Backup, Restore y Continuidad en Sistemas de Información

1.1 Introducción

El backup, la recuperación y la continuidad constituyen una parte central de la administración de Tecnologías de la Información. No se trata únicamente de copiar archivos: se trata de asegurar que la organización pueda seguir funcionando cuando ocurre una falla, un error humano, un ataque, un desastre físico, una pérdida accidental o una interrupción del servicio.

Desde la mirada de la administración, la pregunta principal no es solo si existen copias de respaldo. La pregunta central es si esas copias permiten recuperar los datos y los procesos dentro de los tiempos que el negocio necesita. Una copia que no se puede restaurar no resuelve el problema. Un respaldo con datos corruptos puede generar una falsa sensación de seguridad. Un plan de recuperación que nunca fue probado puede fallar precisamente cuando más se lo necesita.

1.2 1. El principio que organiza todo

Antes de analizar cualquier tecnología o procedimiento de backup, es necesario establecer el principio fundamental:

> **Los datos de una organización son aquellos que no pueden conseguirse ni reemplazarse buscándolos en terceros o en el mercado.**

Una empresa puede reponer una notebook robada comprando otra. Puede reemplazar un servidor dañado adquiriendo uno nuevo. Puede volver a instalar un sistema operativo. Pero **no puede recuperar los datos que ese equipo contenía** si no existe una copia de respaldo. Las facturas emitidas, las cobranzas registradas, los contratos firmados, los legajos de personal, las órdenes de compra procesadas, los registros contables, el historial de clientes: todo eso es irrepetible.

Desde la administración, esta distinción es fundamental: **la tecnología es reemplazable; la información no lo es.**

Esta es la razón por la que el backup no es una tarea técnica opcional: es una **política de protección patrimonial**.

1.3 Conceptos fundamentales

1.3.1 Backup, restore, recuperación ante desastres y continuidad del negocio

Cuatro conceptos que suelen confundirse pero que tienen alcances distintos:

Concepto	Qué es	Pregunta que responde
Backup	Copia de datos, sistemas o configuraciones para conservarlos como resguardo	¿Qué copia existe si algo falla?
Restore / Recuperación	Proceso de recuperar datos o sistemas desde una copia de seguridad	¿Cómo se vuelve a trabajar después de la falla?
Disaster Recovery (DR)	Conjunto de procesos para restablecer sistemas críticos tras una interrupción grave	¿Dónde y cómo se levantan los sistemas?
Business Continuity (BC)	Capacidad de la organización para seguir operando ante incidentes	¿Puede la organización seguir funcionando y en cuánto tiempo?

Un backup sin una estrategia de restore definida es incompleto. Un restore sin copias confiables es imposible. **Ambos deben diseñarse juntos.**

Ejemplo: si un incendio destruye la sala de servidores, el backup permite recuperar los datos; el restore permite volverlos a cargar; el disaster recovery define en qué infraestructura alternativa se levantarán los sistemas; y la business continuity define cómo trabajará la organización mientras eso ocurre.

1.4 Métricas clave: RPO, RTO y MTD

1.4.1 RPO — Recovery Point Objective

Define la **máxima cantidad de datos que una organización puede permitirse perder**, expresada en tiempo. Responde a la pregunta: *¿hasta qué punto en el tiempo podemos retroceder sin que el impacto sea inaceptable?*

Ejemplo: RPO = 1 hora. Esto significa que los backups deben realizarse con frecuencia suficiente para que nunca se pierdan más de 60 minutos de datos.

1.4.2 RTO — Recovery Time Objective

Define el **tiempo máximo aceptable para restaurar los sistemas** y retomar las operaciones normales. Responde a la pregunta: *¿cuánto tiempo puede la organización operar sin sus sistemas?*

Ejemplo: RTO = 2 horas. La organización no puede tolerar más de dos horas de inactividad antes de que el impacto económico u operacional sea crítico.

1.4.3 MTD — Maximum Tolerable Downtime

Representa el **tiempo total máximo en que los datos y sistemas deben estar disponibles** para el negocio. Es el límite absoluto: superarlo compromete la viabilidad operativa de la organización.

Indicador	Qué mide	Pregunta práctica
RPO	Pérdida máxima de información	¿Hasta qué momento deben recuperarse los datos?
RTO	Tiempo máximo de caída	¿En cuánto tiempo debe volver el sistema?
MTD	Límite absoluto de inactividad	¿A partir de qué punto se compromete la viabilidad?

Cuanto menor sea la tolerancia a la pérdida de datos (RPO bajo) y menor el tiempo aceptable de interrupción (RTO bajo), **mayor es el costo de la solución técnica requerida**. Esta relación directa entre riesgo, tiempo y costo es una **decisión de administración**, no solo de tecnología.

Ejemplo integrado: si un sistema de ventas tiene RTO de 2 horas y RPO de 1 hora, la organización debe poder restablecerlo en ese plazo y perder, como máximo, las operaciones de la última hora. Si solo existe un backup diario, ese RPO no se cumple.

