Recuperación de datos ante desastre

Manual del
protocolo de recuperación de datos
y funcionamiento del sistema
de copias de seguridad de la empresa
Elorrieta Cines
(2026)

¿Qué es un BackUp o copia de seguridad?

Una copia de seguridad, comúnmente conocido como *«BackUp»*, es una copia idéntica de cualquier dato que requiera especial cuidado. Estas copias se crean para evitar la pérdida de datos.

Las copias de seguridad se pueden crear de forma manual, copiando y pegando datos de un sitio a otro, o se pueden crear con aplicaciones o herramientas diseñadas específicamente para crear copias de seguridad de la forma más eficiente o más íntegra posible.

Existen varias estrategias para maximizar la eficiencia de una copia de seguridad. En la empresa Elorrieta Cines, se usa el sistema que se apoya en *La regla «3-2-1»*.

Un sistema de BackUp 3-2-1 es una estrategia muy común utilizada para asegurar la supervivencia de los datos. Esta estrategia consiste en mantener 3 copias de los datos, siendo una la original, y las otras dos siendo copias de seguridad como tal. Estas últimas, se sustentan en dos tipos de medios diferentes, como lo podrían ser en un disco duro y un servidor en la nube; y establece que al menos una de estas dos copias se localice fuera del mismo edificio que la compañía para evitar riesgos. Así, en el caso de desastre, la diferencia entre una pérdida completa o una recuperación segura puede ser el radio en km de distancia de la ubicación del BackUp.

Cuando se habla de copias de seguridad, algo importante a mencionar son los tiempos límite a considerar en relación a cuánto tiempo tardaría en restablecerse el sistema desde la última copia o cuánto tiempo en “datos” se pierden como máximo entre copias.

Más detalladamente, esto sería:

- **RTO (Recovery Time Objective,** en español**: Objetivo de Tiempo de Recuperación):** el máximo de tiempo aceptable que puede estar el sistema fuera de servicio sin causar fallos graves. Podría ser por ejemplo un máximo de 8 horas. Pasado ese tiempo, tendría que estar funcionando el sistema de nuevo.
- **RPO (Recovery Point Objective,** en español, **Objetivo de Punto de Recuperación**): el volumen de datos máximo que se pueden

perder en el caso de corromperse el sistema, desde la última copia hasta el momento del desastre. Podría ser, por ejemplo, 4 horas, o 24 horas, etc. Eso significa que si algo sucede, hay garantía de que los datos perdidos solo serán, como máximo, de ese tiempo.

¿Qué datos se gestionan en nuestra empresa?

En Elorrieta Cines, los datos que manejamos y debemos salvaguardar mediante las copias de seguridad, son toda la información relacionada con nuestro cine: nuestra cartelera (películas, sesiones, salas), promociones, ventas, informes estadísticos, relación con proveedores, gestión del personal, marketing, datos de clientes, datos fiscales...

Cuando se trata de hacer una copia de seguridad de una base de datos mySQL, en esta empresa se realiza mediante el formato dump SQL. Dentro del sistema de archivos que del que se quiera hacer un BackUp, se generará un archivo que contenga todas las sentencias para recrear la base de datos en su estado guardado. Este archivo, tendrá como formato de nombre “AAAA-MM-DD.sql”, para identificar correctamente cada una de las copias.

El comando que se debe ejecutar en una consola o terminal para realizar ese BackUp de la base de datos es:

```
mysqldump -u root -p nombreBaseDatos > 2026-02-01.sql
```

*** Si no se sabe cómo abrir la consola/terminal, se explica en la sección posterior de “*Tecnología para utilizar Borg*”.

Tipos de BackUp de nuestro protocolo

Uno de los **BackUp** se hará **en la nube** (gestión remota en la red de Internet) y **full** (es decir, de todos los datos al completo). Debido a esto, ocupará mucho espacio (aproximadamente 50 TB y en aumento) y requerirá de bastante tiempo para realizarse. Por eso, este BackUp se hará **cada mes, el primer lunes por la mañana**. La elección de este día se basa en la baja asistencia en el cine los días entre semana, ya que la mayoría de los espectadores van al cine durante el fin de semana y el día del espectador (miércoles).

