SEGURIDAD02

Mecanismos de Seguridad

Un **mecanismo de seguridad informática** es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y la disponibilidad de un sistema informático. Tipos según el momento en que se usan:

Seguridad Activa

Todos los mecanismos de seguridad que evitan que los sistemas informáticos sufran algún daño.

Seguridad Pasiva

Una vez que hemos sido afectados por una amenaza, todos los mecanismos que permiten minimizar los efectos o desastres causados por un accidente, un usuario o un malware a los sistemas informáticos.

Mecanismos de Seguridad

Otra clasificación que podemos hacer:

Preventivos

Actúan antes que el hecho ocurra y su función es detener agentes no deseados.

Detectivos

Actúan antes que el hecho ocurra y su función es revelar la presencia de agentes no deseados en el sistema, enviar el aviso y registrar la incidencia.

Correctivos

Actúan luego de ocurrido el hecho y su función es corregir las consecuencias.

Medidas de seguridad

- Política de contraseñas
- Listas de control de acceso
- Criptografía
- Política de almacenamiento
- Política de copia de seguridad
- Protección ante software malicioso (malware)
- Securización del software utilizado
- Seguridad perimetral
- Alta disponibilidad

Ejemplos de mecanismos de seguridad

- Sistemas de control de acceso
- Sistemas de seguridad de instalaciones
- Sistemas de vigilancia
- Autenticación
- Autorización
- Verificador de integridad de la información
- Cifrado
- Copias de seguridad
- Software anti-malware
- Firewall
- Sistemas de detección de intrusos / IDS
- Certificados
- Auditoría
- Uso adecuado de contraseñas
- ...

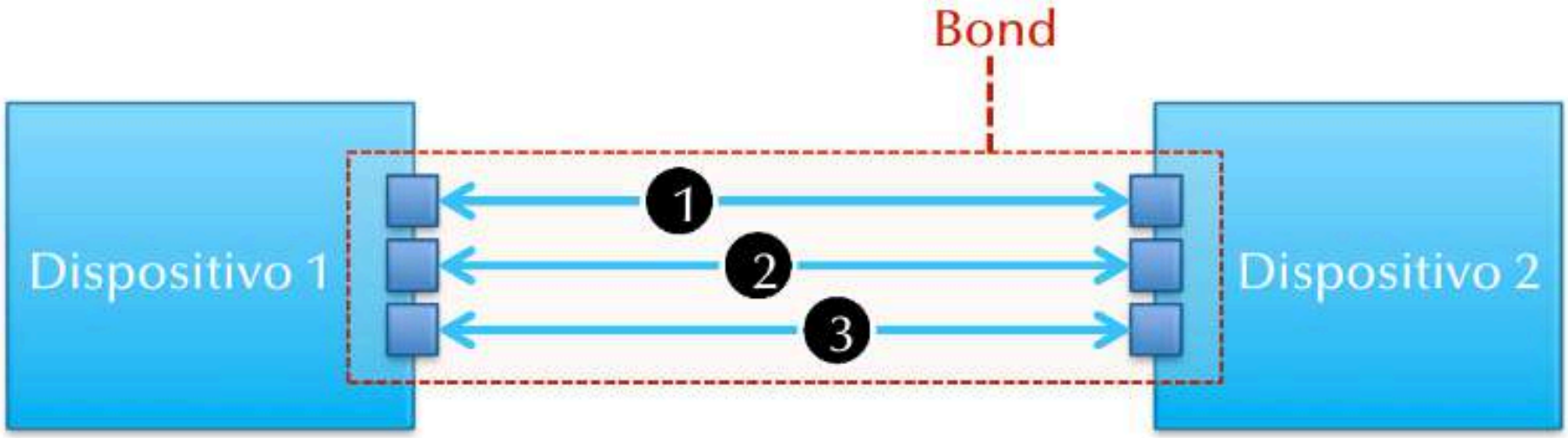
Tipos de medidas de protección

- Las medidas *pasivas* son las que se aplican al sistema informático, normalmente *desde el principio de* su instalación, para minimizar los efectos causados por accidentes, averías y malfuncionamiento, en general. Un ejemplo de este tipo de medidas es la instalación de una alarma antincendios.
- Las medidas *activas* son las que se utilizan en el día a día para combatir daños en el sistema informático provocados, principalmente, por el factor humano e implican la supervisión de un administrador del sistema. Un ejemplo de este tipo de medidas es la instalación, configuración y supervisión de un firewall (cortafuegos).
- Ambos tipos de medidas pueden, a su vez, clasificarse en *preventivas* (o *proactivas*) y *paliativas* (o *correctivas* o *reactivas*).