1.5 Clasificación de datos: críticos, necesarios e innecesarios

La primera decisión administrativa consiste en clasificar la información. No todos los datos tienen el mismo valor ni requieren el mismo nivel de protección. Tratar toda la información como igualmente importante genera costos innecesarios y puede dejar mal protegidos los datos esenciales.

Tipo de dato	Característica principal	Tratamiento recomendado
Crítico	Su pérdida impide operar o cumplir obligaciones	Mayor frecuencia de backup, protección reforzada y recuperación prioritaria
Necesario	Es útil para la gestión, pero no paraliza inmediatamente	Conservación ordenada y frecuencia proporcional
Innecesario	No aporta valor actual ni obligación de conservación	Eliminación según política de retención

Ejemplo: una base de facturación activa es crítica. Un reporte mensual ya presentado puede ser necesario. Copias duplicadas de archivos temporales antiguos son innecesarias.

1.6 Tipos de backup según el alcance

1.6.1 Comparación general

Tipo	Qué copia	Velocidad de backup	Espacio utilizado	Velocidad de restore	Dependencias para restaurar
Full	Todo el conjunto de datos seleccionado	Lenta	Alto	Rápida	Solo el full
Incremental	Solo los cambios desde el último backup (full o incremental)	Rápida	Bajo	Más lenta	Full + todos los incrementales en secuencia
Diferencial	Todos los cambios desde el último full	Media	Crece con el tiempo	Media	Solo el full + el último diferencial
Sintético full	Construye un nuevo full combinando el full	Media	Alto	Rápida	Solo el sintético

Tipo	Qué copia	Velocidad de backup	Espacio utilizado	Velocidad de restore	Dependencias para restaurar
	anterior con los incrementales, sin releer producción				
Snapshot	Estado de un sistema, volumen o VM en un momento determinado	Muy rápida	Variable	Muy rápida	Depende del almacenamiento original
Mirror / Espejo	Réplica 1:1 en tiempo real o casi real del sistema origen	Continua	Igual al origen	Muy rápida	Sistema de replicación activo
CDP	Cambios de manera continua o casi continua	Continua	Alto	Muy rápida (punto exacto)	Sistema de protección continua

1.6.2 Backup completo (Full Backup)

Copia todos los datos seleccionados. Es el esquema más simple de comprender y restaurar, porque contiene una versión íntegra del conjunto respaldado.

- **Ventaja principal:** restauración más simple y autónoma.
- **Desventaja:** mayor consumo de almacenamiento, tiempo y ancho de banda.
- **Uso habitual:** copia semanal o mensual como base de la estrategia, y previa a cambios importantes.

Ejemplo: una empresa realiza un full backup de su servidor todos los domingos a las 02:00 hs, cuando la actividad del sistema es mínima.

1.6.3 Backup incremental

Copia solo los cambios realizados desde la última copia, sea completa o incremental. Consume menos espacio y suele ejecutarse más rápido.

- **Ventaja principal:** ahorro de espacio y velocidad de copia.
- **Desventaja:** la restauración requiere más pasos y es más lenta; si una copia intermedia falla, la cadena se rompe.
- **Uso recomendado:** copias frecuentes (diarias o por hora) de grandes volúmenes.

1.6.4 Backup diferencial

Copia todos los cambios realizados desde el último backup completo. Con el paso de los días, la copia diferencial crece hasta que se realiza una nueva copia completa.

- **Ventaja principal:** la restauración requiere solo dos elementos: el último full y el último diferencial.
- **Desventaja:** el tamaño crece progresivamente hasta el próximo full.
- **Uso recomendado:** equilibrio entre espacio de almacenamiento y velocidad de recuperación.

1.6.5 Diferencia visual entre incremental y diferencial

Backup incremental — cada copia contiene solo lo que cambió desde la copia anterior:

```
Dom       Lun       Mar       Mié       Jue
[FULL] → [+Lun] → [+Mar] → [+Mié] → [+Jue]
         solo lun  solo mar  solo mié  solo jue
```

Backup diferencial — cada copia contiene todo lo que cambió desde el último full:

```
Dom       Lun       Mar       Mié          Jue
[FULL] → [Lun] → [Lun+Mar] → [Lun+Mar+Mié] → [Lun+Mar+Mié+Jue]
         desde dom  desde dom  desde dom      desde dom
```

La copia diferencial **crece** con cada día que pasa desde el último full. La copia incremental **no crece**: solo contiene los cambios del día. Pero para restaurar con incrementales, se necesitan más piezas.

1.6.6 Snapshot

Captura del estado de un sistema, volumen, máquina virtual o base de datos en un momento determinado.

- **Ventaja:** rapidez; útil como punto de control antes de cambios o actualizaciones de sistemas.
- **Limitación:** no protege si se pierde el almacenamiento principal; no siempre puede considerarse un backup suficiente por sí solo.

1.6.7 CDP — Continuous Data Protection

Registra cambios de forma constante o casi constante, permitiendo recuperar información en puntos muy cercanos al momento del incidente.

