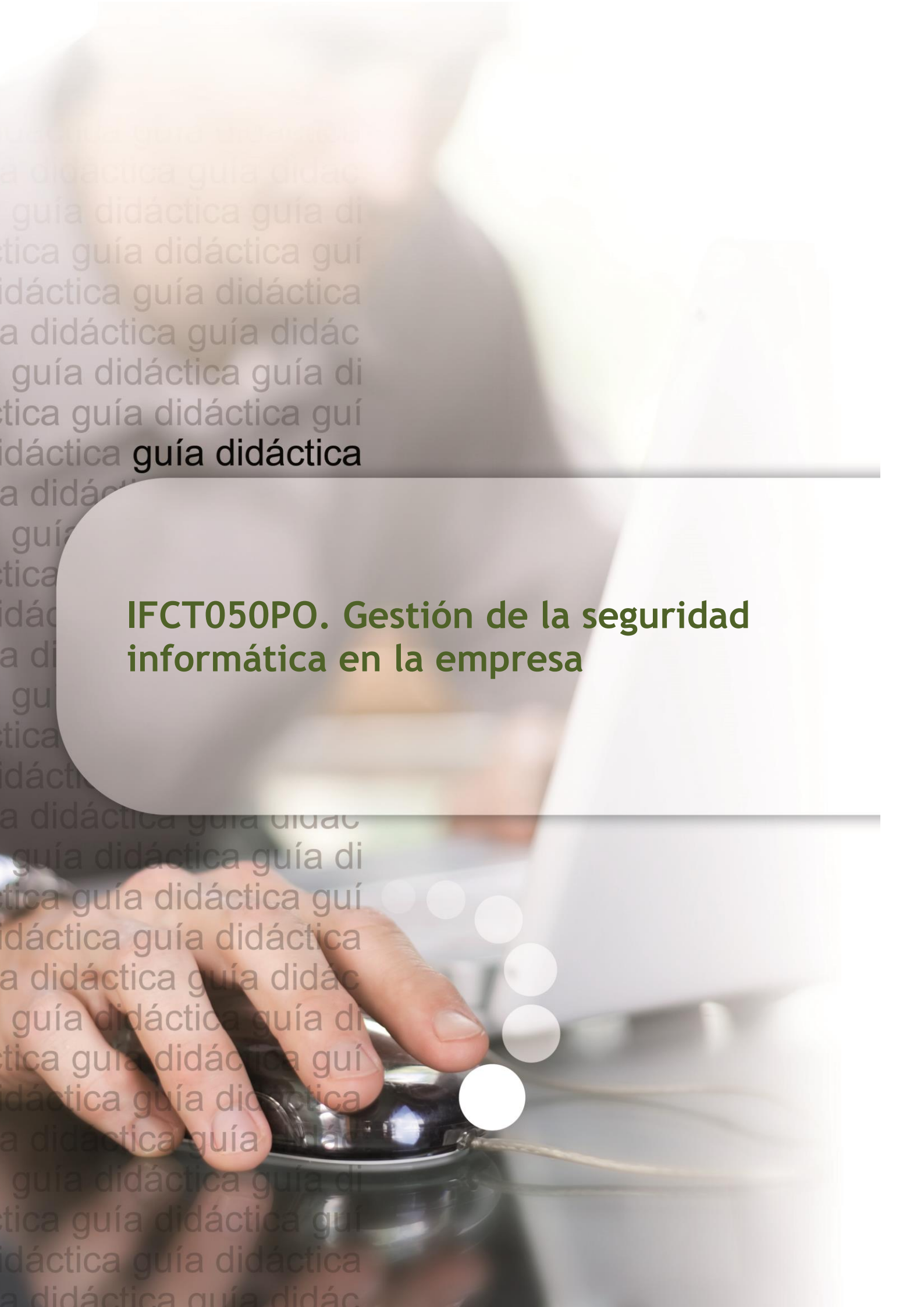

IFCT050PO. Gestión de la seguridad informática en la empresa

Objetivos

- **Objetivo General**

  - Gestionar la seguridad informática en la empresa.