Seguridad física y ambiental

- Ubicación y protección de equipos y servidores.
- Protección ante fallos del cableado.
- Protección ante humedades e inundaciones.
- Protección ante incendios y altas temperaturas.
- Protección ante terremotos.
- Protección ante problemas del suministro eléctrico.
- Protección ante accesos no autorizados y robos.

Protección ante fallos del cableado.



Link Aggregation (IEEE802.3X)

CPD: eficiente, seguro y confiable, garantizando la disponibilidad de los datos y servicios

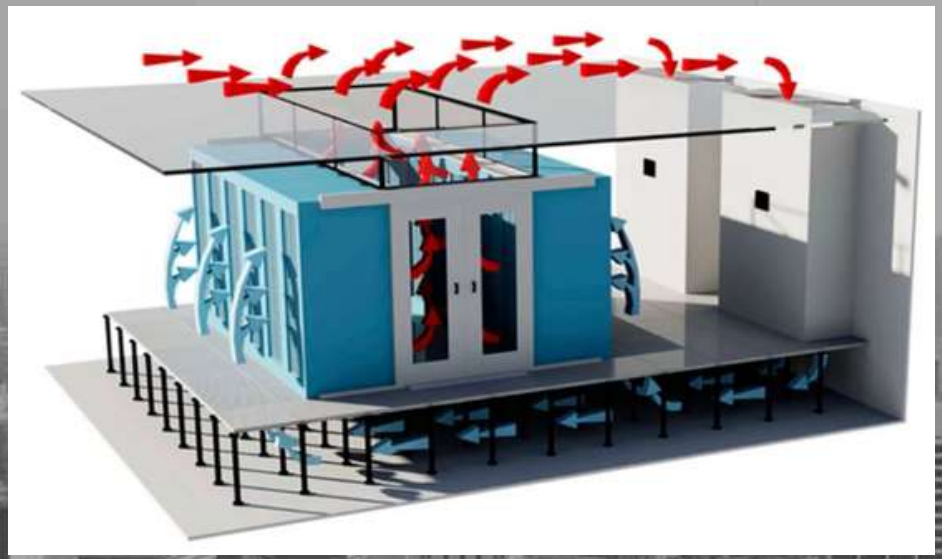
1. Infraestructura Física
   - Edificio o Sala
   - Racks y Bastidores
   - Climatización
   - Sistema de Protección Contra Incendios
2. Equipos de Energía:
   - Fuente de Alimentación Ininterrumpida (SAI, UPS)
   - Generadores
   - Distribución Eléctrica
3. Equipos Informáticos:
   - Servidores
   - Sistemas de Almacenamiento
   - Equipos de Red
4. Sistemas de Seguridad:
   - Control de Acceso
   - Videovigilancia
   - Sistemas de Monitoreo y Alarma
5. Conectividad:
   - Redes de Telecomunicaciones
   - Cableado Estructurado
6. Sistemas de Gestión y Monitoreo:
   - Software de Gestión
   - Sistemas de Monitoreo Ambiental
   - Sistemas de Gestión de Energía (PDU)

Microsoft

Google

Amazon

CPD/ DATA CENTER



Sistemas de alimentación ininterrumpida (SAI)