- **Ventaja:** RPO muy bajo, recuperación casi en tiempo real.
- **Limitación:** costo elevado; puede replicar errores si no se combina con retención histórica.

- **Uso recomendado:** sistemas de alta criticidad.

1.7 Ejemplo práctico — Estrategia de backup en una quincena

1.7.1 Escenario

Una empresa de servicios opera un sistema de gestión que procesa ventas, cobranzas y facturación. La política define: - **Domingos:** backup full de toda la base de datos y archivos del sistema. - **Lunes a sábados:** backup diario, incremental o diferencial.

Situación: el sistema falla el **jueves 12 a las 13:45 hs**. Se activa el proceso de restore.

1.7.2 Estrategia A: backup incremental

Para restaurar, se necesita aplicar **en orden** cada pieza:

Paso	Copia	Contenido
1	Full Dom 8	Estado completo del sistema
2	Incremental Lun 9	Solo cambios del lunes
3	Incremental Mar 10	Solo cambios del martes
4	Incremental Mié 11	Solo cambios del miércoles
5	Incremental Jue 12	Solo cambios del jueves hasta el backup nocturno anterior

Riesgo específico: si cualquier copia incremental de la cadena se daña o no existe, la restauración se interrumpe. No es posible saltar un eslabón.

1.7.3 Estrategia B: backup diferencial

Para restaurar, solo se necesitan **dos piezas**:

Paso	Copia	Contenido
1	Full Dom 8	Estado completo del sistema

Paso	Copia	Contenido
2	Diferencial Mié 11	Todos los cambios desde el domingo (lun + mar + mié)

Las copias diferenciales de lunes y martes **no son necesarias**: ya están incluidas en la del miércoles.

Ventaja: la restauración es más simple y rápida. Si el diferencial del miércoles se daña, se puede intentar con el del martes.

1.7.4 Comparación de ambas estrategias

Dimensión	Estrategia A — Incremental	Estrategia B — Diferencial
Piezas necesarias para restaurar	Full + Inc Lun + Inc Mar + Inc Mié + Inc Jue	Full + Dif Mié
Pasos de restore	5	2
Velocidad de restore	Más lenta	Más rápida
Espacio por copia	Menor (solo cambios del día)	Mayor (crece con los días)
Riesgo si una copia se daña	Alto — la cadena se rompe	Moderado — se puede retroceder al diferencial anterior

1.7.5 ¿Qué datos se pierden en ambos casos?

En ambos escenarios, **los cambios realizados el jueves 12 después del último backup nocturno y antes de las 13:45 hs** no están respaldados. Esa es la **brecha del RPO**: la información del período no cubierto por ninguna copia.

Si la organización no tolera perder ninguna transacción del día, necesita una solución de mayor frecuencia, como backups del log de transacciones cada hora o protección continua (CDP).

1.8 Medios de almacenamiento

1.8.1 Medios locales

Medio	Uso típico	Ventaja principal	Riesgo principal
Disco externo	Copias puntuales, pequeñas organizaciones	Bajo costo, fácil de usar	Si queda conectado, puede ser afectado por ransomware
NAS	Backup centralizado de múltiples equipos	Automatización, acceso en red	Si está conectado permanentemente, puede ser atacado
SAN	Entornos empresariales críticos	Alto rendimiento y escalabilidad	Mayor costo y complejidad
Servidor local de backup	Recuperación rápida dentro de la red	Control directo, restore veloz	Riesgo ante incendio, robo o desastre físico
Cinta magnética	Archivo histórico y cumplimiento legal	Bajo costo por volumen, air gap natural	Restore más lento, gestión física; requiere inventario, rotulado y pruebas de lectura

Medio	Uso típico	Ventaja principal	Riesgo principal
Almacenamiento óptico	Copias de archivo y documentos cerrados	Bajo costo, facilidad de transporte	Capacidad reducida, degradación física, no apto para grandes volúmenes activos

1.8.2 Medios en la nube

Tipo	Uso típico	Característica principal
Almacenamiento estándar	Copias recientes que pueden necesitarse pronto	Acceso rápido, mayor costo por GB
Almacenamiento frío	Copias poco consultadas	Menor costo, mayor tiempo de recuperación
Archivo profundo	Retención de largo plazo por cumplimiento	Muy bajo costo de almacenamiento, recuperación lenta
BaaS	Solución administrada de backup para pymes	Incluye software, almacenamiento, monitoreo y alertas
DRaaS	Recuperación ante desastres como servicio	Permite levantar sistemas replicados ante una falla grave

Importante: no debe confundirse backup en la nube con sincronización. Una carpeta sincronizada replica cambios, incluyendo borrados o archivos cifrados por malware. Para que exista backup real, se necesitan retención, versiones, protección contra eliminación y pruebas de restauración.

1.8.3 Backup local vs. remoto vs. off-site

Tipo de backup	Ventaja	Limitación
Local	Restauración rápida, control directo	Puede afectarse por el mismo incidente que daña los datos originales
Remoto	Mayor separación física o lógica	Depende de conectividad y configuración
Off-site	Protección ante desastre del sitio principal	Puede requerir más tiempo de recuperación

Ejemplo: si el servidor y sus backups están en la misma sala, un incendio puede destruir ambos. Una copia off-site conserva la capacidad de recuperación.

