Engineer

Recuperación ante desastres

recuperar el servicio tras un desastre con un plan probado

Qué es

La recuperación ante desastres es la parte de la planificación de contingencias que cubre el peor caso: se ha perdido el lugar donde funciona un sistema, o resulta inaccesible durante mucho tiempo, y hay que reconstruir el sistema en otro lugar a partir de copias. La guía de planificación de contingencias para sistemas de información federales del NIST, SP 800-34, revisión 1 de 2010, define el plan de recuperación ante desastres como un plan escrito para recuperar uno o varios sistemas de información en unas instalaciones alternativas tras un fallo grave de hardware o software, o la destrucción de las instalaciones. Su alcance es limitado. La guía lo reserva para interrupciones graves, normalmente físicas, que impiden acceder a las instalaciones principales durante un período prolongado, y solo cubre las interrupciones que exigen un traslado.

Ese alcance limitado lo distingue de otros planes afines. En el vocabulario de la guía, un plan de contingencia de un sistema de información restablece un solo sistema donde se encuentre, ya sea tras el fallo de un disco o la corrupción de una base de datos. El plan de recuperación ante desastres está ligado a una sede: traslada las operaciones a la ubicación alternativa y, desde allí, cada sistema se pone en marcha mediante su propio plan de contingencia. Un plan para una base de datos y otro para la pérdida de un centro de datos entero, una región de nube o una cuenta de proveedor son documentos distintos, con responsables distintos; confundirlos es la forma de que una empresa acabe sin ninguno de los dos.

Tres medidas convierten el plan en algo verificable, más allá de una intención. El tiempo máximo de inactividad tolerable (MTD) es la duración total de la interrupción que el responsable del sistema está dispuesto a aceptar. El objetivo de tiempo de recuperación (RTO) es el tiempo máximo que un recurso del sistema puede permanecer indisponible antes de que los daños para otros sistemas y para el negocio resulten inaceptables. Como después también hay que

volver a procesar el trabajo interrumpido, la guía indica que el RTO debe ser normalmente menor que el MTD. El objetivo de punto de recuperación (RPO) mira hacia atrás: es el momento anterior a la interrupción hasta el que se pueden recuperar los datos a partir de la copia de seguridad más reciente, y expresa cuánta pérdida de datos puede admitir el negocio. En términos sencillos, el RTO indica cuánto tiempo permanece fuera de servicio y el RPO, cuánto trabajo pierde.

La sede alternativa puede tener distintos niveles de preparación. Una sede fría solo ofrece espacio e infraestructura; una templada está parcialmente equipada y una caliente está completamente equipada y cuenta con personal. La guía añade sedes móviles, que en muchos casos pueden entregarse en un plazo de 24 horas, tras lo cual empieza su instalación, y sedes en espejo: la opción más cara, a la que atribuye una «disponibilidad de prácticamente el 100 por ciento». Las sedes frías son las más baratas de mantener y pueden requerir bastante tiempo para equiparlas. Una segunda región de nube o un segundo proveedor cumplen hoy la misma función para la mayoría del software, y la relación entre lo que está preparado y el coste de mantenerlo así es la misma.

Utilice el concepto en una decisión

Aplique «¿Qué es la recuperación ante desastres?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Copias de seguridad que se prueban en vez de darse por buenas y un plan escrito para la mañana en que un servidor no vuelva a encenderse.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. 100 copias críticas automatizadas con Barman — 100 copias críticas automatizadas en las bases de datos

100 copias críticas automatizadas con Barman Póngase en contacto →

Por qué importa

Una copia de seguridad es una copia, y por sí sola no ejecuta nada. Pasar de ella a un sistema en funcionamiento también requiere el software que la lee, las claves que la descifran, servidores y una red donde ejecutarlo, la configuración que los conecta y alguien que conozca el orden de los pasos. Cualquiera de esos elementos que solo existiera en la sede perdida se perdió con ella. La recuperación ante desastres es la disciplina que se ocupa de que todos sobrevivan al mismo suceso y que el camino de la copia al servicio se haya recorrido antes de necesitarlo.

