TITULO: Ciberseguridad

HORAS: 57

OBJETIVOS GENERALES:

- ✓ Conocer los diferentes conceptos de seguridad
- ✓ Conocer la procedencia de los ataques informáticos y sus fases
- ✓ Dominar las medidas de seguridad existentes según los recursos a proteger, el momento en el que se produce la seguridad o según los elementos sobre los que se aplicarán las medidas de seguridad.
- ✓ Conocer los diferentes malware que pueden dañar y/o proporcionar acceso al sistema.
- ✓ Aprender qué es y de qué se compone el Sistema de Gestión de Seguridad de la Información (SGSI)
- ✓ Conocer qué es, para qué son importantes y qué debe contener una política de seguridad
- ✓ Diferenciar los softwares dañinos existentes.

CONTENIDOS

Capítulo 1. Introducción a la seguridad en los sistemas informáticos

1. Conceptos de seguridad
2. Clasificación de las medidas de seguridad
   2.1. Según el recurso a proteger
   2.2. Según el momento de su puesta en marcha 2.3. Según el tipo de elemento a proteger
3. Requerimientos de seguridad 3.1. Principales características 3.2. Otras características 3.3. Tipos de ataques

Capítulo 2. Ciberseguridad

1. Conceptos de ciberseguridad
2. Amenazas más frecuentes a los sistemas de información 2.1. Síntomas de equipo infectado
3. Tecnologías de seguridad más habituales
4. Gestión de la seguridad informática 4.1. Políticas de seguridad
5. Otros conceptos sobre seguridad informática 5.1. Spam
   5.2. Phishing

Capítulo 3. Software dañino

1. Conceptos sobre software dañino
2. Clasificación del software dañino 2.1. Virus
   2.2. Gusanos o worm
   2.3. Bombas lógicas
   2.4. Troyanos
   2.5. Spyware
   2.6. Keylogger
   2.7. Adware
   2.8. Zombie
   2.9. Exploit
   2.10. Ransomware
   2.11. Otros malware
3. Amenazas persistentes y avanzadas
4. Ingeniería social y redes sociales

Capítulo 4. Herramientas de seguridad

1. Medidas de protección
2. Control de acceso
   2.1. Permisos de los usuarios 2.2. Registro de usuarios
   2.3. Autenticación de usuarios

3. Gestión segura
   3.1. Gestión de carpetas compartidas en Red 3.2. Tipos de accesos a carpetas compartidas 3.3. Compartir impresoras

4. Protección frente a código malicioso 4.1. Antivirus
   4.2. Cortafuegos (firewall)
   4.3. Antimalware