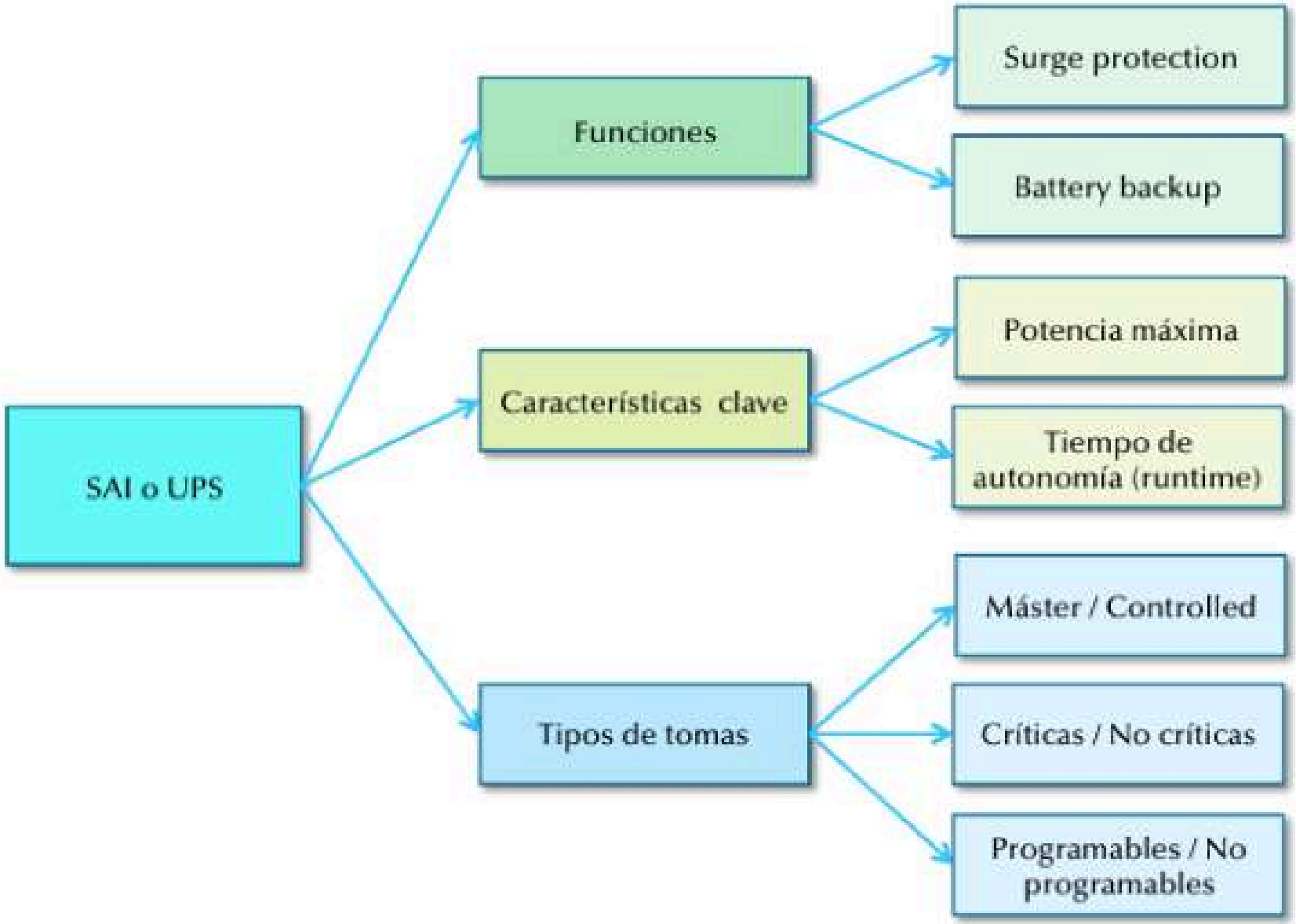
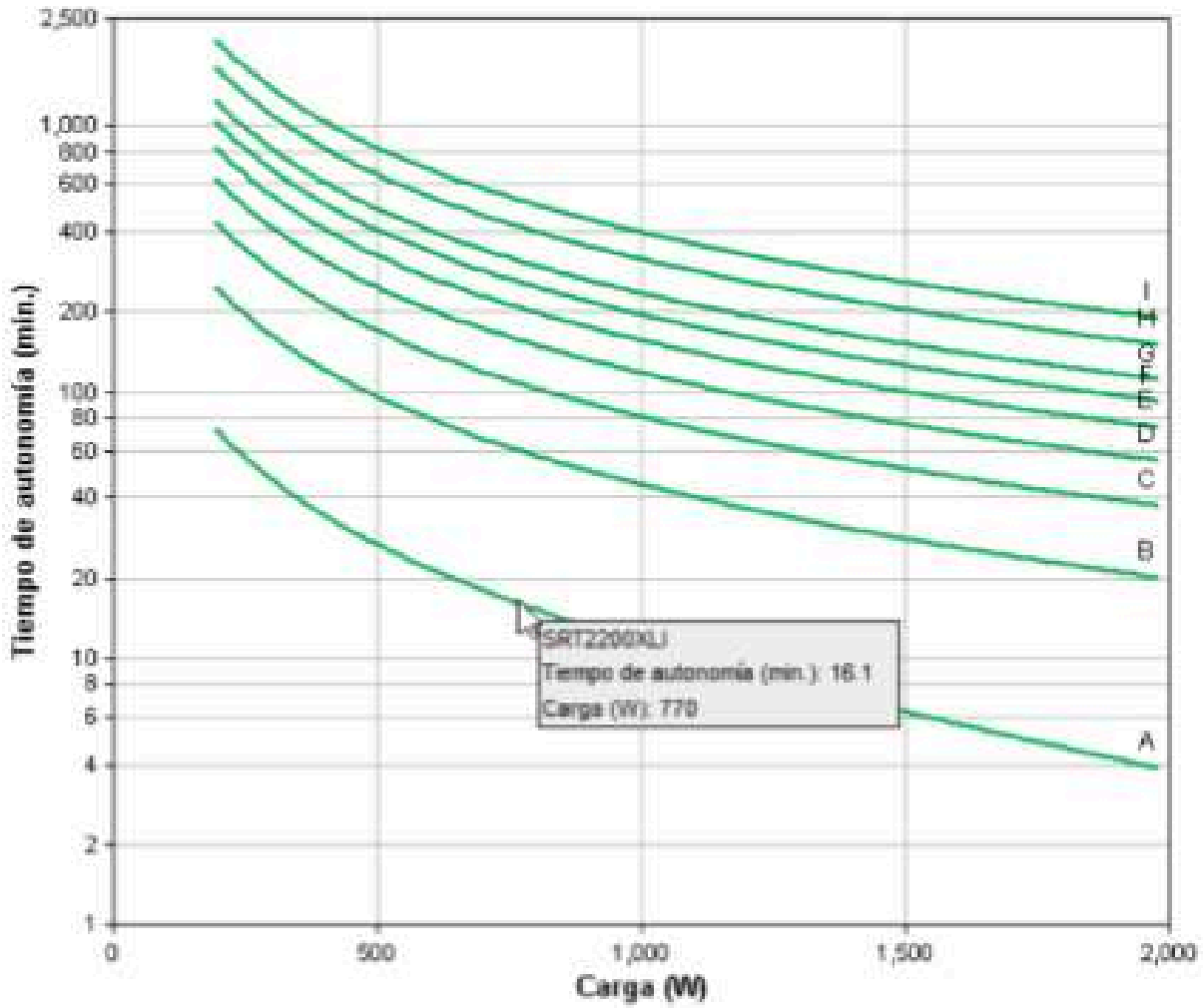


