


The logo for HTS (Hotel Training School) consists of the letters 'HTS' in a bold, white, sans-serif font, set against a solid black rectangular background.

**HOTEL
TRAINING
SCHOOL**

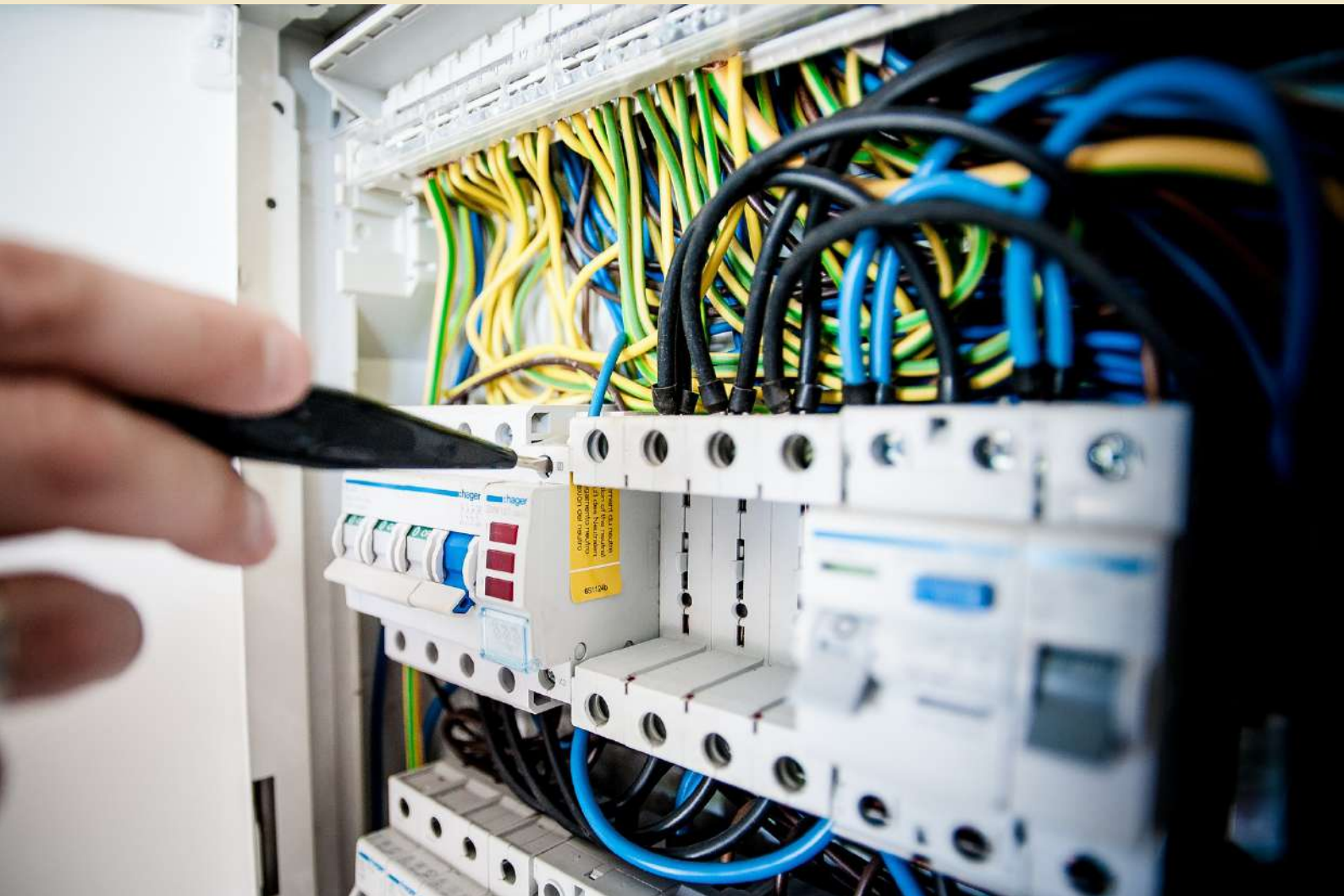
curso de
**SEGURIDAD
INFORMÁTICA
Y REDES**

60 HORAS 
duración

Ésta es el área que se enfoca en la protección de todo el aparato (incluyendo la información contenida). Para ello, existen una serie de estándares, protocolos, métodos y leyes para minimizar los posibles riesgos. Además, conocerás los criterios generales que comúnmente son aceptados sobre protección de los equipos. También, aprenderás sobre cómo implantarlo y cómo actuar en temas de defensa física e industrial de los sistemas y la lógica. Finalmente, conocerás los diferentes tipos existentes de redes que existen en el mercado actual adaptado a cada necesidad.

OBJETIVOS

- Conocer los criterios generales comúnmente aceptados sobre seguridad de los equipos informáticos.
- Aprender sobre el plan de implantación de seguridad informática.
- Saber cómo actuar en temas de seguridad física e industrial de los sistemas y la seguridad lógica.
- Aprender sobre los diferentes tipos de redes.



CONTENIDO

1 *criterios sobre seguridad de los equipos informáticos*

- 1.1 Modelo de seguridad orientado a la gestión del riesgo.
- 1.2 Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes.
- 1.3 Salvaguardas y tecnologías de seguridad habituales.
- 1.4 Gestión de la seguridad informática.

2 *plan de implementación de seguridad*

- 2.1 Seguridad existente de los sistemas VS. a la necesaria.
- 2.2 Selección de medidas de salvaguarda.
- 2.3 Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas.

3 *seguridad física e industrial de los sistemas*

- 3.1 Perímetros de seguridad física.
- 3.2 Sistemas de control de acceso físico frecuentes.
- 3.3 Criterios de seguridad para el emplazamiento físico.
- 3.4 Calidad y continuidad del suministro eléctrico.
- 3.5 Requerimientos de climatización y protección contra incendios.
- 3.6 Normativa de seguridad física e industrial.
- 3.7 Sistemas de ficheros más frecuentes.
- 3.8 Control de accesos a la red de comunicaciones.
- 3.9 Políticas y directivas del directorio de usuarios.
- 3.10 Listas de control de acceso (ACLs) a ficheros.
- 3.11 Altas, bajas y modificaciones de usuarios.
- 3.12 Requerimientos de seguridad relacionados con el control de acceso de los usuarios.
- 3.13 Sistemas de autenticación de usuarios débiles, fuertes y biométricos.
- 3.14 Registros de auditoría del sistema operativo.
- 3.15 Normativa de control de accesos a los sistemas.

4 *redes glámbricas o cableadas*

- 4.1 Introducción.
- 4.2 Definiciones.
- 4.3 Características de la red local.
- 4.4 Medio de transmisión.
- 4.5 Capacidad del medio: ancho de banda.
- 4.6 Topología.
- 4.7 Método de acceso.
- 4.8 El modelo de referencia OSI.
- 4.9 Datagramas.
- 4.10 Protocolos.

5 *elementos hardware en una red*

- 5.1 Elementos Hardware de una red
- 5.2 ¿Cómo construir una red y compartir un acceso a Internet?

6 *internet*

- 6.1 Internet: una red de redes.
- 6.2 ¿Cómo se transmite la información en Internet?
- 6.3 El sistema de nombres por dominio.
- 6.4 Formas de acceder a Internet.
- 6.5 Seguridad en comunicaciones.