	<p align="center"><b>IES HARÍA. DEPARTAMENTO DE INFORMÁTICA</b>  <b>Ciclo formativo:</b> Sistemas Microinformáticos y Redes  <b>Módulo:</b> 0226. Seguridad informática - <b>SGF</b>  <b>Curso:</b>2012-13</p>
---	--


<p><b>U.T. Nº2: Seguridad en el entorno físico</b></p>
<p><b>Horas: 20</b></p>
<p><b>Orientaciones</b></p> <p>A lo largo de esta unidad se comprenderá la importancia de la seguridad en el entorno físico (estancias, plantas y edificios) de un sistema de información.</p> <p>Se conocerán algunos sistemas de control de acceso a personas al recinto y sabremos cuál es la temperatura y la humedad idóneas, para las distintas áreas de equipamiento informático. Podremos conocer los riesgos de inundación y fuego y prevenirlos y comprenderás que el conocimiento de los puntos débiles de sistemas es fundamental.</p> <p>A lo largo de esta unidad veremos los conceptos básicos de seguridad en el entorno físico. Incidiendo en la seguridad activa como elemento de detección de riesgos.</p> <p>Además de comprender ciertos conceptos, esta unidad te ayudará a reflexionar sobre las medidas de seguridad a tomar teniendo en cuenta las características de la empresa que las solicita.</p> <p>Como ejemplo del lugar donde más medidas de seguridad deben ser tomadas se tomará un DATACENTER profundizando en cómo se controla el acceso a ellos con sistemas biométricos.</p> <p>En coordinación con el módulo de servicios se verán las vulnerabilidades, ataques y medidas de protección del servicio de DNS</p>
<p><b>Objetivos</b></p> <p>En esta unidad se alcanza el resultado de aprendizaje 3 del ciclo: "Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático".</p> <ul style="list-style-type: none"> <li>• Conocer las diferencias entre seguridad activa y pasiva.</li> <li>• Conocer los elementos físicos de la seguridad pasiva.</li> <li>• Conocer las mejores características para la ubicación física de los equipos informáticos.</li> <li>• Conocer la necesidad y características de los sistemas de alimentación ininterrumpida.</li> <li>• Conocer la importancia de otros elementos importantes para evitar perder el sistema informático y su información en caso de cualquier contingencia.</li> </ul>
<p><b>Criterios de evaluación</b></p>



- a) Diferencia los elementos de seguridad activa y seguridad pasiva en un sistema informático.
- b) Identifica los elementos del entorno involucrados en un sistema informático y las medidas de seguridad asociadas a los mismos
- c) Selecciona ubicaciones idóneas para los equipos informáticos, así como determina sus condiciones ambientales.
- d) Sabe diferenciar y selecciona los diferentes sistemas de control de acceso.
- e) Conoce las características de los CPD y reconoce las medidas de seguridad física especiales que hay que aplicar en los mismos
- f) Diferencia entre políticas, planes y procedimientos de seguridad y conoce los elementos necesarios para definir una correcta política de seguridad
- g) Conoce las vulnerabilidades del servicio de DNS aplica ataques y medidas de protección a dicho servicio

#### **Contenidos soporte**

- 1. Seguridad en el entorno físico.
  - 1. Acceso de personas al recinto.
  - 2. Alarma contra intrusos.
  - 3. Instalación eléctrica.
  - 4. Seguridad de materiales eléctricos y protección de personas frente a la electricidad.
  - 5. Condiciones ambientales: Humedad y temperatura.
  - 6. Enemigos de los ordenadores: Partículas de polvo, agua y fuego.
- 2. Centro de proceso de datos y su entorno físico.
  - 1. Infraestructura.
  - 2. Acceso.
  - 3. Redundancia.
- 3. Sistemas de control de acceso.
  - 1. Personal de vigilancia y control.
  - 2. Dispositivos de control de acceso en un datacenter.
  - 3. iButton, Touch memories o llaves electrónicas de contacto.
  - 4. Sistemas de reconocimiento de personas.
    - 1. Sistemas biométricos e identificación personal.
    - 2. Propiedades (ideales) de los rasgos biométricos.
    - 3. Sistemas biométricos más utilizados.
    - 4. Comparación de métodos biométricos.

	<p align="center"> <b>IES HARÍA. DEPARTAMENTO DE INFORMÁTICA</b>  <b>Ciclo formativo:</b> Sistemas Microinformáticos y Redes  <b>Módulo:</b> 0226. Seguridad informática - <b>SGF</b>  <b>Curso:</b>2012-13         </p>
---	--

4. Políticas, planes y procedimientos de seguridad.
  1. Elementos de las políticas de seguridad.
  2. Características deseables de las políticas de seguridad.
  3. Definición e implantación de las políticas de seguridad.
  4. Inventario y auditoría.
  5. Elementos de las políticas de seguridad.

**Contenidos organizadores:**

Servicio de DNS. Vulnerabilidades y ataques  
 Servicio de DNS. Medidas de protección  
 Almacenamiento redundante. DRBD  
 Alta disponibilidad de servicios. Heartbeat