- **Objetivos Específicos**

  - Aprender los principios y el ciclo de vida de la seguridad de la información.
  - Conocer las políticas de seguridad y las tácticas de ataque.
  - Saber qué es un hacker y un árbol de ataque.
  - Conocer las amenazas y vulnerabilidades de seguridad típicas.
  - Reflexionar sobre las buenas prácticas, las salvaguardas y las recomendaciones para la seguridad de red.
  - Conocer la importancia de las políticas de seguridad.
  - Saber qué debe contener una política de seguridad.
  - Aprender lo que no debe contener una política de seguridad.
  - Aprender a conformar una política de seguridad.
  - Reflexionar sobre la importancia de que se cumplan las decisiones sobre estrategia y políticas.
  - Saber qué es un sistema de gestión de seguridad de la información (SGSI).
  - Aprender el ciclo de mejora continua de un SGSI.
  - Conocer los activos de seguridad de un SGSI.
  - Aprender los controles más importantes de un SGSI.
  - Conocer las estrategias de seguridad más utilizadas.
  - Aprender qué es una red informática.
  - Saber realizar un inventario de red.
  - Conocer la exploración y el reconocimiento de red.
  - Aprender a limitar las posibilidades de éxito de un hacker.
  - Conocer cómo se realiza una evaluación de seguridad.
  - Aprender la clasificación de los ciberataques.
  - Conocer los ciberataques remotos y los locales.
  - Saber qué hacer ante un ciberataque.
  - Conocer el estándar 802.11 y sus topologías.
  - Reflexionar sobre la seguridad en las redes inalámbricas abiertas.
  - Conocer los mecanismos de cifrado y las vulnerabilidades de estos.
  - Conocer la criptografía y el criptoanálisis.
  - Aprender qué es el cifrado y el descifrado.
  - Conocer el cifrado de una sola vez y la criptografía clásica.

- Conocer la criptografía moderna.
- Reflexionar sobre claves públicas, privadas y sesiones.
- Conocer la validación de identificación en redes.
- Aprender los métodos de autenticación básicos.
- Conocer el intercambio de claves Diffie-Hellman.
- Aprender qué es un centro de distribución de claves y Kerberos.
- Conocer la validación de identificación de clave pública y el protocolo de interbloqueo.

Contenidos

IFCT050PO. Gestión de la seguridad informática en la empresa	Tiempo estimado

Unidad 1: Introducción a la seguridad.
• Introducción, modelo de ciclo de vida y principios de protección de la seguridad de la información.
  ○ 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.
  ○ Vulnerabilidades en los sistemas Windows.
• Buenas prácticas, salvaguardas y recomendaciones para la seguridad de la red.
  ○ Salvaguardas para la seguridad de la red.
  ○ Recomendaciones para la seguridad de una red.
	16,30 horas

Examen UA 01	**30 minutos**
Tiempo total de la unidad	**17 horas**
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.	**10,30 horas**
Examen UA 02	**30 minutos**
Tiempo total de la unidad	**11 horas**
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.	**14,30 horas**

• 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	**30 minutos**
Tiempo total de la unidad	**15 horas**

Unidad 4: Estrategias de seguridad.
• Menor privilegio, defensa en profundidad, punto de choque y el eslabón más débil.
  ○ Menor privilegio.
  ○ Defensa en profundidad.
  ○ Punto en choque.
  ○ El eslabón más débil.
• Postura de fallo seguro, de negación establecida y de permiso establecido.
• Participación universal, diversificación de la defensa, y simplicidad.
	9,30 horas

Examen UA 04	**30 minutos**
Tiempo total de la unidad	**10 horas**
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.	**7,30 horas**
Examen UA 05	**30 minutos**
Tiempo total de la unidad	**8 horas**
Unidad 6: Ataques remotos y locales. • Clasificación de los ataques. • Ataques remotos en UNIX y ataques remotos sobre servicios inseguros en UNIX. ○ Ataques remotos en UNIX. • Ataques locales en UNIX.	**8,30 horas**

• ¿Qué podemos hacer si recibimos un ataque?	
Examen UA 06	**30 minutos**
Tiempo total de la unidad	**9 horas**
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.	**7,30 horas**
Examen UA 07	**30 minutos**
Tiempo total de la unidad	**8 horas**
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. ○ Ejemplo de cifrado por relleno de una sola vez. • Ejemplo de cifrado: criptografía moderna. • Comentarios sobre claves públicas y privadas: sesiones.	**10,30 horas**
Examen UA 08	**30 minutos**
Tiempo total de la unidad	**11 horas**
Unidad 9: Autenticación. • Validación de identificación en redes y métodos de autenticación. ○ 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.	**9,30 horas**
Examen UA 09	**30 minutos**

Tiempo total de la unidad	**10 horas**
Examen final IFCT050PO	**1 hora**
9 unidades	**100 horas**