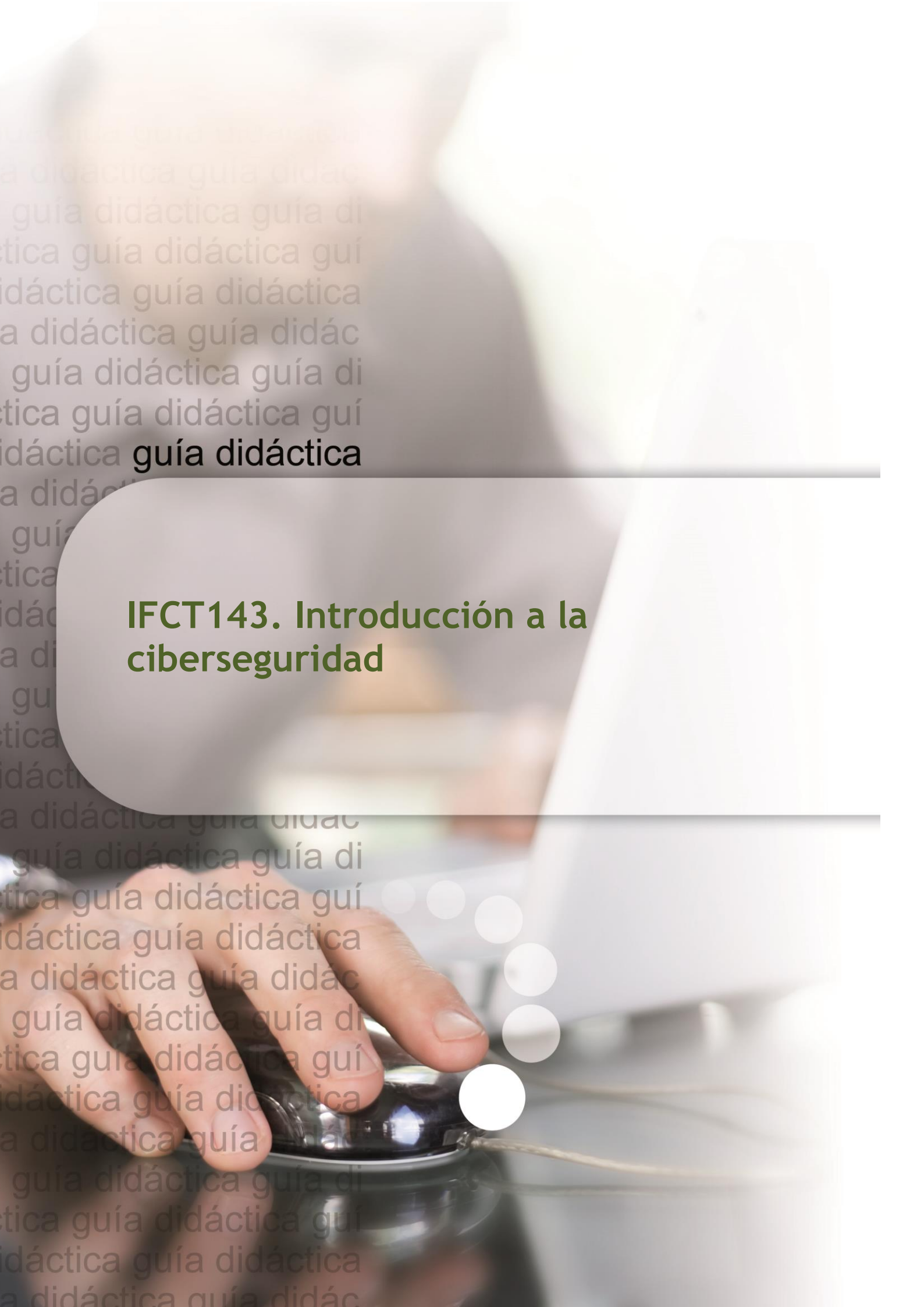


The background image is a blurred photograph of a person's hand clicking a computer mouse. Overlaid on the right side of the image is a vertical column of seven white circles of varying opacities, with the bottom circle being the most prominent. A semi-transparent grey rounded rectangle is positioned on the left side, containing the course title.

