Backups

Por qué son vitales y cómo hacerlos correctamente.

¿Qué es un backup?

Un **backup** o copia de seguridad es una copia de tus archivos que te permite recuperar la información si los datos originales se pierden o se dañan.

Hoy no es solo una precaución: es la última línea de defensa frente a incidentes como estos:

- **Ransomware:** ataques en los que los delincuentes bloquean o cifran la información de un dispositivo y exigen un pago (rescate) para devolverla. Muchas veces también roban los datos y amenazan con publicarlos (doble extorsión).
- **Fallas de hardware:** deterioro o mal funcionamiento de discos, memorias o placas por uso prolongado, defectos de fábrica, sobrecalentamiento o cortes de luz.
- **Errores humanos y robos:** borrados accidentales, formateos o configuraciones incorrectas, y robo o pérdida de celulares, notebooks o pendrives.

Tipos de copias

Hay distintos métodos según cuán rápido necesites recuperar la información, qué tan crítica es y cuánto espacio tenés:

Completo (full)	Copia todo el sistema: archivos, configuraciones y programas. Es la base para una restauración total, pero requiere más tiempo y espacio.
Incremental	Copia solo lo que cambió desde la última copia, completa o incremental. Ahorra espacio y tiempo, pero restaurar es más complejo porque depende de varias copias.
Diferencial	Guarda todos los cambios desde el último backup completo. Equilibra velocidad de restauración y espacio.
Manual	Copia de archivos puntuales, como documentos o fotos. Es simple, pero depende de que te acuerdes de hacerla y no protege el sistema completo.

La regla de oro: guardalas en otro lugar

Las copias siempre tienen que estar en un lugar distinto del original. Los medios más recomendados son:

- **Nube:** permite acceder desde cualquier lugar. Protegé el acceso y, si es posible, mantenela desconectada cuando no estés haciendo la copia, para que un virus no la alcance.
- **Discos externos y SSD:** unidades físicas de gran capacidad y alta velocidad.
- **Sistemas NAS:** almacenamiento conectado a la red, pensado para hogares y pequeñas empresas.

Buenas prácticas

- **Aplicá la regla 3-2-1:** tené al menos 3 copias de tus datos, en 2 medios distintos (por ejemplo, disco externo y nube) y 1 copia fuera del lugar habitual.
- **Guardá una copia offline** (desconectada): es clave para protegerte del ransomware.
- **Automatizá los backups:** así evitás olvidos y errores, y las copias se mantienen al día.

Un backup actualizado es la diferencia entre un susto y una pérdida definitiva. Desde **BA-CSIRT** te recomendamos incorporarlo como un hábito.