CARICHAM
Centre of Excellence

arise

TRANSFORMACIÓN DIGITAL

Respaldo y resiliencia

Respaldo y resiliencia

Una vez que haya adoptado los distintos productos y servicios locales y en la nube de los que se ha hablado anteriormente, es esencial definir cómo protegerá esos datos en caso de desastre u otro incidente que los ponga en peligro. La creación de una empresa resiliente empieza por sus sistemas de información.

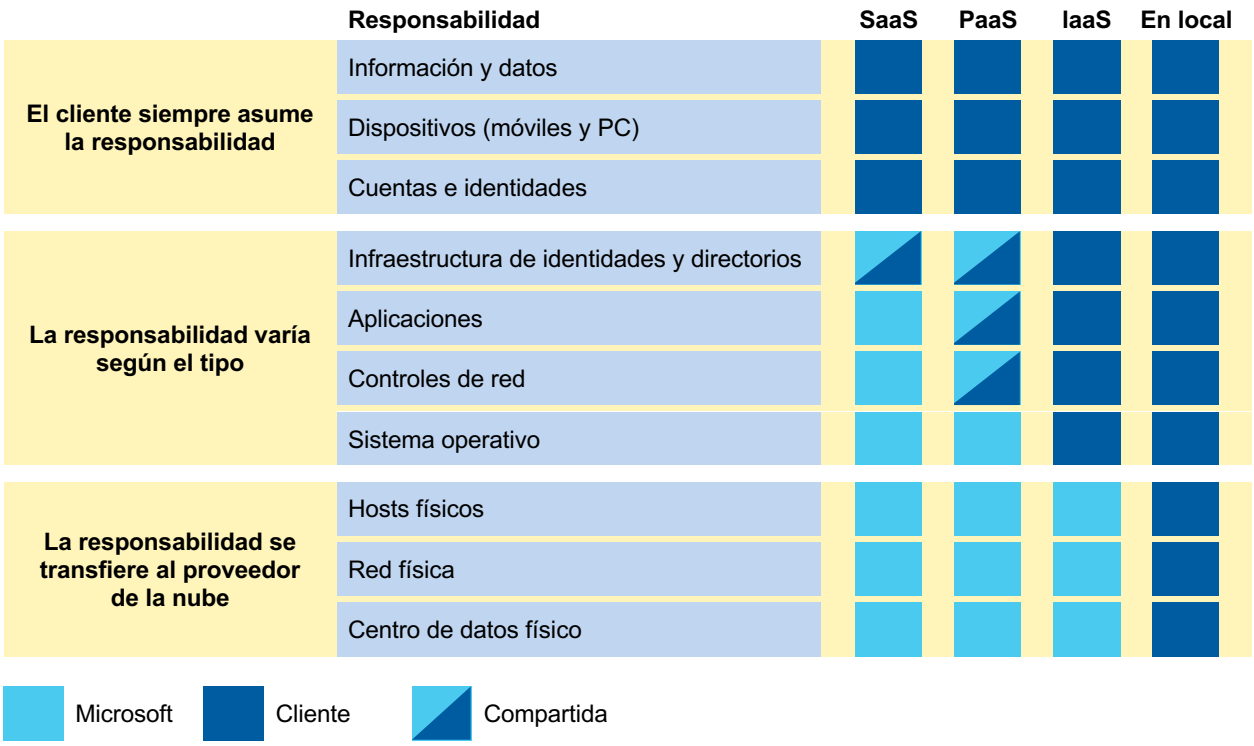
Las copias de seguridad deben considerarse parte de su estrategia global de ciberseguridad y resiliencia. Demasiado a menudo, las empresas no piensan lo suficiente en disponer de una robusta protección de los datos mediante copias de seguridad; sin embargo, estas constituyen la manera fundamental que tienen las empresas de proteger sus sistemas de información y sus datos.

En caso de desastre, la última línea de defensa son las copias de seguridad. Ya sea por un desastre natural, como un huracán o la erupción de un volcán, o por un incidente humano en el que sus datos se vean comprometidos o estén inaccesibles por cualquier otro motivo, la copia de seguridad, por su propia naturaleza, le proporciona una copia independiente de sus datos que puede utilizar para restablecer su actividad.

Esto es cada vez más importante a medida que el mundo avanza hacia una sociedad más conectada o de trabajo en remoto, lo que se traduce en que las empresas están desplegando aplicaciones en la nube para la productividad y los procesos empresariales.

Los productos de software como servicio basados en la nube suelen pasarse por alto, ya que a menudo se ejecutan en ubicaciones de alta seguridad y no están sujetos a los riesgos naturales que solemos padecer en el Caribe. No obstante, esto no es así, tal como ilustra el siguiente gráfico facilitado por Microsoft:

Respaldo y resiliencia



Fuente: Microsoft

Los datos, los dispositivos (ordenadores y teléfonos inteligentes) y las cuentas son su responsabilidad. Con los datos, eso también implica que es su responsabilidad garantizar la protección de estos frente a pérdidas.

En el caso de los datos que se almacenan en local, la siguiente regla es una de las prácticas recomendadas:

La regla 3-2-1:

Debe almacenar **tres** copias de datos en **dos** tipos de formatos distintos y **uno** de ellos debe estar en otra ubicación distinta a la suya.