En segundo lugar, tendremos una **copia de seguridad** también **full cada semana**, en un **disco duro** localizado en un **edificio remoto** e **independiente**. Esta se hará **cada martes**, e implicará bastante espacio de almacenamiento también. Se realiza por una cuestión de no depender exclusivamente de la copia en la nube para poder recuperar todo el volumen de datos. Si solo hay una copia completa y el sistema (nube o disco) se rompe, la empresa estaría en serio peligro. Esta tardaría más ya que no estaría localizada en la red local sino a través de internet, de forma remota al disco de otro edificio.

Adicionalmente, es importante indicar en lo que respecta a la **copia original**, **todos los días a las 09:00 am** (horario laboral sin sesiones activas para espectadores), se almacenará los datos acumulados de las últimas 24h (última copia) en el propio servidor in situ (sistema local del propio cine). Esta copia es **diferencial**, es decir, que de forma diaria solamente acumula los datos nuevos, que sean diferentes de lo último guardado, así que no ocupa tanto espacio y no tarda demasiado tiempo. Esto facilita que si algo falla de forma local, se garantiza que la posible pérdida no afecte a más de 24h de información.

Detalles de la copia full en la nube

Como destino se ha elegido Amazon Web Services (AWS) y la herramienta que se usa para realizar dicha copia es Borg-BackUp.

AWS (AWS S3 en este caso) es la nube, el lugar donde almacenar los datos. Borg-BackUp es el programa que gestiona las copias. Es importante entender que no son lo mismo pero se relacionan, ya que AWS no hace copia por sí solo. Borg se encarga de cifrar las copias para mantener los datos seguros, y cada mes realiza una copia de forma automatizada con todos los datos.

La herramienta Borg-Backup hace uso de un repositorio para implementar sus funcionalidades. Estas funcionalidades son, entre otras:

- La automatización de las copias de seguridad
- La deduplicación de datos
- El cifrado de la información
- La gestión de versiones y retención

Los repositorios de BackUp se alojarán en servidores accesibles mediante SSH (esto permite conexiones seguras y protegidas), ubicados en distintas regiones cloud (la nube/internet), como se indicó previamente, en este caso **Amazon Web Services (AWS – EC2)**, por sus características:

- Servidor con almacenamiento persistente.
- Repositorio Borg principal.
- Ubicación: región primaria (por ejemplo, `us-east-1`).

Con esta copia, el RPO es entonces de un mes, y el RTO será de 14 horas.

Detalles de la copia full en disco

Se realiza en un edificio localizado a más de 100 km del cine, para garantizar que un desastre no afecte a todas las localizaciones donde se guardan datos en sistemas físicos (extremadamente improbable, tendrían que ser catástrofes de nivel nacional...).

Realmente esto sería el destino: un servidor/NAS en un edificio remoto (transmisión de datos por red WAN, internet). Se planteó la posibilidad de llevar físicamente los discos en lugar de hacer la copia de forma remota por internet por una cuestión de velocidad. De momento no se lleva a cabo físicamente, pero como posible medio de transmisión se llegó a considerar, y se descartó por cuestión de protección y seguridad de los datos. Para gestionar esta copia también se usará la herramienta Borg.

Con esta copia, el RPO es entonces de una semana, y el RTO será de 6 horas.

Detalles de la copia original

Para la gestión de los datos original, se usará un servidor en el propio cine (el destino), en la red local, copiando los datos de forma diaria (a las 09:00 am), usando un sistema diferencial. Se usaría también la herramienta **Borg**. Es el primer nivel de protección, rápido y fiable.

Es el respaldo de datos más rápido.

Con esta copia, el RPO es entonces de 24 horas, y el RTO será de 30 minutos.

Recuperación de datos ante desastres

Tecnología para utilizar Borg

Cuando un servidor falla, la prioridad es restablecer el servicio en el menor tiempo posible, garantizando la disponibilidad, integridad y confidencialidad de la información.
En Elorrieta Cines, los equipos de la empresa tienen instalado esta herramienta. A la hora de usar Borg, la herramienta para gestionar las copias, hay que tener en cuenta que se usa sin interfaz gráfica, es decir, sin usar otro software intermediario que aporte ventanas intuitivas para utilizar Borg-BackUp. ¿Esto qué implica? Se usará mediante línea de comandos. Dependiendo del Sistema Operativo, **para poder operar mediante línea de comandos, se hará de la siguiente manera**:

- **Windows OS** ofrece dos alternativas comunes:

  Opción 1: Símbolo del sistema (CMD)
  1. Pulsa la tecla Windows ⊞
  2. Escribe: “cmd”
  3. Pulsa Enter
  4. Se abrirá una ventana negra donde puedes escribir comandos.

