RPO vs. RTO

El **Objetivo de Punto de Recuperación (RPO)** y el **Objetivo de Tiempo de Recuperación (RTO)** son dos de los parámetros más cruciales en la planificación de la **Continuidad del Negocio (BC)** y la **Recuperación ante Desastres (DR).** Definen cuánto riesgo es aceptable para una organización en caso de una interrupción o fallo.

1. RPO (Recovery Point Objective) - Objetivo de Punto de Recuperación

El **RPO** responde a la pregunta: **"¿Cuánta información o datos podemos permitirnos perder?"**

Aspecto	**Detalle**
Definición	Es el **período máximo de tiempo** aceptable en el que los datos se pueden perder a causa de un incidente.
Métrica Clave	**Pérdida de datos.** Se mide en unidades de **tiempo** (segundos, minutos, horas) que transcurren entre la última copia de seguridad válida y el momento del fallo.
Enfoque	Se centra en la **frecuencia** con la que deben realizarse las copias de seguridad o la replicación.
Impacto	Dicta las tecnologías y estrategias de **copia de seguridad/replicación** (ej. si el RPO es de 5 minutos, la réplica debe ser casi continua).

Ejemplo Práctico: Si el RPO de un sistema es de 1 hora, y el sistema falla a las 14:00h, la última copia de seguridad o réplica que se usará para restaurar debe ser, como máximo, de las 13:00h. Se perderán todos los datos generados entre las 13:00h y las 14:00h.

2. RTO (Recovery Time Objective) - Objetivo de Tiempo de Recuperación

El **RTO** responde a la pregunta: **"¿Cuánto tiempo puede estar el sistema inactivo?"**

Aspecto	Detalle
Definición	Es la **duración máxima aceptable** desde el momento de un fallo o desastre hasta que el sistema o proceso de negocio **vuelve a estar operativo** (incluso en una capacidad limitada o degradada).
Métrica Clave	**Tiempo de inactividad.** Se mide en unidades de **tiempo** (minutos, horas, días) desde la detección del incidente hasta la restauración.
Enfoque	Se centra en la **velocidad** con la que la infraestructura de TI y las aplicaciones pueden restaurarse.
Impacto	Dicta las estrategias de **infraestructura y tecnología** (ej. si el RTO es de 2 horas, debe haber una infraestructura de recuperación ante desastres (DR) preconfigurada y lista para entrar en línea rápidamente).

Ejemplo Práctico: Si el RTO de una aplicación es de 4 horas, y falla a las 14:00h, la aplicación debe estar completamente disponible y funcional de nuevo a más tardar a las 18:00h.

3. Principales Diferencias: RPO vs. RTO

La diferencia fundamental es lo que cada métrica busca mitigar:

Característica	RPO (Recovery Point Objective)	RTO (Recovery Time Objective)
Lo que mide	La **cantidad** de datos perdidos.	El **tiempo** que el negocio está parado.

Característica	RPO (Recovery Point Objective)	RTO (Recovery Time Objective)
Focus	La **pérdida de datos** aceptable.	El **tiempo de inactividad** aceptable.
Estrategia	Frecuencia de **Backups / Replicación.**	Velocidad de **Restauración / Conmutación por Error (Failover).**
Unidad de Medida	Tiempo (entre el último backup y el fallo).	Tiempo (entre el fallo y la reanudación del servicio).

Ejercicios de Cálculo y Práctica

A continuación, se presentan tres escenarios. El objetivo es determinar el RPO y el RTO.

Ejercicio 1: El Servidor de Correo Electrónico (Alta Prioridad)

Una empresa minorista depende en gran medida de su servidor de correo electrónico (Exchange) para gestionar pedidos urgentes y la comunicación con el cliente. La gerencia ha determinado lo siguiente:

1. **Impacto Máximo de Pérdida de Datos (RPO):** Perder más de **30 minutos** de correos electrónicos y pedidos se considera catastrófico e impacta directamente en los ingresos.
2. **Impacto Máximo por Inactividad (RTO):** El equipo de ventas no puede estar más de **4 horas** sin acceso al correo electrónico, incluso si se usa un sistema alternativo con funcionalidad limitada.

Pregunta: ¿Cuál es el RPO y el RTO de esta aplicación?