Gráfico de tiempo de ejecución

Curve	Part Number(s)
A	SRT2200XLI
B	SRT2200XLI + (1)SRT72BP
C	SRT2200XLI + (2)SRT72BP
D	SRT2200XLI + (3)SRT72BP
E	SRT2200XLI + (4)SRT72BP
F	SRT2200XLI + (5)SRT72BP
G	SRT2200XLI + (6)SRT72BP
H	SRT2200XLI + (8)SRT72BP
I	SRT2200XLI + (10)SRT72BP



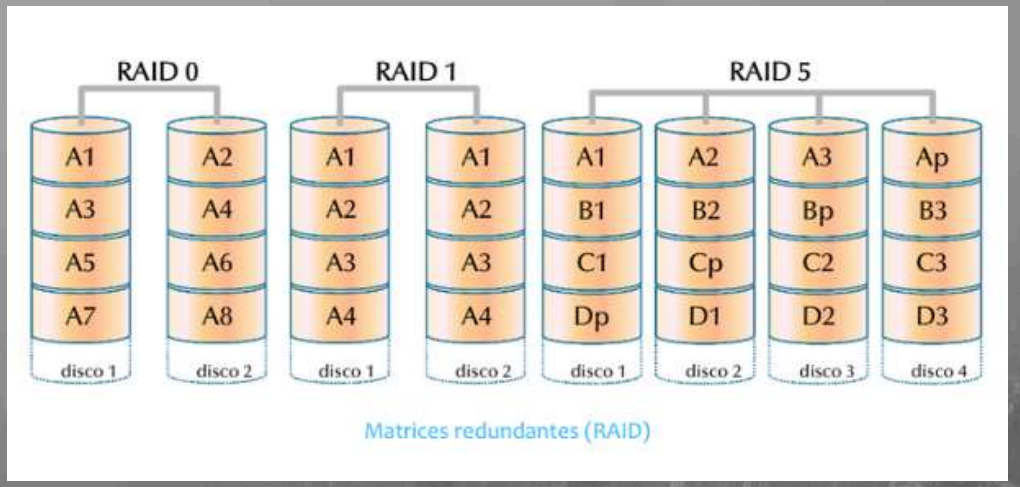
Gráfica de tiempo de autonomía de un modelo de SAI con diferente número de baterías, según potencia requerida.

