

Este curso tiene como objetivo principal conocer los aspectos básicos para un correcto uso de Internet, así como realizarlo de forma segura. Gracias a esto, el discente podrá conocer los ataques que pueda sufrir, así como saber cómo actuar ante dichos ataques.

Al finalizar el curso, el alumno será capaz de:

- Estudiar aspectos básicos de la ciberseguridad.
- Usar de forma adecuada dispositivos digitales.
- Conocer la normativa que regula la ciberseguridad en la empresa.
- Estudiar aspectos acerca del tratamiento de la información y cómo tratarla de forma segura.
- Formarse acerca de diferentes amenazas cibernéticas.
- Aprender a navegar de forma segura.

Unidad 1. LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

1. El concepto de ciberseguridad
2. Conceptos de seguridad en los sistemas
3. Medidas de seguridad informática
4. Diferencia entre seguridad de la información y seguridad informática
5. Tecnologías de seguridad más habituales

Unidad 2. NORMATIVA QUE REGULA LA SEGURIDAD DE LA INFORMACIÓN

1. Normativa internacional sobre la seguridad de la información
2. Legislación española sobre seguridad de la información
3. Instituto Nacional de Ciberseguridad (INCIBE)
4. Aplicación de la LOPD en seguridad informática

Unidad 3. TRATAMIENTO DE LA INFORMACIÓN

1. Clasificación de la información
2. Dimensiones de la información (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad)
3. Los salvaguardas: tipos
4. Los soportes de la información: tipos y características

Unidad 4. MEDIDAS DE SEGURIDAD

1. Medidas de seguridad para aplicar a los soportes de la información
2. Contraseñas robustas
3. Archivo de la documentación en papel
4. Otras medidas

Unidad 5. NAVEGAR POR INTERNET

1. Principales riesgos de navegar por Internet
2. Virus y antivirus
3. Navegar por Internet de forma segura
4. Certificados de seguridad. Tipos
5. Control de la navegación en Internet

Unidad 6. LOS ATAQUES CIBERNÉTICOS

1. Qué son los ataques cibernéticos
2. ¿Quién hay detrás de un ataque?
3. Principales riesgos cibernéticos
4. Principales amenazas cibernéticas
5. Consecuencias
6. ¿Qué hacer frente a un ataque cibernético?
7. Qué es el Password Cracking
8. Las auditorías wifi
9. Exploits
10. Malware