1.9 8. La Regla 3-2-1 y su evolución

1.9.1 Regla clásica 3-2-1

Componente	Qué significa	Por qué importa
3 copias	Una original y dos de respaldo	Si una falla, hay alternativas
2 medios distintos	Por ejemplo, disco local + nube	Un único medio puede fallar
1 copia fuera del sitio	Off-site: nube, otra sede, proveedor	Un incendio o inundación destruye lo que está en el mismo lugar

Ejemplo de implementación:

Servidor principal (Original)

↓

NAS local (Copia 1)

↓

Nube (Copia 2)

↓

Disco externo fuera del sitio — Off-site

1.9.2 Evolución: esquema 3-2-1-1-0

Ante el avance del ransomware, el esquema 3-2-1 se reforzó:

Componente adicional	Significado
+1 copia inmutable	Una copia que no puede modificarse ni eliminarse, ni por usuarios con altos privilegios, durante un período definido
+0 errores verificados	Las copias deben probarse periódicamente; solo cuenta como backup lo que puede restaurarse exitosamente

El ransomware moderno busca destruir o cifrar también los backups antes de exigir el rescate. Sin copias inmutables o aisladas (*air-gapped*), el ataque puede inutilizar toda la estrategia de recuperación.

1.10 RAID, redundancia y replicación: no reemplazan el backup

Un error frecuente es confundir disponibilidad con protección de datos.

Concepto	Qué resuelve	Qué NO resuelve
RAID	Falla de ciertos discos físicos	Borrado accidental, ransomware, corrupción lógica de datos

Concepto	Qué resuelve	Qué NO resuelve
Redundancia	Interrupción por falla de componentes	Recuperación a un punto anterior en el tiempo
Replicación off-site	Mejora disponibilidad y reduce tiempos de recuperación	Si se replica un error o cifrado malicioso, el problema se copia al sitio alternativo
Backup	Recuperación de datos o sistemas a un punto anterior	Alta disponibilidad inmediata por sí solo

Ejemplo: un servidor con discos redundantes puede seguir funcionando si falla un disco. Pero si una base de datos se corrompe por error de software, el RAID conservará la corrupción. Para volver a un punto anterior se necesita backup.

La replicación debe combinarse con versiones históricas, copias inmutables o backups separados.

1.11 Seguridad de las copias de backup

Las copias contienen información tan valiosa como los sistemas originales y deben protegerse con controles equivalentes.

Control	Por qué es necesario
Cifrado en tránsito	Protege los datos mientras se transfieren hacia el destino de backup
Cifrado en reposo	Protege los datos almacenados en el destino de backup

Control	Por qué es necesario
Control de acceso y MFA	Evita que cualquier usuario pueda borrar o modificar copias
Cuentas separadas de producción	Si el atacante obtiene las credenciales del entorno productivo, no debe poder alcanzar los backups
Registro de auditoría	Permite saber quién accedió, modificó o intentó eliminar una copia
Inmutabilidad	Impide modificaciones aunque el atacante tenga privilegios elevados

1.12 El restore: proceso, tipos y modalidades

1.12.1 El restore como prueba de verdad

“Un backup que no se prueba, no existe.”

Un backup que nunca fue probado es una promesa sin verificar. Muchas organizaciones descubren que sus copias eran incompletas, corruptas o inaccesibles recién cuando enfrentan una emergencia real.

1.12.2 Qué debe verificar una prueba de restore

Elemento	Qué verifica
La copia existe	El archivo o repositorio está disponible y accesible
Puede leerse	No está corrupto ni inaccesible
Contiene los datos esperados	No falta información crítica

Elemento	Qué verifica
Puede restaurarse dentro del RTO	El tiempo real de recuperación es aceptable
La información es consistente	Los datos restaurados son coherentes y utilizables
El personal sabe ejecutarlo	No depende de una sola persona que puede estar ausente
La documentación está actualizada	El procedimiento escrito coincide con el proceso real

1.12.3 Proceso de restore paso a paso

1. **Identificar** — Determinar con precisión qué datos o sistemas necesitan restaurarse.
2. **Localizar** — Encontrar la copia adecuada (la más reciente o la que corresponde al punto de recuperación deseado).
3. **Preparar** — Disponer del entorno necesario: hardware, software, permisos y recursos humanos.
4. **Restaurar** — Ejecutar el proceso técnico de restauración de datos.
5. **Verificar** — Validar la integridad y el funcionamiento correcto del sistema restaurado.
6. **Documentar** — Registrar qué ocurrió, qué se hizo, cuánto tiempo llevó y qué lecciones se obtuvieron.

