

MODULO 2 – Capítulo 5

Clonación

¿Qué es la clonación de un sistema informático?

La clonación consiste en copiar un disco duro o una partición completa, incluyendo el sistema operativo, aplicaciones, configuraciones y archivos, para crear una réplica exacta que puede transferirse a otro disco o usarse como respaldo.

¿Cuándo se usa?

- Para migrar un sistema operativo y datos a un disco nuevo (ej. actualizar de HDD a SSD).
- Implementar múltiples equipos con la misma configuración (clonación en masa).
- Recuperar un sistema después de fallos graves.

¿Para qué sirve?

- Facilita restaurar un sistema en su estado exacto.
 - Asegura uniformidad en configuraciones en entornos empresariales.
 - Simplifica el cambio de hardware.
-

Diferencia entre clon y una imagen

- **Clon:** Es una copia exacta y funcional del disco duro. Puede usarse inmediatamente, ya que incluye el sistema de arranque.
 - **Imagen:** Es un archivo comprimido que contiene los datos del disco. Necesita ser restaurada antes de usarse y ocupa menos espacio.
-

¿Qué es el backup y en qué se diferencia de la clonación?

- **Backup (copia de seguridad):** Copia de archivos o datos importantes que pueden restaurarse en caso de pérdida o daño. No incluye necesariamente el sistema operativo o configuración.
 - **Diferencias:**
 - **Backup:** Protección de datos específicos (documentos, fotos). Es incremental o diferencial.
 - **Clonación:** Reproducción exacta de un disco completo.
-

Recomendaciones para usar la clonación y el backup

- **Clonación:**
 - Úsala para migrar sistemas o crear réplicas completas de discos.
 - Realiza el proceso en sistemas desconectados para evitar inconsistencias.

- Almacena los discos clonados en un lugar seguro.
 - **Backup:**
 - Programa copias regulares para mantener datos actualizados.
 - Usa herramientas que soporten encriptación para proteger la información.
 - Realiza pruebas periódicas de recuperación.
-

Pasos para realizar copia de seguridad en Windows 10 y Windows 11

1. **Acceder al panel de copias de seguridad:**
 - Ve a *Configuración > Actualización y seguridad > Copia de seguridad* (Windows 10).
 - En Windows 11, ve a *Configuración > Sistema > Almacenamiento > Copia de seguridad*.
 2. **Activar y configurar:**
 - Selecciona "Agregar una unidad" y elige el disco donde guardarás la copia.
 - Activa el "Historial de archivos".
 3. **Elegir qué respaldar:**
 - Personaliza las carpetas a incluir.
 4. **Automatización:**
 - Configura la frecuencia de copias (por defecto cada hora).
-

¿Qué es el historial de archivos?

El historial de archivos es una función de Windows que realiza copias automáticas de archivos almacenados en carpetas como *Documentos*, *Imágenes*, y *Escritorio*. Permite restaurar versiones anteriores en caso de pérdida o modificación accidental.

Herramientas de terceros para clonación

Privativas:

- **Acronis True Image:** Potente, con opciones avanzadas de copia en la nube.
- **Macrium Reflect:** Popular para usuarios empresariales y domésticos.
- **EaseUS Todo Backup:** Intuitiva y con múltiples opciones.

Libres:

- **Clonezilla:** Gratuita, ideal para clonar discos y particiones.
 - **Redo Rescue:** Sencilla y efectiva para recuperación y clonación.
 - **dd (Linux):** Comando para clonar discos directamente.
-

Herramientas de terceros para backup

Privativas:

- **AOMEI Backupper:** Copias de seguridad y sincronización en tiempo real.
- **Carbonite:** Backup en la nube, ideal para pequeñas empresas.
- **Paragon Backup & Recovery:** Versátil y fácil de usar.

Libres:

- **Duplicati:** Copias encriptadas, ideal para almacenamiento remoto.
- **Bacula:** Completa y robusta para sistemas grandes.
- **rsync (Linux):** Herramienta para sincronización y respaldo.

Tipos de Backup

Existen diferentes tipos de backups según el método y los datos a guardar:

Tipo	Descripción	Ventajas	Desventajas
Completo	Copia de todos los datos seleccionados.	Restauración rápida y sencilla.	Toma más tiempo y espacio de almacenamiento.
Incremental	Copia solo los cambios realizados desde el último backup (ya sea completo o incremental).	Rápido y ocupa menos espacio.	Restauración más lenta, requiere múltiples backups.
Diferencial	Copia los cambios realizados desde el último backup completo.	Más rápido que completo, más fácil de restaurar que incremental.	Consume más espacio con el tiempo.
Espejo	Replica exacta de los datos seleccionados, sin compresión ni historiales.	Acceso inmediato a datos.	Sin historial ni versiones antiguas.
Snapshot	Captura del estado del sistema o datos en un momento específico.	Ideal para bases de datos y máquinas virtuales.	Puede requerir software/hardware específico.
Incremental Forever	Backup inicial completo seguido de incrementales continuos, consolidando backups más antiguos para ahorrar espacio.	Eficiencia a largo plazo.	Configuración compleja.

Plan de Backup de Dos Semanas

Un plan ideal debe alternar entre backups completos e incrementales para garantizar eficiencia y seguridad:

Día	Tipo de Backup	Datos Respaldados	Ubicación	Frecuencia
Lunes (S1)	Completo	Todos los datos críticos	Disco externo 1	Semanal
Martes	Incremental	Cambios desde el lunes	Nube	Diario
Miércoles	Incremental	Cambios desde el martes	Nube	Diario
Jueves	Incremental	Cambios desde el miércoles	Disco externo 2	Diario

Día	Tipo de Backup	Datos Respaldados	Ubicación	Frecuencia
Viernes	Diferencial	Cambios desde el lunes	Nube	Semanal
Sábado	Incremental	Cambios desde el viernes	Nube	Diario
Domingo	Sin respaldo	---	---	---
Lunes (S2)	Completo	Todos los datos críticos	Disco externo 2	Semanal
Resto de días	Similar a S1			

Cómo Restaurar el Backup

1. Identificar el backup más reciente:

- Si es **completo**, úsalo directamente.
- Si es **incremental o diferencial**, restaura primero el último backup completo, luego los diferenciales o incrementales en orden.

2. Usar herramientas adecuadas:

- Windows tiene herramientas integradas como "Historial de Archivos".
- Usar software de terceros si el plan se configuró con ellos (p. ej., AOMEI, Macrium Reflect).

3. Verificar la restauración:

- Confirma la integridad de los datos restaurados.
 - Asegúrate de que los permisos y configuraciones sean correctos.
-

Normas de Buenas Prácticas para el Backup Empresarial

1. Regla 3-2-1:

- Mantén 3 copias de datos (1 principal y 2 de respaldo).
- Usa 2 tipos diferentes de almacenamiento (local y remoto).
- Almacena 1 copia fuera del sitio.

2. Automatiza el proceso:

- Programa respaldos automáticos para minimizar el error humano.

3. Encriptación:

- Protege los datos respaldados con cifrado, especialmente si están en la nube.

4. Prueba de restauración:

- Verifica periódicamente que los backups puedan restaurarse con éxito.

5. Segmentación de datos:

- Clasifica datos según su criticidad y establece prioridades de respaldo.

6. Documentación:

- Lleva un registro detallado de la estrategia de backup y las configuraciones.