

Las copias de seguridad

# Definición y justificación

---

- Proceso que duplica la información existente en otro soporte, de modo que se pueda recuperar si falla el original.
- Persigue almacenar la información crítica en más de un sitio, evitando su pérdida.
- Los soportes de almacenamiento tienen una vida útil limitada, con lo que en algún momento se perderá.
- La pérdida de información no respaldada puede tener graves consecuencias, entre otras:
  - Pérdida de horas de trabajo.
  - Pérdida de información de negocio.
  - Impacto en imagen ante clientes.

# El plan de recuperación ante desastres

---

- **DRP: Disaster Recovery Plan.**
- Permite a los departamentos de TI (Tecnologías de Información) planificar todos los aspectos necesarios para recuperar la actividad ante los diferentes desastres.
- Este plan debe incluir diversas políticas, entre las que se encuentra la política de copias de seguridad.
- El **DRP** forma parte del Plan de Continuidad de Negocio (BCP), junto con:
  - **BRP** (Business Recovery Plan): recuperación de los procesos de negocio.
  - **OEP** (Occupant Emergency Plan): protección de personas y resto de activos.
  - **COOP** (Continuity Operations Planning): continuidad de funciones estratégicas.
  - **IRP** (Incident Response Plan): gestión de incidentes causantes de la disrupción.

# ¿De qué hacer backup?

---

- Se debe hacer un inventario de los activos de información, y clasificarlos en base a su criticidad para el negocio.
  - Por su confidencialidad: información confidencial, interna o pública.
  - Por su utilidad: de clientes y proveedores, de compras y ventas, de personal, de gestión interna, logística, etc.
  - Por el impacto de la pérdida:
    - Daño de imagen
    - Consecuencias legales
    - Consecuencias económicas
    - Paralización de actividad

# Tipos de copia – Completa (full)

- Esta técnica consiste en realizar una copia de TODA la información que se quiere respaldar a otro soporte.
- Es el tipo de copia más básica y sencilla.
- Ventaja:
  - Restauración de los datos fácil y rápida (1 sola recuperación).
- Inconvenientes:
  - Necesita más espacio de almacenamiento, el que ocupen los archivos a copiar. Guardamos varias veces archivos que es posible que no se hayan modificado.
  - Es el tipo de copia que requiere más tiempo.



Fuente imagen: <https://qloudea.com/blog/tipos-de-backup-con-nakivo/>

# Tipos de copia – Incremental

- Solo se copian los archivos modificados y nuevos respecto a la copia anterior, ya sea completa o incremental.
- Ventajas
  - Es el tipo de copia que requiere menos espacio de almacenamiento.
  - El tiempo de realización de la copia es más corto.
- Inconveniente:
  - El tiempo para hacer una restauración puede ser alto → tenemos que restaurar desde la copia completa base y todas las copias incrementales intermedias.



# Tipos de copia – Diferencial

- Se guardan aquellos archivos que han cambiado y los que se han creado desde la última copia completa.
- Ventajas
  - Requiere menos espacio que la copia completa.
  - La restauración solo necesita la última copia completa y la diferencial.
- Inconvenientes:
  - Conforme pasa el tiempo se hace backup de más elementos, con lo que ocupa más espacio y lleva más tiempo realizar la copia.



# Tipos de copia – Ejemplos prácticos (I)

---

- Supongamos que tenemos un sistema a respaldar.
  - Tamaño de datos: 1TB
  - Modificaciones de un día a otro: 10% del total
- Caso 1:
  - Copia completa primer domingo del mes.
  - Diferencial el resto de domingos.
  - Incremental resto de los días.
- Caso 2:
  - Copia completa el primer domingo del mes.
  - Incremental resto de los días.



# Tipos de copia – Ejemplos

---

- Suponiendo que todos los meses tienen este calendario

L	M	X	J	V	S	D
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

**Para los casos prácticos anteriores, **tarea:****

- Capacidad de almacenamiento para guardar copias durante 1 mes.
- Número de copias de las que es necesario restaurar para recuperar los datos del jueves de la cuarta semana del mes .

# Plazos de retención/conservación de

---

- Las copias no se pueden mantener para siempre → se debe planificar el tiempo durante el que se mantendrán.
- Pasado este tiempo, los medios de almacenamiento empleados se liberan para reutilizan en nuevas copias.
- Es habitual definir varios plazos. Por ejemplo:
  - Mantener un backup completo mensual durante 12 meses
  - Mantener un backup de las últimas 4 semanas
  - Mantener un backup diario de los últimos 7 días

## **Tarea:**

- En el Caso 1 anterior, ¿qué capacidad de almacenamiento total será necesaria?

# Destinos de las copias

---

- Las copias de seguridad se pueden almacenar en distintos tipos de medios.
- No son excluyentes, se pueden combinar y tener varios niveles.
- En primer lugar, el más directo es realizar copias locales en discos HDD o unidades SSD.
  - utilizado frecuentemente como mecanismo de copia a nivel individual, para poder ir a una versión anterior.
  - Muy buenas velocidades de acceso.
- También se pueden usar soportes ópticos, aunque no es muy común.
  - La principal ventaja es que no se pueden modificar, que en algunos entornos específicos es requerido.
  - Inconveniente: se deteriora fácilmente.

