

Unidad 4 – Seguridad Protección frente al Software Malicioso.
Seguridad Informática
2º SMR – IES Camas – Curso 24-25

Ejercicios

1. Clasificación de Malware

- a) Define el término **malware**.
- b) Enumera y describe brevemente cinco tipos de malware (por ejemplo: virus, gusanos, troyanos, ransomware, spyware), explicando las diferencias fundamentales entre ellos.
- c) Indica un ejemplo de situación real (caso práctico) en la que cada tipo de malware podría afectar a un sistema informático.

2. Análisis de Casos Prácticos:

Analiza la siguiente situación:

- Una empresa sufre un ataque en el que varios equipos comienzan a mostrar mensajes pidiendo un rescate en bitcoins a cambio de devolver el acceso a los archivos.
 - a) ¿De qué tipo de malware se trata?
 - b) Explica brevemente cómo se propaga este tipo de malware y cuál podría ser la principal vía de infección.
 - c) Propón dos medidas preventivas para evitar este tipo de infección en el futuro.

3. Verificación de Autenticidad:

- a) Explica por qué es importante descargar software únicamente de los sitios oficiales del fabricante o a través de repositorios confiables.
- b) Describe dos métodos para verificar la autenticidad de un archivo de instalación (por ejemplo, verificar la firma digital o comparar el hash del archivo con el proporcionado por el desarrollador).
- c) Menciona las consecuencias de instalar software de origen desconocido sin verificar su integridad.

4. Importancia de las Actualizaciones:

- a) ¿Por qué mantener el sistema operativo y las aplicaciones actualizadas ayuda a prevenir la infección por software malicioso?
- b) Explica cómo las actualizaciones corrigen vulnerabilidades y por qué esto es crucial para la seguridad.