Debido a que los archivos se mantienen tanto en memoria principal como en el disco, debemos asegurarnos de que un fallo del sistema no de por resultado la perdida de datos o inconsistencia en los mismos.

La destrucción de la información, ya sea accidental o intencional, es una realidad y tiene distintas causas:

* Fallas de hardware y de software
* Fenómenos meteorológicos atmosféricos
* Fallas en el suministro de energía
* Incendios e inundaciones
* Robos, vandalismo (incluso terrorismo)

Esta posible destrucción de la información debe ser tenida en cuenta por:

* Los sistemas operativos en general
* Los sistemas de archivos en particular

Una técnica muy usada para asegurar la disponibilidad de los datos es realizar respaldos periódicos:

1. Hacer con regularidad una o más copias de los archivos y colocarlas en lugar seguro.
2. Todas las actualizaciones realizadas luego del último respaldo pueden perderse.

Otra técnica es pasar todas las transacciones a un archivo, copiándolas en otro disco:

* Genera una redundancia que puede ser costosa
* En caso de fallas en el disco principal, puede reconstruirse todo el trabajo perdido si el disco de reserva no se dañó también

También existe la posibilidad del respaldo incremental:

* Durante una sesión de trabajo los archivos modificados quedan marcados.
* Cuando un usuario se retira del sistema (deja de trabajar), un proceso del sistema efectúa el respaldo de los archivos marcados.

Se debe tener presente que es muy difícil garantizar una seguridad absoluta de los archivos.

El método correcto de manejar fallos consiste básicamente en detectarlos a tiempo y de forma correcta. La inclusión de equipos de test en el sistema es esencial para mantener esta capacidad de monitorización.

En cualquier caso, la caída total o parcial del sistema se puede subsanar en parte si hay puntos de restauración del sistema (chkpt). Esta posibilidad aumenta la disponibilidad de recuperación en caso de fallos.

Mecanismos de Protección

**Dominios de Protección**

Muchos objetos del sistema necesitan protección, tales como la cpu, segmentos de memoria, unidades de disco, terminales, impresoras, procesos, archivos, bases de datos, etc.

Cada objeto se referencia por un nombre y tiene habilitadas un conjunto de operaciones sobre él.

Un dominio es un conjunto de parejas (objeto, derechos):

* + Cada pareja determina:
		- Un objeto.
		- Un subconjunto de las operaciones que se pueden llevar a cabo en él.

Un derecho es el permiso para realizar alguna de las operaciones. Es posible que un objeto se encuentre en varios dominios con “distintos” derechos en cada dominio.

Un proceso se ejecuta en alguno de los dominios de protección:

* Existe una colección de objetos a los que puede tener acceso.
* Cada objeto tiene cierto conjunto de derechos.

Una forma en la que el S. O. lleva un registro de los objetos que pertenecen a cada dominio es mediante una matriz :

* Los renglones son los dominios.
* Las columnas son los objetos.
* Cada elemento de la matriz contiene los derechos correspondientes al objeto en ese dominio, por ej.: leer, escribir, ejecutar.

**Listas Para Control de Acceso**

Las “matrices de protección” son muy grandes y con muchos lugares vacíos Desperdician espacio de almacenamiento.

* Existen métodos prácticos que almacenan solo los elementos no vacíos por filas o por columnas.

La lista de control de acceso (ACL: access control list):

* Asocia a cada objeto una lista ordenada con:
	+ Todos los dominios que pueden tener acceso al objeto.
	+ La forma de dicho acceso (ej: lectura ®, grabación (w), ejecución (x)).

Una forma de implementar las ACL consiste en:

* Asignar tres bits (r, w, x) para cada archivo, para:
	+ El propietario, el grupo del propietario y los demás usuarios.
* Permitir que el propietario de cada objeto pueda modificar su ACL en cualquier momento:
	+ Permite prohibir accesos antes permitidos.

**Posibilidades**

La matriz de protección también puede dividirse por renglones.

Se le asocia a cada proceso una lista de objetos a los cuales puede tener acceso.

* Se le indican las operaciones permitidas en cada uno.
* Esto define su dominio.

La lista de objetos se denomina lista de posibilidades y los elementos individuales se llaman posibilidades. Cada posibilidad tiene:

* Un campo tipo:
	+ Indica el tipo del objeto.
* Un campo derechos:
	+ Mapa de bits que indica las operaciones básicas permitidas en este tipo de objeto.
* Un campo objeto:
	+ Apuntador al propio objeto (por ej.: su número de nodo-i).