1.12.4 Tipos de restore según el alcance

Tipo	Cuándo se usa
Archivo individual	Un documento específico fue eliminado o corrompido
Carpeta o directorio	Se perdió un conjunto de archivos relacionados
Base de datos completa	El sistema de gestión no puede operar por corrupción de datos
Punto temporal de base de datos	Se detectó un error o eliminación masiva en un momento determinado
Bare-metal restore	Recuperación completa de un equipo físico desde cero
Máquina virtual completa	Se perdió o corrompió un servidor virtualizado
Restore granular	Se necesita recuperar un correo específico, una tabla o un objeto dentro de un sistema
Restore de sitio completo	Una sede o toda la infraestructura debe reconstituirse

1.12.5 Modalidades de restauración según la ubicación

Modalidad	Uso recomendado
Ubicación original	Retorna rápidamente al esquema habitual; requiere certeza de que la versión respaldada es correcta y que la causa del problema fue corregida

Modalidad	Uso recomendado
Ubicación alternativa	Pruebas, comparación, análisis y validación antes de pasar a producción
Carpeta única	Recuperación parcial de documentos para revisión sin mezclarlos con versiones activas
Sitio alternativo	Continuidad ante caída del sitio principal

Sobre el reemplazo de archivos: si una carpeta contiene quinientos archivos y solo tres fueron eliminados por error, restaurar toda la carpeta reemplazando podría borrar cambios recientes en los otros cuatrocientos noventa y siete. Un procedimiento adecuado permite recuperar solo lo necesario.

1.13 DRP, planes de contingencia y BCP

1.13.1 Plan de recuperación de desastres (DRP)

El DRP organiza la recuperación tecnológica ante eventos graves. Debe incluir:

Elemento del DRP	Finalidad
Inventario de sistemas críticos	Saber qué debe recuperarse primero
Dependencias entre sistemas	Evitar restaurar en orden incorrecto
RTO y RPO por sistema	Definir exigencias de recuperación
Responsables y contactos	Reducir improvisación
Procedimientos de restauración	Guiar acciones técnicas
Credenciales de emergencia	Acceso en condiciones de crisis

Elemento del DRP	Finalidad
Pruebas periódicas	Confirmar viabilidad real

Ejemplo: ante la pérdida del centro principal, el DRP puede indicar que primero se recupera conectividad, luego identidad y accesos, luego bases de datos, luego facturación y finalmente reportes.

1.13.2 Planes de contingencia

Los planes de contingencia son procedimientos alternativos para operar mientras se recupera el servicio normal.

Situación	Contingencia posible
Caída del sistema de ventas	Registro manual prenumerado de pedidos
Caída del correo	Canal alternativo aprobado para comunicaciones críticas
Falta de conectividad	Procedimiento local temporal y carga posterior
Indisponibilidad de proveedor	Activación de proveedor alternativo o proceso manual

Un plan de contingencia debe indicar cuándo se activa, quién lo activa, qué límites tiene, cómo se registran operaciones, cómo se regulariza luego y quién aprueba excepciones. La contingencia no debe abrir riesgos mayores que la falla original.

1.13.3 Plan de continuidad del negocio (BCP)

Aspecto	DRP	BCP
Foco	Recuperación tecnológica	Continuidad del negocio completo

Aspecto	DRP	BCP
Incluye	Sistemas, redes, bases, aplicaciones	Personas, procesos, proveedores y comunicación
Responsable típico	TI y seguridad	Dirección, administración y áreas críticas
Objetivo	Restaurar capacidades tecnológicas	Mantener funciones esenciales del negocio

Ejemplo: si una oficina queda inaccesible, el DRP define cómo estarán disponibles los sistemas. El BCP define cómo trabajará el personal, cómo se atenderá a clientes, cómo se aprobarán pagos y cómo se comunicará la situación.

1.13.4 Cadena de continuidad

Backup → Recuperación → DRP → BCP forman una cadena. Si uno de los eslabones falla, la continuidad puede verse afectada. Una organización puede tener backups y no tener DRP; en ese caso, quizá tenga datos pero no un procedimiento claro para restaurar sistemas. También puede tener DRP y no tener BCP; en ese caso, puede recuperar servidores pero no saber cómo operar las áreas críticas.

1.14 Amenazas que justifican la política de backup

Amenaza	Descripción
Ransomware	Malware que cifra los datos y exige un rescate. Puede también atacar las copias de seguridad si estas no están aisladas.
Error humano	Eliminación accidental de archivos o bases de datos críticas.
Desastre físico	Incendios, inundaciones, terremotos, cortes de energía que destruyen infraestructura.

Amenaza	Descripción
Corrupción de datos	Errores de hardware, software o humanos que deterioran la integridad de los datos.
Falla de hardware	Discos duros defectuosos, errores de sistema operativo, actualizaciones fallidas.