CASO PRÁCTICO DE SAI

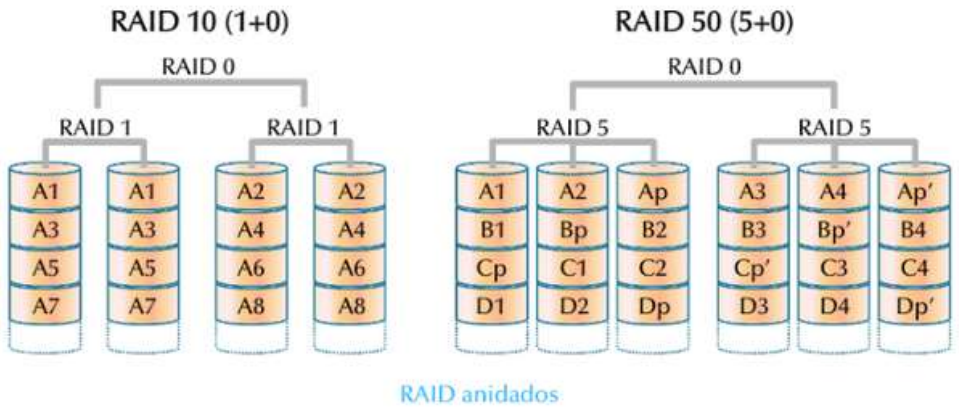
Protección de almacenamiento

Los puntos fundamentales sobre los que debe establecerse son los siguientes:

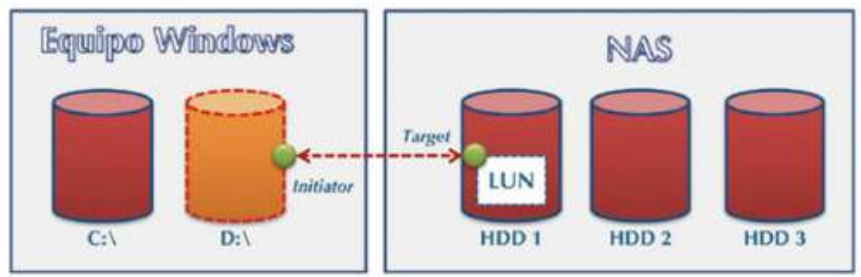
- Ubicación.
- Tipo.
- Redundancia.
- Alta disponibilidad.



Matrices redundantes (RAID)



