

The background image shows a person's hand using a computer mouse. On the right side, there is a vertical stack of seven white circles of varying sizes, with the largest one at the bottom. The text 'IFCT0024. Ciberseguridad para usuarios' is displayed in a dark green font within a semi-transparent grey rounded rectangle.

IFCT0024. 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

Ciberseguridad para usuarios	Tiempo estimado
<p>Unidad 1: Introducción y conceptos de seguridad en sistemas de información.</p> <ul style="list-style-type: none"> • Aproximación a la seguridad en sistemas de información • Clasificación de las medidas de seguridad. • Requerimientos de seguridad en los sistemas de información. Confidencialidad, integridad, disponibilidad 	
Examen UA 01	30 minutos
Actividad/es de Evaluación UA 01	30 minutos
Tiempo total de la unidad	2 horas
<p>Unidad 2: Conocimiento del ámbito de la Ciberseguridad para usuarios.</p> <ul style="list-style-type: none"> • Concepto de ciberseguridad. • Amenazas más frecuentes a los sistemas de información. • Tecnologías de seguridad más habituales. • Gestión de la seguridad informática. 	
Examen UA 02	30 minutos
Actividad/es de Evaluación UA 02	30 minutos
Tiempo total de la unidad	2 horas

<p>Unidad 3: Identificación de softwares dañinos.</p> <ul style="list-style-type: none"> • Conceptos sobre software dañino. • Clasificación del programa malicioso. • Amenazas persistentes avanzadas. • Ingeniería y redes sociales. 	
Examen UA 03	30 minutos
Actividad/es de Evaluación UA 03	30 minutos
Tiempo total de la unidad	2 horas
<p>Unidad 4: Gestión de seguridad en redes inalámbricas.</p> <ul style="list-style-type: none"> • Seguridad en redes inalámbricas. 	
Examen UA 04	30 minutos
Actividad/es de Evaluación UA 04	30 minutos
Tiempo total de la unidad	2 horas
<p>Unidad 5: Aplicación de herramientas de seguridad.</p> <ul style="list-style-type: none"> • 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. 	
Examen UA 05	30 minutos
Actividad/es de Evaluación UA 05	30 minutos
Tiempo total de la unidad	2 horas

Examen final / Evaluación final	30 minutos
5 unidades	10 horas