

A close-up photograph of a person's hand using a black computer mouse. The background is blurred, showing a computer monitor and keyboard. On the right side of the image, there is a vertical bar of seven white circles of varying sizes, with the bottom-most circle being the largest and brightest. The text 'IT Seguridad' is overlaid on a semi-transparent grey rounded rectangle on the left side of the image.

## IT Seguridad

## Objetivos

---

### □ **Objetivo General**

- En el presente curso el alumno conocerá los aspectos principales de la seguridad de la información: confidencialidad e integridad. Además, entre otros puntos muy importantes en seguridad, el alumno también aprenderá los hitos básicos de la criptografía: encriptación simétrica y asimétrica o algoritmos de cálculo. Para obtener la Certificación Oficial EUCIP IT Administrator, se han de realizar 5 exámenes, el quinto de ellos se corresponde con este módulo formativo.

### □ **Objetivos Específicos**

- Comprender los principales aspectos de la seguridad.
- Familiarizarnos con la evaluación de riesgos.
- Saber cómo gestionar la seguridad de la información.
- Identificar los organismos de normalización y sus estándares.
- Comprender qué es la criptografía y su importancia.
- Familiarizarnos con los métodos criptográficos simétricos y asimétricos.
- Saber qué son las funciones hash y para qué se utilizan.
- Conocer los usos de la criptografía.
- Comprender las definiciones de autenticación.
- Familiarizarnos con los diferentes métodos de autenticación existentes (passwords, tokens...).
- Saber cómo funciona la autenticación en redes.
- Conocer cómo se controla el acceso en una base de datos.
- Comprender la necesidad de tener la información siempre disponible.
- Familiarizarnos con los tipos de RAID que permiten duplicar un disco duro en tiempo real.
- Saber cómo funciona un sistema de balanceo de carga en red.

- Conocer cómo podemos automatizar la creación de backups y comprobar que funcionan correctamente.
- Comprender algunas vulnerabilidades de un ordenador.
- Familiarizarnos con la administración automática de archivos.
- Saber qué tipo de código automático puede afectar a nuestro sistema.
- Conocer los diferentes tipos de virus.
- Comprender las infraestructuras de clave pública y cómo funcionan.
- Familiarizarnos con los registros y certificados digitales.
- Saber qué son los certificados X.509.
- Conocer cómo funcionan los servicios LDAP.
- Comprender algunos conceptos básicos sobre telecomunicaciones y redes inalámbricas.
- Familiarizarnos con los controles de acceso HTTP y de correo electrónico.
- Saber gestionar los registros.
- Conocer cómo funcionan los cortafuegos y como detectar a intrusos.
- Comprender los conceptos básicos sobre privacidad.
- Familiarizarnos con algunos aspectos éticos sobre la seguridad informática.
- Conocer algunos aspectos legales de nivel europeo.

## Contenidos

IT Seguridad	Tiempo estimado
<p><b>Unidad 1:</b> Generalidades.</p> <ul style="list-style-type: none"> <li>• Conceptos básicos.</li> <li>• Gestión de riesgos.</li> <li>• Gestión de la seguridad de la información.</li> <li>• Estándares y organismos de normalización.</li> </ul>	
Examen UA 01	<b>30 minutos</b>
Actividad de Evaluación UA 01	<b>30 minutos</b>
Tiempo total de la unidad	<b>5 horas</b>
<p><b>Unidad 2:</b> Criptografía.</p> <ul style="list-style-type: none"> <li>• Generalidades.</li> <li>• Criptografía simétrica.</li> <li>• Criptografía asimétrica.</li> <li>• Funciones hash y resumen.</li> <li>• Comparativa entre métodos de encriptación.</li> <li>• Uso de la criptografía.</li> <li>• Aplicaciones.</li> </ul>	
Examen UA 02	<b>30 minutos</b>
Actividad de Evaluación UA 02	<b>30 minutos</b>
Tiempo total de la unidad	<b>5 horas</b>
<p><b>Unidad 3:</b> Autenticación y control de acceso.</p> <ul style="list-style-type: none"> <li>• Conceptos generales sobre la autenticación.</li> <li>• Passwords.</li> <li>• Token.</li> <li>• Biométrica.</li> <li>• Autenticación de red.</li> <li>• Control de acceso.</li> </ul>	
Examen UA 03	<b>30 minutos</b>

Actividad de Evaluación UA 03	<b>30 minutos</b>
Tiempo total de la unidad	<b>4 horas</b>
<p><b>Unidad 4:</b> Disponibilidad.</p> <ul style="list-style-type: none"> <li>• General.</li> <li>• Resiliencia.</li> <li>• Backup.</li> </ul>	
Examen UA 04	<b>30 minutos</b>
Actividad de Evaluación UA 04	<b>30 minutos</b>
Tiempo total de la unidad	<b>2 horas</b>
<p><b>Unidad 5:</b> Código malicioso.</p> <ul style="list-style-type: none"> <li>• Programas.</li> <li>• Administración automática de tipos de archivo.</li> <li>• Código descargable.</li> <li>• Software viral.</li> </ul>	
Examen UA 05	<b>30 minutos</b>
Actividad de Evaluación UA 05	<b>30 minutos</b>
Tiempo total de la unidad	<b>4 horas</b>
<p><b>Unidad 6:</b> Infraestructura de clave pública.</p> <ul style="list-style-type: none"> <li>• PKI.</li> <li>• Servicios de directorio.</li> </ul>	
Examen UA 06	<b>30 minutos</b>
Actividad de Evaluación UA 06	<b>30 minutos</b>
Tiempo total de la unidad	<b>3 horas</b>

<p><b>Unidad 7:</b> Seguridad de Red.</p> <ul style="list-style-type: none"> <li>• Conceptos básicos de las telecomunicaciones.</li> <li>• Redes inalámbricas.</li> <li>• Control de acceso.</li> <li>• Gestión de registros.</li> <li>• Control de acceso a servicios HTTP.</li> <li>• Control de acceso a servicios de correo electrónico.</li> <li>• Cortafuegos.</li> <li>• Detección de intrusiones.</li> <li>• Redes privadas virtuales.</li> </ul>	
Examen UA 07	<b>30 minutos</b>
Actividad de Evaluación UA 07	<b>30 minutos</b>
Tiempo total de la unidad	<b>7 horas</b>
<p><b>Unidad 8:</b> Aspectos sociales, éticos y legales de la seguridad informática.</p> <ul style="list-style-type: none"> <li>• Conceptos básicos.</li> <li>• PET´s.</li> <li>• Leyes europeas.</li> </ul>	
Examen UA 08	<b>30 minutos</b>
Actividad de Evaluación UA 08	<b>30 minutos</b>
Tiempo total de la unidad	<b>4 horas</b>
Examen final	<b>1 hora</b>
<b>8 unidades</b>	<b>35 horas</b>