# Destinos de las copias

- Cintas magnéticas DLT/LTO.
  - Soluciones de muy bajo coste por bit.
  - Vida útil superior a discos magnéticos (30años).
  - LTO 8 Ultrium: hasta 12TB por cartucho (30TB con compresión).
  - Pueden estar conectadas localmente al equipo (SAS, USB, ...) o también accesibles mediante red de datos o SAN → Robots.
  - Menor velocidad de acceso que discos (360MB/s).



# Destinos de las copias (II)

---

- Soluciones NAS (Network Attached Storage)
  - El coste varía en función del almacenamiento del dispositivo (número de unidades HDD o SSD, tipo de las unidades, RAID, ...)
  - Permite acceso desde los equipos a través de la red, con protocolos como SMB, NFS o FTP.
  - Las usuarias y usuarios pueden mapear unidades de estos equipos como si fuesen directorios locales.
  - Estos dispositivos suelen incorporar funcionalidades para recuperar versiones antiguas de archivos.

# Destinos de las copias (III)

---

- Cloud (Nube)
  - Empleamos almacenamiento ubicado en terceros.
  - Se accede a través de la red → Dimensionar bien el ancho de banda en función de las necesidades.
  - Permite tanto acceso a nivel de bloque (como si fuese un disco) o a nivel de fichero (como si fuese NAS).
  - Principales ventajas frente a uso de almacenamiento local:
    - Mantenemos una copia fuera de la empresa.
    - Nos protege en caso de desastre dentro de la organización.
  - Si usamos almacenamiento en Cloud, cuidado con requisitos legales.

# Destinos de las copias(IV)

---

- D2D2T (Disk to Disk To Tape).
  - Solución mixta.
  - Los datos se copian primero a disco → gran velocidad
  - Posteriormente se vuelca a cinta → reducido coste por bit
- D2D2C (Disk To Disk To Cloud)
  - Similar a la anterior, pero llevamos la copia a la nube.
- C2C (Cloud To Cloud)
  - Válida cuando trabajamos con soluciones SaaS (Software as a Service)
  - Copiamos a otra ubicación en la nube.

# Buenas prácticas: estrategia 3-2-1

---

- Diversificamos las copias para garantizar que siempre haya alguna de la que recuperar:
  - **3:** debemos mantener 3 copias de cualquier fichero importante → el original + 2 copias adicionales.
  - **2:** almacenamos en dos soportes distintos. Si uno falla, seguimos teniendo otro.
  - **1:** una de las copias debe residir fuera de la empresa → idónea la nube.
- Ejemplo de implementación:
  - En disco tenemos nuestro fichero.
  - Almacenamos una copia en un disco duro externo.
  - Almacenamos otra copia en la nube (ejemplo, Drive).



# Política de copias de seguridad

---

- Esta política forma parte del DRP.
- La política establecida debe garantizar cumplimiento de RTO y RPO requerido.
- Debe contemplar:
  - La frecuencia con la que se realiza una copia de seguridad de los datos.
  - El nivel de la copia (total, incremental, diferencial) y su plazo de retención.
  - La gestión de los soportes asociados → ver siguiente slide.
  - Los procedimientos necesarios para la solicitud de copias y restauraciones.
  - Los procedimientos de auditoría implantados para garantizar que el sistema funciona → PRUEBAS PERIÓDICAS!!!
  - El personal autorizado para realizar copias y restauraciones.
  - Los mecanismos de registro de cada operación realizada.

# Control de soportes

---

- Ubicación de las copias si se realizan en soportes extraíbles.
- Vida útil. Retirada planificada de soportes. OJO al borrado.
- Conservación
  - Aunque la copia ya no se vaya a utilizar puede haber requisitos legales de conservación (ej: facturas)
  - Puede ser necesario conservar copias durante largos períodos. Ej: hago una completa al mes y la guardo 1 año.
- Identificación de los soportes. Registro

<b>Código</b>	<b>Tipo</b>	<b>Fecha y hora</b>	<b>Lugar almacenamiento</b>	<b>Personal responsable</b>
---------------	-------------	---------------------	---------------------------------	---------------------------------

# RTO y RPO

---

- Ambos parámetros nos los marcarán las necesidades del negocio.
- No toda la información/sistemas tiene los mismos valores → BIAS (Business Impact Analysis).
- RTO: Recovery Time Objective
  - Tiempo en el que debemos tener el sistema/datos recuperado. El tipo de copia utilizado influye (no es el único parámetro).
- RPO: Recovery Point Objective
  - Cantidad de datos que podemos perder. La frecuencia de las copias determina este valor.
  - Ej: si hacemos 1 copia al día, el RPO debe ser igual o inferior a 24 horas.