1.15 Verificación y pruebas periódicas

1.15.1 Tipos de pruebas

Tipo de prueba	Qué verifica
Pruebas de restauración	Que el proceso de restore funciona correctamente y los datos son recuperables y utilizables
Pruebas de integridad	Que el contenido de la copia es íntegro mediante comparación de checksums o hashes
Pruebas periódicas de desastre	Simulación de escenarios (disaster recovery drills) para evaluar la capacidad real de recuperación

1.15.2 Evidencia de auditoría

Evidencia	Qué demuestra
Reporte de backup	Que la copia se ejecutó
Log sin errores	Que no hubo fallas visibles

Evidencia	Qué demuestra
Prueba de restauración	Que la copia puede usarse
Medición de tiempo real	Que se cumple o no se cumple el RTO
Validación funcional	Que el dato restaurado sirve al negocio
Registro de responsable	Que existe rendición de cuentas

No basta con afirmar que existen copias. Debe demostrarse que pueden restaurarse.

1.16 Indicadores de gestión

Indicador	Qué permite observar
Porcentaje de backups exitosos	Confiabilidad del proceso de copia
Cantidad de fallas por mes	Estabilidad del esquema de respaldo
Tiempo promedio de restauración	Capacidad real de recuperación
Porcentaje de restauraciones probadas	Evidencia de recuperabilidad
Cumplimiento de RTO	Si se recupera dentro del tiempo requerido
Cumplimiento de RPO	Si se pierde menos información que el máximo aceptado
Cantidad de sistemas sin respaldo	Brechas de cobertura
Antigüedad de la última prueba	Riesgo por falta de validación reciente
Cantidad de accesos a backups	Control sobre datos sensibles
Espacio disponible	Capacidad de sostener la política definida

Un indicador aislado puede ser engañoso. Si el 98% de los backups finaliza correctamente, pero nunca se probó una restauración, el riesgo sigue siendo alto.

1.17 Ciclo de vida de la política de backup

Una política de backup no es un documento que se configura una vez. Es un proceso continuo:

Paso	Acción
1	Identificar activos críticos
2	Clasificar datos por valor e impacto
3	Definir RPO y RTO por sistema
4	Seleccionar medios y herramientas
5	Configurar frecuencia y retención
6	Proteger copias con cifrado, accesos y controles
7	Monitorear ejecuciones diariamente
8	Probar restores periódicamente
9	Documentar procedimientos y resultados
10	Revisar y actualizar ante cambios en la organización

1.18 Responsabilidades administrativas

El backup no es responsabilidad exclusiva del área técnica. La administración debe:

Responsabilidad	Quién interviene
Definir qué información es crítica	Alta dirección y áreas usuarias
Aprobar presupuesto para la estrategia	Finanzas y dirección
Establecer RPO y RTO por proceso de negocio	Administración, TI y área usuaria

Responsabilidad	Quién interviene
Verificar que se realizan pruebas de restore	Auditoría interna
Asegurar que la política está documentada	TI y gestión de calidad
Controlar proveedores de servicios de backup	Compras, legal y TI
Revisar el cumplimiento con obligaciones legales de retención	Legal y compliance

1.19 Errores frecuentes en estrategias de backup

Error	Consecuencia
No probar restauraciones	La copia puede existir pero no ser recuperable
Confundir sincronización con backup	Si se borra un archivo local y se sincroniza, se borra también en la nube
Mantener el backup en el mismo equipo que los datos originales	Una falla del equipo destruye datos y copia a la vez
Dejar el disco de backup siempre conectado	Un ransomware puede cifrarlo junto con el sistema
No cifrar copias externas	Si la copia se extravía o es robada, la información queda expuesta
No definir RPO ni RTO	Sin criterios, no hay forma de saber si la estrategia es adecuada

Error	Consecuencia
No proteger backups frente a borrado privilegiado	Un atacante con credenciales administrativas puede eliminar todas las copias
No documentar el procedimiento de restore	Si el responsable técnico no está disponible, nadie sabe cómo recuperar
No revisar la política cuando cambia la organización	Una política válida hace dos años puede ser insuficiente hoy
Confiar solo en RAID o replicación	No protegen ante borrado accidental, ransomware ni corrupción lógica

1.20 Caso integrador

Una empresa comercial utiliza un sistema para ventas, facturación, cuentas corrientes, cobranzas y reportes contables. La información se guarda en un servidor local y se sincroniza con una carpeta en la nube. El área administrativa considera que esa sincronización es suficiente como backup.

Un día, un ransomware cifra los archivos del servidor. La sincronización replica los archivos cifrados en la nube. La empresa descubre que no tenía versiones históricas protegidas, que las copias no eran inmutables y que nunca se había probado una restauración completa.

Elemento	Análisis
Error principal	Confundir sincronización con backup
Riesgo materializado	Pérdida de disponibilidad e integridad de datos

Elemento	Análisis
Impacto	Interrupción de ventas, facturación y cobranzas
Controles ausentes	Versionado, copia aislada, prueba de restauración
Decisión pendiente	Definir RTO, RPO y estrategia 3-2-1-1-0
Aprendizaje	La continuidad debe probarse antes del incidente

Este caso muestra que la existencia de una copia no garantiza recuperabilidad. La administración debe exigir evidencia de restauración, no solo evidencia de copia.