RAID anidados

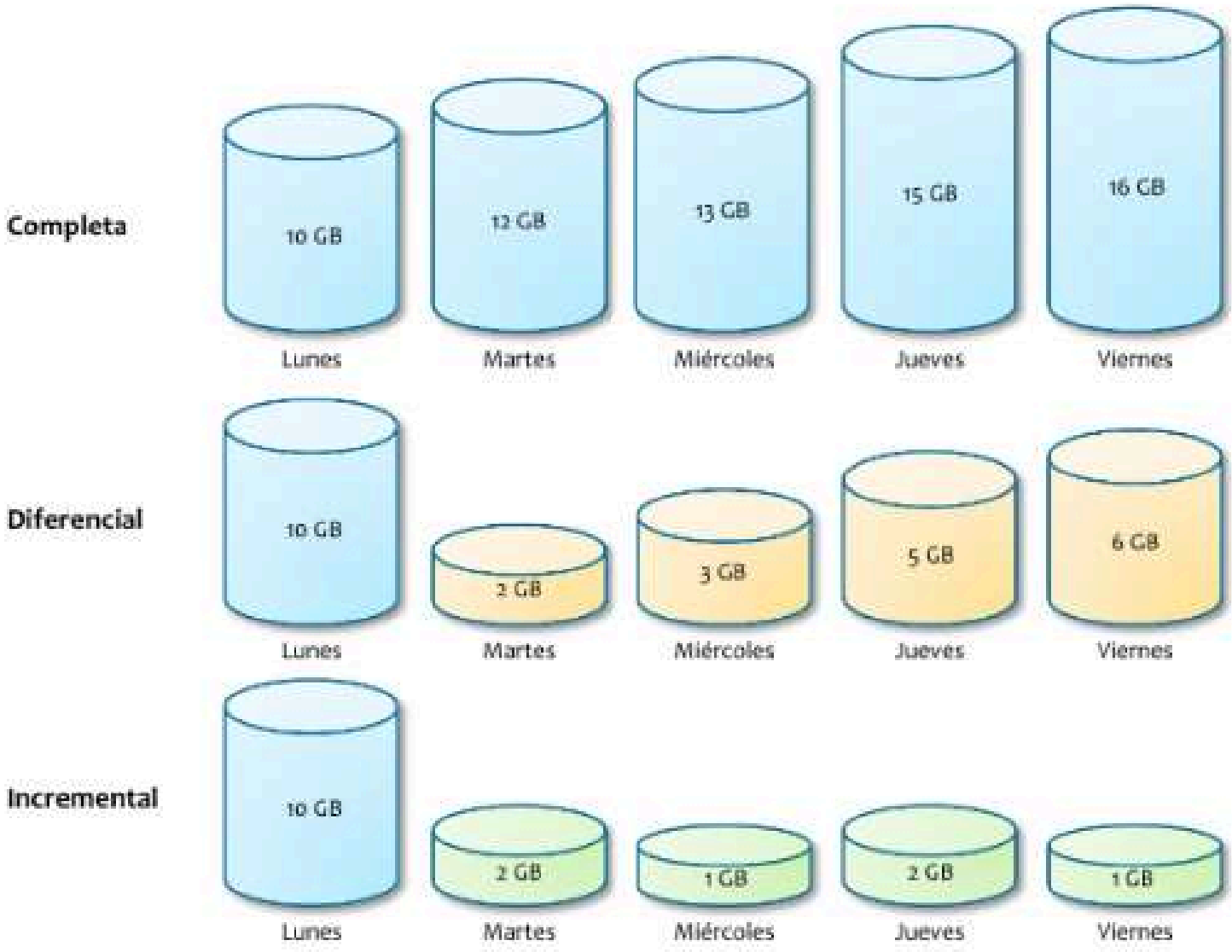


iSCSI (Windows → NAS)