IFCT143. Introducción a la ciberseguridad

Objetivos

❑ **Objetivo general**

- Ofrecer de forma concisa una útil introducción al diseño de políticas de seguridad informática y en la implantación práctica de medidas tanto tecnológicas como metodológicas que prevendrán accidentes en relación al uso de tecnologías informáticas, o con los datos que con ellas se manejan, en nuestro negocio, empresa o institución.

❑ **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.
- Comprender los conceptos básicos de los dispositivos tamper-proof y su importancia en la seguridad de los sistemas.
- Aprender sobre las técnicas de side channel análisis y su aplicación en la evaluación de la seguridad de los dispositivos.
- Identificar las características y ventajas de las redes de radio definidas por software y las redes de radio cognitivas, y su relación con la seguridad.
- Analizar las diferentes técnicas de control de acceso para proteger los sistemas de accesos no autorizados.
- 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.
- Proporcionar una comprensión básica de los conceptos y tecnologías de interconexión remota de redes.
- Estudiar y conocer los mecanismos y sistemas de seguridad de las redes inalámbricas.
- Configurar la seguridad de la red inalámbrica.
- Conocer los conceptos de autenticación y autorización en el contexto de servicios web y aplicaciones.
- Analizar las vulnerabilidades comunes en la autenticación y autorización en servicios web y aplicaciones.
- Describir las ventajas de OAuth y OAuth2 en términos de autenticación y autorización.
- Brindar una introducción a los conceptos legales que son importantes en el mundo de la tecnología y la seguridad informática. Conocer los mecanismos y sistemas de seguridad.
- Conocer los conceptos básicos de la protección de datos, como la recopilación, el almacenamiento y la utilización de datos personales. Exponer diferentes medidas de protección para el acceso a los recursos y comunicaciones.
- Seguir unas correctas políticas de seguridad para poder establecer comunicaciones seguras.
- Proporcionar una comprensión de los conceptos básicos relacionados con la propiedad intelectual. Estudiar las principales medidas de seguridad frente a código malicioso.

Contenidos

Introducción a la ciberseguridad	Tiempo estimado
Unidad 1: Fundamentos. • Fundamentos de Seguridad. • Riesgos. • Amenazas. ○ Confidencialidad. ○ Integridad. ○ Disponibilidad.	
Examen UA 01	30 minutos
Actividad de Evaluación UA 01: Seguridad en los sistemas de información	30 minutos
Tiempo total de la unidad	4 horas
Unidad 2: Políticas de seguridad informática. • Gestión de la ciberseguridad. • Políticas de seguridad. • Medidas de protección. ○ Criptografía. ○ Sistemas SIEM. ○ Plataformas de administración de la movilidad empresarial (EMM). ○ Sistemas IDS.	
Examen UA 02	30 minutos
Actividad de Evaluación UA 02: Caso práctico	30 minutos
Tiempo total de la unidad	4.5 horas

Unidad 3: Seguridad física y seguridad lógica. • Dispositivos tamper-proof. • Side channel análisis. • Software Defined Radio y Cognitive Radio Networks. • Control de acceso. • Amenazas y software dañino.	
Examen UA 03	30 minutos
Tiempo total de la unidad	6 horas
Unidad 4: Acceso remoto. • Interconexión remota de redes. • Demostración práctica de distintas redes privadas virtuales. ○ Red en el hogar. ○ Configuración práctica de distintas redes privadas virtuales. ○ Red en el hogar. ○ Configuración de seguridad de una red Wi-Fi. ○ Configuración de seguridad avanzada. ○ Redes inalámbricas privadas. ○ Redes inalámbricas públicas. ○ HTTPS. ○ VPN. ○ Acceso desde dispositivos móviles.	
Examen UA 04	30 minutos
Actividad de Evaluación UA 04: Comprometer la seguridad de la empresa	30 minutos
Tiempo total de la unidad	3 horas
Unidad 5: Control de acceso a aplicaciones. • Autenticación y autorización en servicios WEB. • OAuth, OAuth2 y tokens.	
Examen UA 05	30 minutos
Tiempo total de la unidad	3 horas

Unidad 6: Aspectos legales. • Aspectos jurídicos en entornos tecnológicos. • Protección de datos y control de accesos. • Protección intelectual y licencias. • Protección frente a código maliciosa.	
Examen UA 06	30 minutos
Tiempo total de la unidad	4 horas
Examen final	30 minutos
6 unidades	25 horas