1.21 Ideas clave

- Los datos de una organización son **irrecuperables**: no existen en el mercado, no pueden comprarse ni conseguirse de terceros. La infraestructura tecnológica es reemplazable; la información que contiene, no.
- El **backup sin restore probado** es una promesa sin verificar. Solo cuenta como backup lo que puede restaurarse exitosamente dentro del tiempo requerido.
- El **RPO** define cuánta información puede perderse. El **RTO** define cuánto tiempo puede estar caído el sistema. Ambos son decisiones de negocio, no solo técnicas, y determinan directamente el costo de la solución.
- El backup **incremental** requiere menos espacio por copia pero más piezas para restaurar. El backup **diferencial** requiere más espacio pero simplifica la restauración a solo dos piezas: el último full y el último diferencial.
- La sincronización de archivos en la nube **no es un backup**. Si se elimina un archivo y la eliminación se sincroniza, el archivo desaparece también del repositorio.

- El **esquema 3-2-1** — tres copias, dos medios diferentes, una copia fuera del sitio — sigue siendo un estándar válido, pero debe reforzarse con **copias inmutables** ante el riesgo de ransomware.
- Los backups contienen información tan valiosa como los sistemas originales y deben protegerse con el **mismo nivel de seguridad**: cifrado, control de acceso, MFA y separación de cuentas.
- **RAID, redundancia y replicación** mejoran la disponibilidad, pero no reemplazan el backup ni permiten recuperar un punto anterior en el tiempo.
- El backup es una **inversión en continuidad operativa**, no un gasto accesorio. El costo de no tenerlo —pérdida de ventas, sanciones, reconstrucción manual, pago de rescates— es sistemáticamente mayor que el costo de implementarlo.

1.22 Preguntas de evaluación

1. ¿Por qué los datos de una organización se consideran irrecuperables y qué consecuencias tiene esa característica para la política de backup?
2. ¿Cuál es la diferencia entre backup incremental y backup diferencial? Utilice el ejemplo de la quincena para explicar cuántas piezas se necesitan para restaurar en cada caso.
3. Una empresa tiene backup full los domingos y backups incrementales de lunes a sábado. El sistema falla el miércoles a las 15:00 hs. Describa paso a paso la secuencia de restore necesaria e identifique qué información no podrá recuperarse.
4. ¿Qué son el RPO y el RTO, y por qué su definición es una decisión de administración y no exclusivamente técnica?
5. ¿Por qué sincronizar archivos en servicios como OneDrive o Google Drive no equivale a tener una estrategia de backup? ¿Qué riesgo concreto introduce?
6. ¿En qué consiste el esquema 3-2-1 y por qué el avance del ransomware llevó a agregar copias inmutables o air-gapped como extensión de ese esquema?

7. ¿Por qué un snapshot no siempre puede considerarse un backup suficiente? ¿En qué situaciones es útil y en cuáles no protege adecuadamente?
8. ¿Qué debería incluir una prueba periódica de restore y por qué no alcanza con que el software reporte “backup exitoso”?
9. ¿Por qué RAID no debe considerarse backup? ¿Qué situaciones resuelve y cuáles no?
10. Una empresa descubre que su administrador de sistemas es la única persona que conoce el procedimiento y las credenciales de restore. ¿Qué riesgos organizacionales genera esa situación y cómo deberían resolverse?
11. ¿Cuál es la diferencia entre backup, recuperación y continuidad del negocio?
12. ¿Qué diferencia existe entre DRP y BCP? ¿Por qué una organización puede necesitar ambos aunque tenga buenas políticas de backup?
13. ¿Cuándo conviene restaurar en ubicación original y cuándo en ubicación alternativa? ¿Qué riesgo implica reemplazar archivos sin análisis previo?
14. ¿Qué indicadores deberían presentarse a la dirección para demostrar que el proceso de backup y recuperación funciona correctamente?
15. Analice el caso integrador e indique qué decisiones de administración habrían reducido el impacto del incidente.

1.23 Glosario

Término	Traducción / Explicación
Air gap	Aislamiento físico o lógico. Una copia separada de la red principal: una cinta desconectada, un disco retirado físicamente o un repositorio cloud configurado para impedir modificaciones externas.

Término	Traducción / Explicación
BaaS	*Backup as a Service*. Modelo en el que un proveedor externo ofrece una solución administrada de copias de seguridad que incluye software, almacenamiento, monitoreo y soporte.
Backup	Copia de respaldo. Copia de datos, sistemas o configuraciones destinada a permitir recuperación posterior.
Bare-metal restore	Restauración desde cero. Recuperación completa de un equipo físico o servidor, reconstruyendo sistema operativo, aplicaciones y datos desde una copia de seguridad.
BC / BCP	*Business Continuity / Business Continuity Plan*. Continuidad del negocio / Plan de continuidad del negocio. Capacidad de sostener o restablecer procesos críticos durante una crisis. Incluye tecnología, personas, procesos, proveedores, instalaciones y comunicación.
CDP	*Continuous Data Protection*. Protección continua de datos. Mecanismo que registra cambios de forma constante o casi constante, permitiendo recuperar información en puntos muy cercanos al momento del incidente.
Checksum / Hash	Huella digital calculada sobre datos. Permite verificar si el contenido cambió o fue corrompido.
Cloud Backup	Backup en la nube. Respaldo almacenado en infraestructura remota provista como servicio.
Cold storage	Almacenamiento frío. Tipo de almacenamiento cloud de bajo costo orientado a datos que se consultan raramente, con mayor tiempo de recuperación.