Los datos recuperables solo llegan hasta la última copia que se pueda restaurar, sea cual sea el RPO que deba cumplir la programación de las copias de seguridad. Un trabajo nocturno que lleva una semana fallando en silencio deja en riesgo los datos de una semana, diga lo que diga el documento de políticas. La guía del NIST señala lo mismo para las cintas: recomienda probar las copias periódicamente para confirmar que los datos se almacenan correctamente y que los archivos pueden recuperarse sin errores ni pérdidas. Un indicador verde en un trabajo de copia demuestra que se escribió algo. Solo una restauración demuestra que se puede volver a leer.

El plan también se deteriora. Las personas se marchan, se sustituyen servidores, los proveedores rediseñan sus consolas y caducan las contraseñas del manual de operaciones. De los siete pasos que el NIST establece para planificar contingencias, los dos últimos son las pruebas, la formación y los ejercicios, y el mantenimiento del plan. La guía pide que sea un documento vivo, revisado al menos una vez al año y siempre que cambien significativamente el sistema o los recursos utilizados para recuperarlo. Un plan que nunca se ha ensayado suele fallar por detalles que nadie pensó en escribir: el orden de arranque de los servicios, un registro DNS con un tiempo de vida de un día o la única credencial que se guardaba en la máquina que ya no está.

Para los equipos de software, el desastre suele afectar a una cuenta más que a un edificio. Un proyecto de nube eliminado, un acceso de administrador comprometido, una cuenta de proveedor suspendida o un comando destructivo ejecutado contra producción eliminan el acceso al sistema de forma tan completa como una inundación. Los servidores en espera no protegen frente al último caso: aplican un `DROP TABLE` equivocado en unos instantes, igual que cualquier otro cambio.

Cómo se aplica en la práctica

En una base de datos PostgreSQL, un intervalo de pérdida potencial de datos mucho menor que el tiempo entre dos copias se consigue mediante el archivado continuo del registro de escritura anticipada (WAL), además de una copia base. El servidor copia cada segmento WAL terminado a un lugar seguro y la restauración reproduce esos segmentos sobre la copia base hasta cualquier momento elegido desde que se realizó esa copia:

```
# postgresql.conf on the protected server
wal_level = replica
archive_mode = on
archive_command = 'test ! -f /mnt/archive/%f && cp %p /mnt/archive/%f'
```

Para restaurar, se extrae una copia base en un directorio de datos nuevo, se coloca en él un archivo vacío llamado `recovery.signal` y se indica en la configuración de recuperación dónde se guardan los segmentos archivados y dónde detenerse:

```
restore_command = 'cp /mnt/archive/%f %p'
recovery_target_time = '2026-03-10 17:14:00+01'
recovery_target_action = 'pause'
```

La documentación de PostgreSQL cuenta la situación para la que existen estos ajustes: alguien elimina una tabla crítica un martes a las 5:15 de la tarde, lo descubre el miércoles al mediodía y restaura hasta las 5:14. Al alcanzar el objetivo, la acción predeterminada es pausar, para que las consultas permitan comprobar que es el momento correcto antes de promover el servidor para aceptar conexiones. Si no lo es, se apaga el servidor, se fija un objetivo posterior y se vuelve a iniciar. El momento de recuperación elegido debe ser posterior a la finalización de la copia base, y la documentación aconseja configurar y probar el archivado antes de realizar la primera copia base. Cuando termina la recuperación, el servidor elimina `recovery.signal` para no volver a entrar en recuperación por accidente.

Engineer ApS ofrece copias de seguridad y recuperación ante desastres como servicio, descrito como copias que se prueban en lugar de darse por válidas y un plan escrito para la mañana en que un servidor no vuelve a arrancar. Dos páginas del portafolio muestran qué significa. En copias de seguridad y recuperación ante desastres como código, trabajo realizado en un puesto desempeñado desde 2025, la retención de las copias se configuró en Bicep junto a la base de datos, de modo que la restauración a un momento dado forma parte de la plantilla y no de un ajuste que alguien seleccionó una vez en un portal. También se definió como código el entorno de la base de datos: difícilmente se puede considerar recuperada una base de datos restaurada en un entorno reconstruido de memoria. Después se auditó y documentó la situación de recuperación,

indicando sus carencias: la redundancia geográfica estaba desactivada y el objetivo de tiempo de recuperación era una propuesta, no una medición, porque no se había realizado ningún simulacro.

