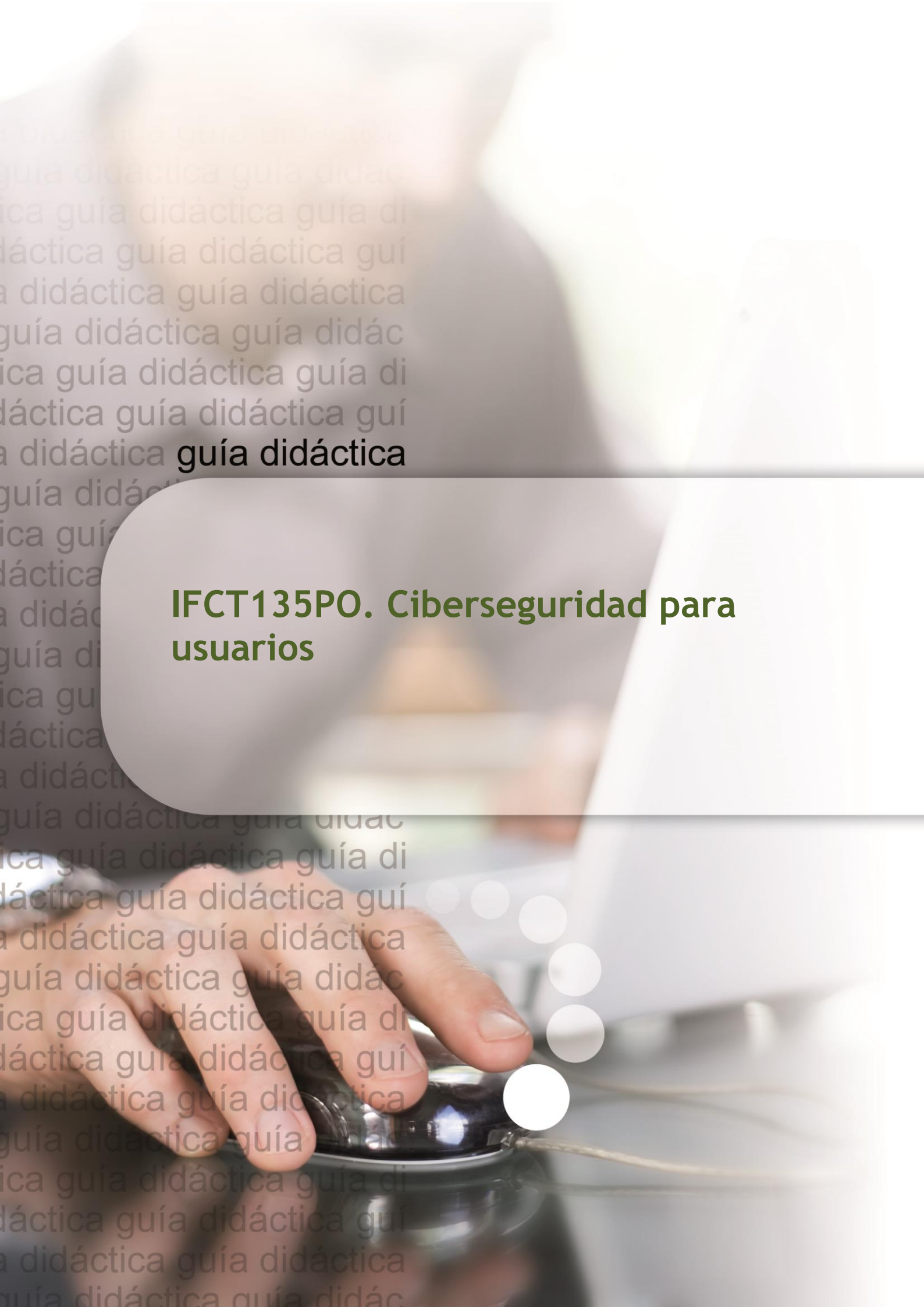

IFCT135PO. Ciberseguridad para usuarios

Objetivos

Objetivo General

- Valorar la necesidad de la gestión de la seguridad en las organizaciones. Conocer las principales amenazas a los sistemas de información e identificar las principales herramientas de seguridad y su aplicación en cada caso.

Objetivos Específicos:

- Conocer y asimilar los conceptos de seguridad en los sistemas de información, en función de la sociedad de la información.
- Estudiar los principales riesgos de seguridad, tipos de vulnerabilidades, fallos de programa, programas maliciosos, etc.
- Saber aplicar los principales estándares y buenas prácticas en materia de seguridad en sistemas de información.
- Conocer los conceptos en torno a la ciberseguridad.
- Analizar e identificar las amenazas más frecuentes en los sistemas de información.
- Estudiar los principales estándares que rigen la ciberseguridad.
- Comprender el significado e importancia de la criptografía.
- Estudiar los conceptos en torno al software dañino.
- Clasificar el tipo de software dañino según las características que presenta.
- Conocer la ingeniería y las redes sociales.
- Estudiar y conocer los mecanismos y sistemas de seguridad de las redes inalámbricas.
- Configurar la seguridad de la red inalámbrica.
- Conocer los mecanismos y sistemas de seguridad.
- Exponer diferentes medidas de protección para el acceso a los recursos y comunicaciones.
- Seguir unas correctas políticas de seguridad para poder establecer comunicaciones seguras.
- Estudiar las principales medidas de seguridad frente a código malicioso.

- **Contenidos**

10 HORAS	IFCT135PO. Ciberseguridad para usuarios
2 horas	❑ **Unidad 1:** Introducción a la seguridad en sistemas de formación. • Conceptos de seguridad en los sistemas • Clasificación de las medidas de seguridad • Requerimientos de seguridad en los sistemas de información
2 horas	❑ **Unidad 2:** Ciberseguridad. • Concepto de ciberseguridad • Amenazas más frecuentes a los sistemas de información • Tecnologías de seguridad más avanzadas • Gestión de la seguridad informática
2 horas	❑ **Unidad 3:** Software dañino. • Conceptos sobre software dañino • Clasificación del programa malicioso • Amenazas persistentes avanzadas • Ingeniería y redes sociales
2 horas	❑ **Unidad 4:** Seguridad en redes inalámbricas. • Seguridad en redes inalámbricas
2 horas	❑ **Unidad 5:** Herramientas de seguridad. • Medidas de protección • Control de acceso de los usuarios al sistema operativo • Gestión segura de comunicaciones, carpetas y otros recursos compartidos • Protección frente a código malicioso
10 horas	**5 unidades didácticas**