3.7 Seguridad e Integridad

Trabajo de Investigación

Introducción

La seguridad e integridad de la información son elementos fundamentales en cualquier sistema operativo. Estas permiten proteger los datos, garantizar el correcto funcionamiento del equipo y evitar pérdidas de información por fallas, errores o accesos no autorizados. En este trabajo se desarrollan los subtemas: **Planificación de seguridad**, **Planificación y ejecución de mantenimiento**, y **Mecanismos de recuperación ante fallos**, cada uno con su definición, un ejemplo y una actividad práctica.

3.7.1 Planificación de Seguridad

Definición

La planificación de seguridad es el proceso de crear estrategias, normas y medidas para proteger los datos, los usuarios y los recursos de un sistema. Incluye la creación de políticas de contraseñas, asignación de permisos, protección contra malware, copias de seguridad y supervisión del sistema.

Ejemplo

En una oficina se implementa un plan de seguridad que establece lo siguiente:

- Contraseñas seguras con al menos 10 caracteres.
- Permisos de acceso según el nivel de cada empleado.
- Copias de seguridad automáticas cada 24 horas.
- Antivirus actualizado semanalmente.

Estas medidas evitan accesos no autorizados y posibles pérdidas de datos.

Actividad

Actividad 1: Elaboración de un Plan Básico de Seguridad
El estudiante deberá crear un documento donde especifique:

1. Reglas para crear contraseñas seguras.
2. Clasificación de carpetas en privadas, compartidas y públicas.
3. Proceso a seguir en caso de detectar un virus.
4. Frecuencia de las copias de seguridad.

El documento deberá entregarse en una cuartilla.

3.7.2 Planificación y Ejecución de Mantenimiento

Definición

La planificación y ejecución del mantenimiento consiste en organizar y realizar tareas preventivas o correctivas para asegurar el funcionamiento óptimo del sistema operativo. Incluye la actualización de software, limpieza del hardware, revisión de fallas y reparación de errores.

Ejemplo

En una institución educativa se programan dos tipos de mantenimiento:

- **Preventivo mensual:** limpieza interna, actualización de drivers y sistema operativo, revisión de ventiladores.
- **Correctivo:** atención a computadoras que presentan fallas como reinicios inesperados o errores durante el arranque.

Estas acciones mantienen los equipos funcionando por más tiempo y evitan daños mayores.

Actividad

Actividad 2: Elaboración de un Plan de Mantenimiento
El estudiante deberá crear una tabla con 10 computadoras, donde especifique:

- Tipo de mantenimiento (preventivo o correctivo).
- Fecha del mantenimiento.
- Responsable asignado.
- Actividad a realizar.

La tabla puede elaborarse en Excel o en un documento escrito.

3.7.3 Mecanismos de Recuperación ante Fallos (FS, Procesadores, Memoria)

Definición

Los mecanismos de recuperación ante fallos son herramientas y procedimientos utilizados por los sistemas operativos para restablecer su funcionamiento después de una falla. Estos mecanismos actúan en:

a) Sistema de archivos (FS)

Incluyen copias de seguridad, sistemas de archivos con journaling (como NTFS o ext4) y restauración de versiones anteriores.

b) Procesadores

Comprenden técnicas como el multiprocesamiento, reasignación de procesos y modos de arranque seguro que permiten al sistema seguir funcionando aun después de un error.

c) Memoria

Incluyen memorias ECC que corrigen errores, técnicas de paginación y mecanismos de restauración del estado previo del sistema.

Ejemplo

Una computadora experimenta un apagón inesperado. Al encenderla de nuevo:

- El sistema de archivos NTFS repara automáticamente archivos dañados mediante su registro (journaling).
- Windows ofrece restaurar el sistema a un punto anterior.
- La memoria reconstruye el último estado seguro del sistema.

Gracias a estos mecanismos, el usuario puede continuar trabajando sin perder información importante.

Actividad

Actividad 3: Investigación y Evidencia de Herramientas de Recuperación
El estudiante deberá investigar y describir en media cuartilla los siguientes mecanismos en su propio equipo:

- Restaurar sistema.
- Historial de archivos o copias de seguridad.
- Comprobación de unidad (chkdsk).

Además, deberá incluir una captura de pantalla de alguna de estas herramientas como evidencia.

Conclusión

La seguridad e integridad en los sistemas operativos permiten garantizar el funcionamiento estable, la protección de los datos y la recuperación de la información ante fallas. La planificación adecuada, el mantenimiento oportuno y los mecanismos de recuperación son elementos esenciales para mantener la continuidad operativa en cualquier entorno tecnológico.