Ejercicio 2: El Sistema de Nóminas (Prioridad Media/Baja)

El sistema utilizado para calcular la nómina de los empleados se ejecuta una vez al mes, pero los datos se actualizan a diario con horas extras y cambios. El equipo de RR.HH. indica:

1. **Impacto Máximo de Pérdida de Datos (RPO):** Perder los datos de más de **24 horas** implica un trabajo manual excesivo y es inaceptable.
2. **Impacto Máximo por Inactividad (RTO):** Si el sistema falla, hay un proceso manual que puede usarse para pagar a los empleados. Por lo tanto, el sistema puede estar inactivo por un máximo de **48 horas** antes de que se convierta en una crisis seria.

Pregunta: ¿Cuál es el RPO y el RTO de esta aplicación?

Ejercicio 3: El Portal Web de Marketing (Prioridad Baja)

El portal web de marketing y noticias se actualiza ocasionalmente.

1. **Impacto Máximo de Pérdida de Datos (RPO):** Una pérdida de datos de hasta **7 días** es tolerable, ya que el contenido puede ser reconstruido a partir de borradores de documentos.
2. **Impacto Máximo por Inactividad (RTO):** El portal no genera ingresos directos, por lo que puede estar fuera de servicio hasta **5 días** antes de que la reputación de la empresa se vea gravemente afectada.

Pregunta: ¿Cuál es el RPO y el RTO de esta aplicación?

PLAN DE COPIAS DE SEGURIDAD

1. Servidor de Correo Electrónico (Alta Prioridad)

Objetivo	Valor Definido	Implicación Tecnológica
RPO	**30 minutos**	Se requiere una solución de **replicación continua o casi continua** para minimizar la pérdida de datos.
RTO	**4 horas**	Se necesita un sitio de recuperación **caliente (hot site)** o **tibio (warm site)** para garantizar un tiempo de activación rápido.

Plan de Copias de Seguridad Ideal

El enfoque para este escenario debe ser la **Replicación y Alta Disponibilidad (HA)**, no la copia de seguridad tradicional.

Componente	Frecuencia / Método	Propósito (RPO/RTO)
Replicación de Servidor	**Continua o Cada 15 min.**	Cumple con el **RPO de 30 min.** Se utiliza tecnología de **Replicación a Nivel de Bloque** (ej. VMware vSphere Replication, Hyper-V Replica, o Grupos de Disponibilidad de Bases de Datos - DAGs de Exchange).

Componente	Frecuencia / Método	Propósito (RPO/RTO)
Copia de Seguridad Tradicional	**Diaria (nocturna)**	Para la **recuperación a largo plazo** o **recuperación de un borrado accidental** (ej. un borrado de buzón de hace 3 semanas).
Estrategia de DR	**Failover Automatizado/Semiautomatizado**	Asegura el cumplimiento del **RTO de 4 horas** al permitir la activación del servidor de réplica con solo unos clics.
Almacenamiento	**SSD/SAN** en el sitio de DR	Reduce el tiempo de arranque y restauración para el RTO.

2. Sistema de Nóminas (Prioridad Media/Baja)

Objetivo	Valor Definido	Implicación Tecnológica
RPO	**24 horas**	La pérdida de un día de trabajo es aceptable, lo que permite un **único backup diario**.
RTO	**48 horas**	El proceso de restauración puede tardar hasta dos días, permitiendo el uso de **medios de backup externos** y una infraestructura de DR más simple.

Plan de Copias de Seguridad Ideal

El enfoque aquí es el **Backup Diario Diferencial** con una estrategia de **Recuperación a un Sitio Alterno (Cold Site)** o en la **Nube.**

Componente	**Frecuencia / Método**	**Propósito (RPO/RTO)**
Backup Completo	**Semanal (fin de semana)**	Base para la restauración completa.
Backup Diferencial	**Diario (nocturno)**	Captura los cambios de las últimas 24 horas para cumplir con el **RPO de 24 horas.**
Rotación de Medios	**Estrategia 3-2-1**	Copias locales, copias en la nube/externas y cintas.
Estrategia de DR	**Restauración en Infraestructura Virtual**	Se utiliza el **RTO de 48 horas** para transferir y restaurar el backup diario en un nuevo servidor virtualizado o en un entorno de Infraestructura como Servicio (IaaS) en la nube.

3. Portal Web de Marketing (Prioridad Baja)

Objetivo	**Valor Definido**	**Implicación Tecnológica**
RPO	**7 días**	Se acepta una pérdida de una semana, lo que permite un **backup semanal** de bajo costo.
RTO	**5 días**	Se necesita una restauración en línea más rápida que el RPO, lo que requiere un proceso de **reconstrucción** ágil, aunque la frecuencia de los datos no sea alta.

Plan de Copias de Seguridad Ideal

Según lo indicado ¿Cuál sería el plan de copias ideal?