

CONTENIDOS DEL CURSO / PRESTAKUNTZA EKINTZAREN EDUKIAK

DENOMINACION / IZENA:

Seguridad en Equipos Informáticos

1. INTRODUCCIÓN

A través del estudio de esta acción formativa, se pretende alcanzar como objetivo ofrecer un marco teórico-práctico sobre los aspectos didácticos de la Seguridad Informática.

Para ofrecer la máxima funcionalidad de los elementos curriculares – contenidos y actividades - , se presenta el curso con la siguiente estructura:

- **Contenidos:** En unidades didácticas (UD), prestando especial interés en los contenidos, procedimientos y actitudes.
- **Actividades:** Donde el docente dispondrá de una serie de ejercicios relacionados con cada unidad didáctica.

2. OBJETIVOS

- Establecen las capacidades que se espera al final del curso hayan desarrollado los y las asistentes.
- Estos objetivos expresan los resultados que deben ser alcanzados por los y las asistentes:
- Ofrecer un marco teórico-práctico sobre los aspectos didácticos de la seguridad informática.
- Conocer la diferencia y aplicar mecanismos de seguridad activa y pasiva en redes.
- Gestionar dispositivos de almacenamiento asegurando la integridad de la información.
- Conocer la normativa existente sobre seguridad informática.
- Implantar mecanismos de protección frente a posibles vulnerabilidades de los sistemas.
- Recuperar datos en sistemas afectados.
- Crear un espacio para la comunicación, el desarrollo e intercambio de experiencias en torno al uso, elaboración y aplicación de materiales didácticos relacionados con la seguridad informática.

3. CONTENIDOS

La manera de organizar, secuenciar y presentar los contenidos es decisiva, pues deben estar contextualizados, (al entorno del grupo, y en este caso, al perfil de que se trate), deben ser coherentes y lógicos para los alumnos/as y la metodología adecuada al tipo de conocimiento que se desea construir.

El aprendizaje no dependerá únicamente de la cantidad de información que se proporciona a los alumnos/as, sino también de las conexiones que estos logran establecer entre lo que ya saben y lo que desconocen.

3.1 UNIDADES DIDÁCTICAS

Unidad didáctica 1. Conceptos básicos de seguridad informática

3.1.1 Seguridad activa y pasiva.

3.1.2 Seguridad física y lógica.

Unidad didáctica 2. Gestión de la seguridad

3.2.1 Normativa y legislación.

3.2.2 LSSI.

3.2.3. LOPD.

Unidad didáctica 3. Gestión de dispositivos de almacenamiento

3.3.1 Políticas de seguridad

3.3.2 Almacenamiento redundante y distribuido

3.3.3 Almacenamiento remoto y extraíble

4. METODOLOGÍA

La actividad didáctica ha de ser pues, activa, favoreciendo el profesor que el alumno/a sea, de alguna manera, protagonista de su propio aprendizaje. Además, los contenidos de lo aprendido deben resultar "funcionales", se trata de utilizarlos en circunstancias reales de la vida cotidiana.

La metodología que se propone es la siguiente:

- En cada tema se desarrollan los siguientes tipos de actividades:
 - Actividades teórico-prácticas introductorias.
 - Actividades teórico-prácticas avanzadas.
- Procedimientos:
 - Evitar daños a Sistemas Informáticos.
 - Minimizar los efectos causados por un accidente.
 - Identificación de los distintos tipos de software malicioso.
 - Elaboración de un plan de seguridad.

Al finalizar cada unidad didáctica, se propondrá a los alumnos/as la resolución de actividades de enseñanza-aprendizaje, que faciliten la mejor comprensión del tema propuesto (aplicaciones prácticas, etc.)

5. MATERIALES Y RECURSOS DIDÁCTICOS

- Manual del curso.
- Ejercicios para practicar lo impartido en la teoría.
- Enlaces web de ayuda y profundización en la materia.
- Software necesario y adicional para conseguir llegar a los objetivos expuestos.
- Video tutoriales interactivos que faciliten el aprendizaje y la profundización en la materia fuera del horario de clase accesibles desde la web.