  Opción 2: PowerShell
  1. Pulsa la tecla Windows ⊞
  2. Escribe: “PowerShell”
  3. Pulsa Enter

- **Linux**

  En la mayoría de distribuciones:
  Pulsa Ctrl + Alt + T

  Si no funciona:
  1. Abre el menú de aplicaciones
  2. Busca Terminal
  3. Haz clic para abrirla

- **macOS**

    1. Abre Finder
    2. Ve a Aplicaciones
    3. Entra en Utilidades
    4. Abre Terminal

    Alternativa rápida:
    1. Pulsa la tecla de comando ⌘ + la tecla Espacio
    2. Escribe: “Terminal”
    3. Pulsa Enter

Cómo seleccionar la copia para restaurar los datos

Dependiendo del desastre o catástrofe, de su gravedad y alcance, se usará un BackUp u otro. Lo primero será seleccionar el destino de donde extraer los datos:

- Si fuera un accidente **local no demasiado grave**, se podría usar perfectamente la **copia diferencial diaria** en el **servidor** del **propio** cine.
- Si el cine se viera **afectado** y el **servidor propio** quedara inutilizado (incendio del edificio, inundación...), se usaría la **copia full semanal del edificio remoto**.
- Si el **desastre** es **grave** e implicara a ambos edificios (terremoto, ataque, apagón nacional...), se usaría la **copia** que hay **en la nube**, el **BackUp mensual full**, ya como último recurso.

Para poder identificar cuál es la copia de seguridad, una vez sabemos el destino del que la vamos a extraer (local, edificio remoto, nube), tenemos que usar el comando “**borg list**” para ver cuál ha sido la última copia realizada más recientemente y en estado correcto.

Cómo restaurar/montar un servidor con un BackUp

Pasos para **recuperar** la copia de seguridad en el sistema de archivos local (o sistema de archivos de red montado **localmente**):

1. Listar la lista de copias de seguridad

```
borg list /ruta/de/repositorio
```

2. Recuperar la copia de seguridad seleccionada.

- Para restaurar archivos específicos si el daño fue parcial, sería pues una restauración parcial:

```
borg extract --progress /ruta/del/repositorio::root-2025-12-12 /ruta/archivo/importante
```

- Restaurar totalmente el repositorio, en caso de pérdida completa, una restauración de todos los datos:

```
borg extract --progress /ruta/del/repositorio::root-2025-12-12
```

Para restaurar archivo o archivos montando un sistema de archivos del repositorio, Borg permite montar el backup como un sistema de archivos, así puedes buscarlo y copiar un archivo o conjunto de archivos desde allí.

```
borg mount /ruta/del/repositorio::root-2025-12-12 /tmp/mountpoint
```

Pasos para recuperar la copia de seguridad en **remoto:**

Accediendo a través de ssh user@host:

1. Listar la lista de copias de seguridad

```
borg list ssh://user@host:port/ruta/de/repositorio
```

2. Recuperar la copia de seguridad seleccionada

- Para restaurar archivos específicos si el daño fue parcial, sería pues una restauración parcial:

```
borg extract --progress
ssh://user@host:port/ruta/del/repositorio::root-2025-12-12
/ruta/archivo/importante
```

- Restaurar totalmente el repositorio, en caso de pérdida completa, una restauración de todos los datos:

```
borg extract --progress
ssh://user@host:port/ruta/del/repositorio::root-2025-12-12
```

Para restaurar archivo o archivos montando un sistema de archivos del repositorio, Borg permite montar el backup como un sistema de archivos, así puedes buscarlo y copiar un archivo o conjunto de archivos desde allí.

```
borg mount ssh://user@host:port/ruta/del/repositorio::root-2025-12-12
/tmp/mountpoint
```

Conclusión

En Elorrieta Cines se implementa el sistema 3-2-1 para generar y gestionar copias de seguridad de los datos de la empresa. Garantiza la integridad de los datos, una recuperación segura y eficaz, con la mínima pérdida en caso de haber un desastre que interrumpa el sistema o destruya un servidor.
Las herramientas como Borg, AWS... son fiables y probadas. Luchamos por el mejor mantenimiento y la prevención.
Con nuestros RTO y RPO, tenemos un sistema de recuperación aceptable en la gran variedad de accidentes que podrían afectar a nuestro Cine.