La automatización de las copias y de las pruebas de restauración de la empresa se diseñó para llevar la recuperación más allá de una instantánea del proveedor. Un rol de Ansible instala scripts de restic y unidades de systemd para un volcado de base de datos cuando está configurado, instantáneas cifradas y deduplicadas en el almacenamiento de otro proveedor por SFTP, la eliminación de copias según su retención y comprobaciones de integridad. Un flujo mensual separado restaura un archivo conocido en una ubicación temporal y compara sus bytes. La copia y la restauración tienen señales de éxito separadas, la frase de contraseña procede de un archivo protegido y los temporizadores dependen de un repositorio configurado. Esos controles están implementados; una recuperación real es un entregable aparte. El registro de implementación del 2026-10-27 indica que los temporizadores estaban desactivados por no haber repositorio y no recoge ninguna restauración real completada. Por tanto, respalda el trabajo de automatización, no un compromiso de tiempo de recuperación ni la afirmación de que la empresa ya puede afrontar con seguridad la pérdida del host.

Dónde surgen los problemas

La copia nunca se ha restaurado. Un trabajo que informa de éxito cada noche no dice si su salida puede leerse, descifrarse y cargarse; la primera restauración real es un mal momento para descubrirlo. Programe restauraciones igual que programa copias: una comprobación automatizada que extraiga datos conocidos y los compare, y una restauración completa en un entorno limpio con suficiente frecuencia para que su duración sea una cifra medida.

La copia comparte el destino del original. Una instantánea en la misma cuenta de nube, un disco de copias en el mismo bastidor o un bucket de archivo detrás del mismo acceso de administrador caen con lo que derribe al sistema principal. La guía del NIST pide elegir almacenamiento fuera de la sede y sedes alternativas en función de lo improbable que sea que sufran el mismo desastre. Mantenga al menos una copia con otro proveedor o en otra cuenta con credenciales separadas, y guarde las claves de descifrado en un lugar que no dependa de los sistemas que protegen.

Solo se planificó la recuperación de los datos. Restaurar una base de datos es una pequeña parte de recuperar un servicio si los servidores, las reglas de cortafuegos, DNS, los certificados y los secretos que la rodean tienen que reconstruirse de memoria. Defina el entorno mediante infraestructura como código bajo control de versiones e incluya su reconstrucción en el simulacro, además de cargar los datos.

Los objetivos son conjeturas. Un RTO escrito en un documento sin un simulacro que lo respalde es una propuesta; un RPO que supone que todas las copias tuvieron éxito es optimista. Mida ambos en un ejercicio. El NIST distingue los ejercicios de mesa, que solo consisten en debatir y no despliegan equipos, de los funcionales, que simulan las operaciones, hasta llegar a los ejercicios a escala completa que cubren todos los elementos del plan. Las cifras proceden del segundo tipo.

Se cuenta un servidor en espera como copia. Un servidor en espera o una base de datos con replicación geográfica protegen frente a la pérdida de hardware, pero copian las eliminaciones, la corrupción y los archivos cifrados por ransomware con la misma fidelidad que las escrituras correctas. Mantenga copias de momentos concretos que un error en el sistema principal no pueda alcanzar, y consérvelas durante más tiempo del que suele tardarse en detectar un error.

El plan describe el sistema del año pasado. Un manual de operaciones que enumera servidores retirados, personas que se han marchado y contraseñas que ya no funcionan ralentiza la recuperación en lugar de guiarla. Revise el plan después de cada cambio significativo y cada simulacro, registre lo que salió mal en él y revise todavía más a menudo las partes que más cambian, como las listas de contactos, tal como también recomienda el NIST.

Lecturas adicionales

- SP 800-34, revisión 1: guía de planificación de contingencias para sistemas de información federales — La guía completa: definición y alcance del DRP, los siete pasos de planificación, MTD, RTO y RPO, sedes alternativas y tipos de ejercicios, con plantillas de planes.
- Archivado continuo y recuperación a un momento dado (PITR) — El capítulo de PostgreSQL 18 sobre archivado WAL, copias base y restauración hasta un momento elegido.
- Registro de escritura anticipada — La referencia de configuración para `archive_command` , `restore_command` y los ajustes del objetivo de recuperación.

Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es la recuperación ante desastres?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/disaster-recovery/