Protección y seguridad

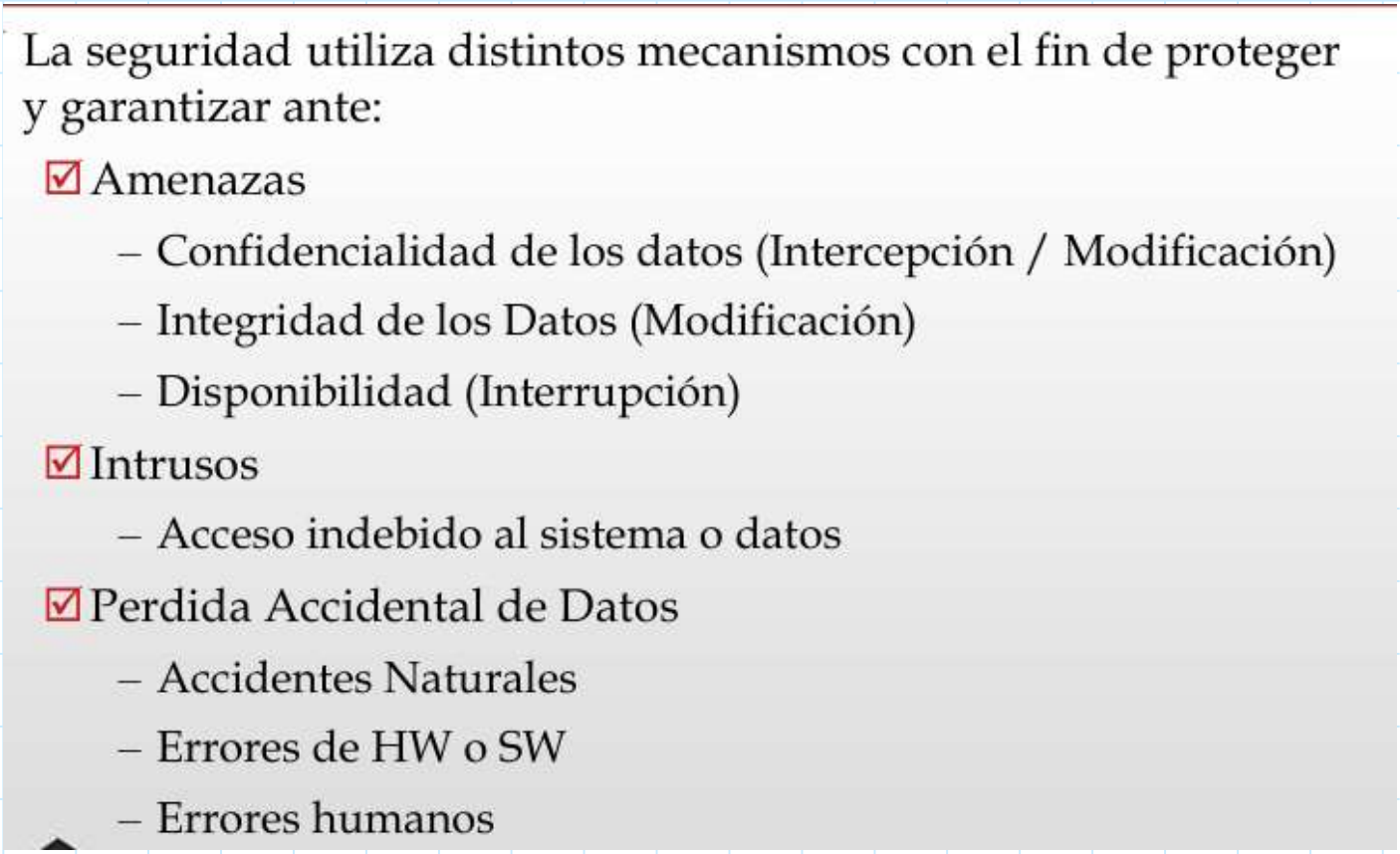
miércoles, 14 de mayo de 2025 20:50

Qué queremos proteger?

- Datos, info
- Cpu, memoria, dispositicos

SO se ocupa de eso mediante varios mecanismos

Protección != seguridad.
Protección: mecanismos del so para proteger la data dentro de la compu. Acceso de los procesos o users a recursos existentes
Es como poner **puertas con cerraduras** dentro de una casa: define **quién puede acceder a qué** y **qué operaciones puede realizar**.
Seguridad: protección interna y externa (ej ataques)
Es como asegurar **la casa completa** contra ladrones, incendios o catástrofes, no solo poner cerraduras internas.



Acceso al sistema se controla con autentificación y control sobre una base de usuarios,
Acceso a los recursos del sistema se resuelve con permisos y control de acceso

Hay que definir las mpolíticas antes que los mecanismos.
Las políticas son lo que se quiere lograr en términos de setguridad o protección. Qué restricciones tiene qyue habver, quien puede hacer cada cosa.
Los mecanismos es cómo implemento estas poíticas
Dominio:
Un derecho es autorización para hacer algo
Por ejemplo, el dominio d pyuede tener la pareja (archivo A, {read,write}) y un proceso que esté en el dominio d puede leer y escribir a
Es el conjuntod e permisis o privilegios que un user o proceso tiene para acceder a algo

Principio POLA: principle of least autority:
los procesos accedan sólo a los objetos que necesitan (con los derechos que necesiten) para completar su

tarea.

Relación entre un procesio y un dominio puede ser estática o dinámica
Estática: si el conjunto de objetos a los que el proceso accede drante el ciclo de vida es fijo(el dominio no cambia, puede pasar que en un momento dado el procesao rtenga más permisos de los que necesita)
Dinámica: va cambiando el conjunto de objetos

El dominio lo definen el UID y el gid.

- `setuid` **(Set User ID)**: Cuando un archivo ejecutable tiene este bit activado, **el proceso que se crea al ejecutarlo toma el UID del dueño del archivo, en lugar del UID del usuario que lo ejecutó**.
- Esto se usa cuando se necesita que un programa se ejecute con **privilegios más altos temporalmente**, por ejemplo, como **root**.

Objeto / Dominio	File1	File2	File3	Printer	D1	D
D1	Read	Read		Print		sv
D2		Read	execute	print		
D3	Read/write	Read/write			**switch**	

- ☑ Copy, owner y control son operaciones utilizan para controlar cambios al conte matriz de acceso.
- ☑ Switch y Control: son aplicables sólo a c
- ☑ Copy y owner: puede modificar derech de una columna.
- ☑ Control: puede modificar derechos dent fila