EJERCICIO – SIMULACIÓN DE INVESTIGACIÓN DE INCIDENTE – RECOGIDA DE EVIDENCIAS

En una empresa que dispone de equipos de sobremesa y portátiles para sus empleados, se utiliza un entorno Windows con múltiples usuarios gestionados mediante un sistema centralizado (similar a Active Directory).

Un lunes por la mañana, uno de los equipos de la organización comienza a presentar los siguientes comportamientos:

- Rendimiento extremadamente lento
- Aparición de mensajes de error del sistema
- Bloqueos frecuentes de aplicaciones
- Actividad inusual del disco duro

El equipo afectado es utilizado habitualmente por varios usuarios.

Desde el departamento de ciberseguridad, se sospecha que el sistema podría estar comprometido. Entre las posibles causas se consideran:

- Ejecución de un archivo malicioso descargado de Internet
- Apertura de un correo electrónico con contenido malicioso
- Uso de un dispositivo USB (pendrive) infectado
- Acceso a páginas web comprometidas

Uno de los aspectos más importantes es **determinar el posible vector de entrada del incidente**.

TAREA DEL ALUMNADO

Como responsable de ciberseguridad, debes definir **la estrategia a seguir para la recopilación y almacenamiento de evidencias**, teniendo en cuenta las buenas prácticas estudiadas.

Cuestiones a responder

1. ¿Qué acciones realizarías en primer lugar al detectar el incidente?
2. ¿Qué tipo de evidencias recogerías en este caso?
3. ¿Qué datos consideras más volátiles y cuáles menos volátiles?
4. ¿Cómo garantizarías la integridad de las evidencias recopiladas?
5. ¿Qué precauciones tomarías para no alterar las evidencias?
6. ¿Utilizarías herramientas del propio sistema comprometido? Justifica tu respuesta.
7. ¿Cómo almacenarías las evidencias para su posterior análisis?

- Justifica todas tus decisiones
- Ten en cuenta la **cadena de custodia**

- No es necesario realizar el análisis, solo la **recogida y preservación de evidencias**

El escenario se sitúa en un instituto público de educación secundaria con aproximadamente 800 alumnos, 80 profesores y 10 miembros del personal de administración y servicios.

El centro dispone de una infraestructura informática distribuida en varias aulas de informática, equipos en sala de profesores, administración y portátiles asignados al profesorado. Todos los sistemas utilizan un entorno Windows gestionado de forma centralizada mediante Active Directory.

La gestión de usuarios se organiza en diferentes grupos:

- Alumnos: cuentas con permisos limitados, acceso a carpetas de asignaturas y uso restringido de aplicaciones.
- Profesores: acceso a recursos docentes, carpetas compartidas por departamentos y herramientas de gestión académica.
- Administración: acceso a aplicaciones de gestión interna y datos sensibles.
- Administradores TIC: control total del sistema, gestión de usuarios, equipos y servicios.

Los recursos del centro se organizan mediante un servidor de archivos con carpetas compartidas estructuradas por materias y departamentos. El acceso se controla mediante permisos asignados a grupos del directorio activo.

El centro dispone además de varios servicios:

- Servidor web interno basado en Apache HTTP Server para contenidos educativos.
- Servidor de archivos con almacenamiento centralizado.
- Servicio de autenticación y control de acceso mediante Active Directory.
- Sistema de copias de seguridad periódicas.
- Red segmentada con separación entre alumnado, profesorado y administración.

Este entorno permite la gestión centralizada de usuarios y recursos, pero también introduce riesgos si no se controlan adecuadamente los accesos y el uso de dispositivos externos.