Hable con los especialistas informáticos de su zona, que pueden proporcionarle el hardware y los conocimientos necesarios para hacer copias de seguridad de sus datos de forma segura.

Respaldo y resiliencia

Siga los pasos anteriores para diseñar e implementar un plan de copias de seguridad resiliente.

1. **Haga un inventario** de los ordenadores y otros dispositivos que están conectados a la red (impresoras, discos, enrutadores, etc.). Cree un inventario de todos los programas informáticos que use, como Office, Photoshop, Quickbooks, etc., o cualquier otro programa que se utilice para el funcionamiento de su empresa. Anote el proveedor, la fecha de compra, la fecha de fin de garantía, el coste y su vida útil prevista.
2. Lleve a cabo una **evaluación de riesgos** mediante la plantilla proporcionada en la sección de recursos de este sitio. La evaluación determinará qué partes de la TI son las más vulnerables y, por tanto, las más importantes a la hora de hacer copias de seguridad para aumentar la resiliencia.
3. **Defina los objetivos de punto de recuperación y los de tiempo de recuperación** (consulte el cuadro de definiciones). Tenga en cuenta que los objetivos más cortos son más complejos y más caros de implementar.
4. **Defina su política de copias de seguridad** utilizando como punto de partida la plantilla proporcionada en la sección de recursos de este sitio.
5. **Implemente su estrategia de copias de seguridad** de acuerdo con su política definida. No dude en recurrir a un especialista de su zona para que le ayude a configurarla de la mejor forma posible. Supervise periódicamente sus copias de seguridad para asegurarse de que funcionan correctamente.
6. Lleve a cabo una **revisión cada 6 meses** de su política de copias de seguridad o cuando aplique un cambio importante en el software o hardware que se utiliza en la empresa. Por ejemplo, si cambia de software de contabilidad, debe revisar su política como parte del procedimiento de cambio de software para asegurarse de que sus copias de seguridad ofrecen resiliencia.

Utilice la plantilla de plan de copias de seguridad de datos que se incluye en los recursos para desarrollar su plan. Adaptado de este sitio, que incluye más instrucciones.

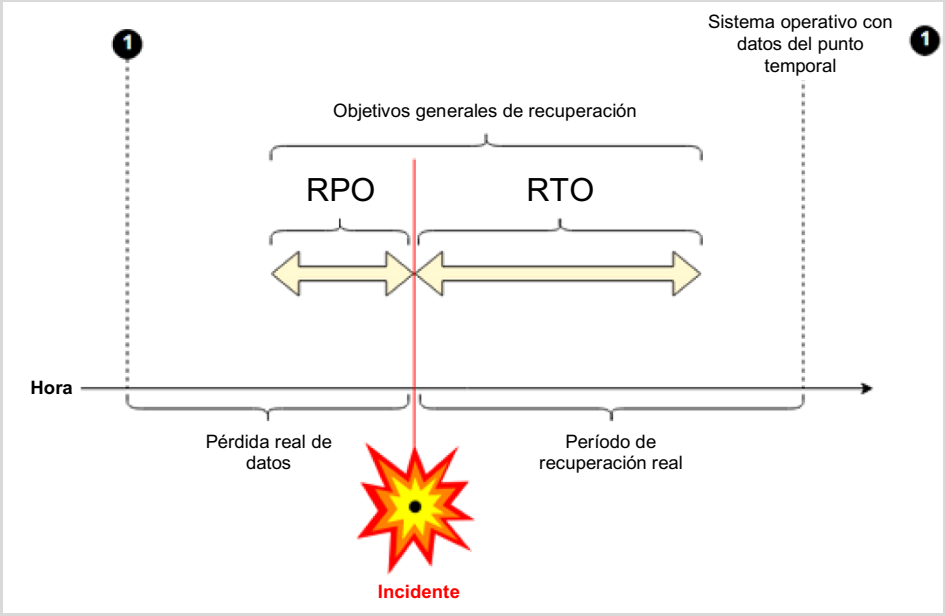
Respaldo y resiliencia

RECUADRO 1: Definiciones

Política de copias de seguridad: procedimientos y normas para garantizar que los datos corporativos se guardan en copias de seguridad y cuentan con la protección adecuada. Define el tipo de copias de seguridad, la frecuencia y el historial de copias de seguridad accesibles en caso de desastre.

Objetivo de punto de recuperación (RPO): el RPO es el punto máximo aceptable en el que pueden perderse datos. Por ejemplo, si se pueden perder los datos de un día, pero no los de dos, el RPO debe fijarse en un día.

Objetivo de tiempo de recuperación (RTO): el RTO es el tiempo máximo aceptable para ejecutar el proceso de recuperación con el objetivo de garantizar que la empresa reanude su funcionamiento tras un desastre.



Fuente: Wikipedia

Copia de seguridad incremental: este tipo de copia de seguridad contiene únicamente los archivos que han cambiado desde la copia de seguridad incremental o completa más reciente. Permite llevar a cabo copias de seguridad más rápidas, pero puede requerir más tiempo de recuperación.

Copia de seguridad completa: una única copia de seguridad que contiene todos los datos seleccionados para la copia de seguridad.

Copia de seguridad diferencial: una copia de seguridad acumulativa de los datos modificados desde la última copia de seguridad completa. Se utiliza para hacer copias de seguridad más rápidas, pero puede alargar el tiempo necesario para recuperar los datos por completo.