Término	Traducción / Explicación
Deep archive	Archivo profundo. Tipo de almacenamiento cloud para retención de largo plazo, con muy bajo costo pero tiempos de recuperación lentos.
Differential Backup	Backup diferencial. Copia todos los cambios realizados desde el último backup completo.
DR / DRP	*Disaster Recovery* / *Disaster Recovery Plan*. Recuperación ante desastres / Plan de recuperación de desastres. Conjunto de procesos, tecnologías y procedimientos para restablecer sistemas críticos luego de una interrupción grave.
DRaaS	*Disaster Recovery as a Service*. Recuperación ante desastres como servicio. Permite replicar sistemas en infraestructura alternativa y activarlos si el sitio principal falla.
Encryption at rest	Cifrado en reposo. Protección de datos almacenados mediante cifrado, de modo que sean ilegibles si el medio es robado o accedido sin autorización.
Encryption in transit	Cifrado en tránsito. Protección de datos mientras se transmiten entre sistemas, evitando que puedan ser interceptados y leídos.
Full Backup	Backup completo. Copia todos los datos seleccionados. Es el punto de partida para cualquier cadena de restore.
Immutable Backup	Backup inmutable. Copia que no puede modificarse ni eliminarse durante un período definido, ni siquiera por usuarios con altos privilegios administrativos.
Incremental Backup	Backup incremental. Copia solo los cambios realizados desde la última copia, sea completa o incremental.

Término	Traducción / Explicación
MFA	*Multi-Factor Authentication*. Autenticación multifactor. Mecanismo que exige más de un factor de verificación para acceder a un sistema o repositorio.
Mirror Backup	Copia espejo. Réplica 1:1 en tiempo real o casi real de los datos de origen. Alta disponibilidad, pero si se elimina un archivo en el origen también se elimina en el espejo.
MTD	*Maximum Tolerable Downtime*. Máximo tiempo de inactividad tolerable. Tiempo total máximo en que los sistemas deben estar disponibles para el negocio; superarlo compromete la viabilidad operativa.
NAS	*Network Attached Storage*. Almacenamiento conectado a la red. Dispositivo que centraliza copias de múltiples equipos, accesible por red local.
Off-site	Fuera del sitio. Ubicación externa a las instalaciones principales donde se conserva al menos una copia de seguridad, como protección ante desastres físicos.
Point-in-time recovery	Recuperación a un punto en el tiempo. Restauración de una base de datos a un estado exacto en un momento determinado, posible cuando existen backups de logs de transacciones.
RAID	*Redundant Array of Independent Disks*. Conjunto redundante de discos independientes. Mejora disponibilidad o tolerancia a fallas físicas, pero no reemplaza el backup.
Ransomware	Software malicioso que cifra los datos de la víctima y exige un pago para restaurar el acceso. Suele intentar destruir o cifrar también los backups antes de activarse.

Término	Traducción / Explicación
Recovery	Recuperación. Proceso de volver a poner datos, sistemas o servicios en condiciones operativas.
RPO	*Recovery Point Objective*. Objetivo de punto de recuperación. Indica cuánta información puede perder la organización, medida en tiempo, ante un incidente.
RTO	*Recovery Time Objective*. Objetivo de tiempo de recuperación. Indica cuánto tiempo puede estar caído un sistema antes de generar un impacto inaceptable para el negocio.
SAN	*Storage Area Network*. Red de área de almacenamiento. Infraestructura de almacenamiento de alto rendimiento, habitual en centros de datos empresariales.
SaaS	*Software as a Service*. Software como servicio. Los datos generados en plataformas SaaS también requieren estrategia de backup independiente.
SLA	*Service Level Agreement*. Acuerdo de nivel de servicio. Compromiso formal sobre disponibilidad, tiempos de respuesta o calidad del servicio; incluye parámetros de RTO y RPO.
Snapshot	Instantánea. Captura del estado de un sistema, volumen, máquina virtual o base de datos en un momento determinado. Útil como punto de control, pero no siempre equivale a un backup independiente.
Synthetic Full Backup	Backup completo sintético. Copia completa construida combinando un full anterior con incrementales posteriores, sin releer el sistema de producción.

Término	Traducción / Explicación
Tape Backup	Backup en cinta. Copia almacenada en cinta magnética, útil para archivo, respaldo fuera de línea y retención prolongada.
Transaction Log Backup	Backup del registro de transacciones. Copia de los registros de operaciones de una base de datos, que permite restaurar a un punto específico en el tiempo.
Versioning	Versionado. Conservación de versiones anteriores de archivos o datos para recuperar estados previos.
VM	*Virtual Machine*. Máquina virtual. Servidor virtualizado que se ejecuta sobre infraestructura física compartida. Puede respaldarse como unidad completa.