Copia de seguridad

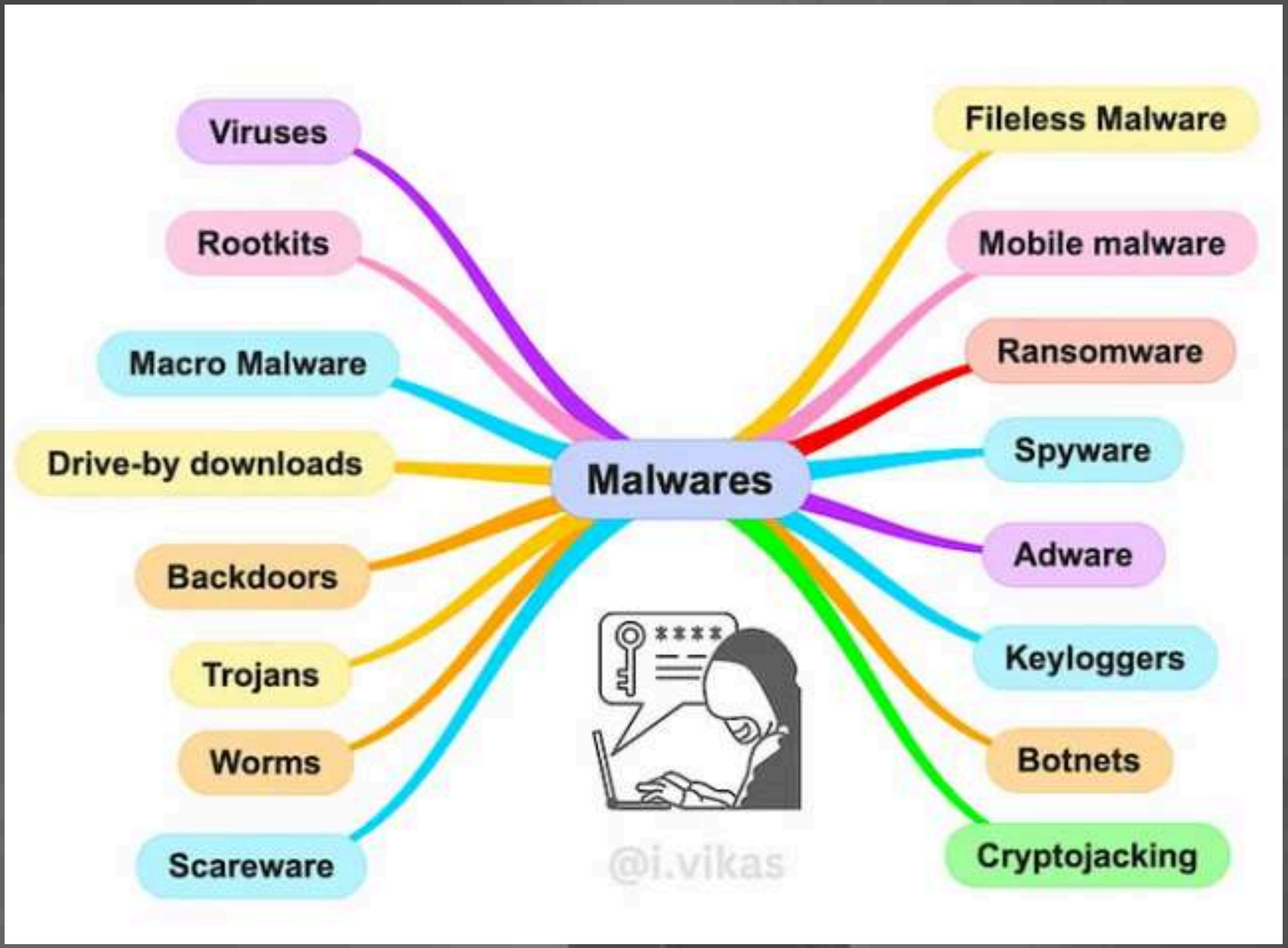
Una *copia de seguridad* (*backup*) es un archivo o conjunto de archivos, almacenado en una ubicación denominada *destino* (*destination*), que contiene una copia de los directorios y ficheros elegidos previamente por el usuario, denominados *origen* (*source*).

La copia de seguridad puede estar comprimida (para ocupar menos espacio) y cifrada (para evitar su lectura por personas no autorizadas).



Tipos de copias de seguridad

Fases de un ataque informático



Enlace a definiciones

Ataques por ingeniería social

Phishing, Vishing y Smishing
Baiting o Gancho
Shoulder surfing
Dumpster Diving
Spam
Fraudes online

Ataques a las conexiones

Redes trampa
Spoofing
Ataques a Cookies
Ataques DDoS
Inyección SQL
Escaneo de puertos
Man in the middle
Sniffing

Enlace a definiciones

ALTA DISPONIBILIDAD

- Alta disponibilidad se refiere a la capacidad de que aplicaciones y datos se encuentren operativos para los usuarios en todo momento y sin interrupciones, debido principalmente a su carácter crítico.
- Ejemplos: sistemas sanitarios, control aéreo, de comercio electrónico, bancarios, transporte marítimo, militares, etc.
- Dos tipos de interrupciones.
    - Previstas. Que se realizan cuando paralizamos el sistema para realizar cambios o mejoras.
    - Imprevistas. Que suceden por acontecimientos imprevistos (como un apagón, un error del hardware o del software, problemas de seguridad, un desastre natural, virus, accidentes, caídas involuntarias del sistema.
- La seguridad de todo el sistema es igual a la de su punto débil.
- La educación de los usuarios es fundamental para que la tecnología de seguridad pueda funcionar.
- Por mucha tecnología de seguridad que se implante debe existir implicación por parte de la directiva y una cultura a nivel de usuarios.
    - Sistema de seguridad = Tecnología + Organización