Hewlett Packard Enterprise

WHITEPAPER

Guía básica

para la protección de datos empresariales

Hewlett Packard Enterprise

La mayoría de las empresas están al tanto del poder de los datos y su impacto en los mercados, por eso han desarrollado complejos procesos para gestionarlos. Sin embargo, algunas organizaciones utilizan los términos "seguridad de los datos" y "privacidad de los datos" indiscriminadamente. Lo cierto, es que los **procesos de protección** tienen sus particularidades y todas juegan un papel fundamental para asegurar no sólo el **acceso a la información**, sino también la **continuidad del negocio**.

Estas son las principales **diferencias de los procesos** más comunes relacionados con la **integridad de los datos**:

Seguridad de datos

Las medidas que protegen la integridad de la información contra manipulación y malware.

Privacidad de datos

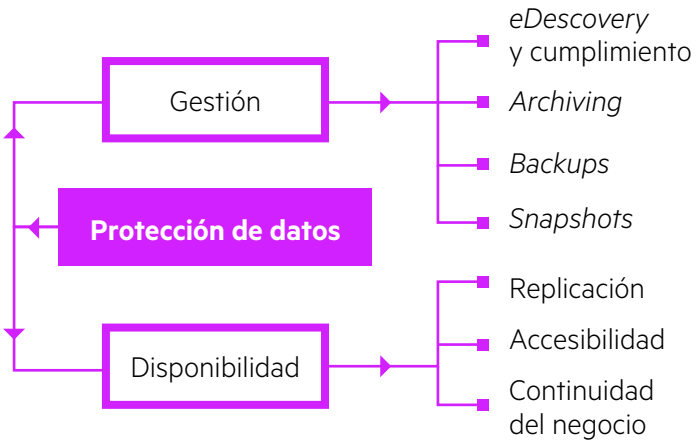
Se refiere al control de acceso para asegurar que sólo las personas autorizadas puedan ver y gestionar los datos.

Protección de datos

Conjunto de estrategias que **aseguran los datos contra pérdidas** a través de copias de seguridad y sistemas de recuperación.

Los principios más importantes de la protección de datos son la **salvaguarda y accesibilidad** en todas las circunstancias. Eso implica desde la realización de copias de seguridad hasta un plan eficaz de continuidad empresarial y recuperación ante desastres.

El siguiente esquema muestra las **ramas complementarias** que deben incorporarse en la estrategia de negocio para la protección de datos:



Fuente: Enterprise Strategy Group.

Hewlett Packard Enterprise

Retos, amenazas y soluciones

En el uso cotidiano, las empresas prestan atención a cómo estructuran y ordenan sus archivos, sin embargo, las soluciones más avanzadas, **incluyen los siguientes procesos en un sólo paso automatizado:**

Archiving

Busca recolectar todos los datos, nuevos y viejos, y trasladarlos a una ubicación segura, accesible y amigable para el usuario.

Backup

Es una copia de los datos originales que busca asegurar la recuperación en casos de pérdidas, ataques o corrupción.

Snapchot

Es una representación instantánea del estado del sistema que genera indicadores a la información almacenada para permitir recuperaciones más rápidas.

Protección de datos continua

Crea una copia de seguridad de los archivos en el momento exacto en que son modificados.

Fuente: TechTarget.

En orden de importancia, las principales amenazas que los procesos anteriores buscan superar son:

- Fallas en los archivos
- Corrupción de datos
- Fallas en el sistema de almacenamiento
- Fallas en el centro de datos

Hewlett Packard
Enterprise

Ninguna de las estrategias es completamente infalible, cada una tiene sus **ventajas y desventajas**, por eso es vital elegir la más adecuada, **de acuerdo con las necesidades de la operación** de cada corporación.

Los principales sistemas integrados para enfrentar éstas y otras amenazas complementan o reemplazan los datos faltantes directamente del sistema de copias de seguridad a través de estos mecanismos:

Mirroring

Escribe los datos localmente y en un sitio remoto al mismo tiempo hasta asegurarse que la información sea idéntica en ambos lugares. Exige duplicar la capacidad para almacenar ambas copias.

RAID

Este método almacena los datos en múltiples soportes locales, entre los cuales se distribuyen y replican. Requiere menos capacidad, pero consume más recursos y puede ser lenta.

Codificación de borrado (*Erasure coding*)

Escribe los datos localmente y en un sitio remoto al mismo tiempo hasta asegurarse que la información sea idéntica en ambos lugares. Exige duplicar la capacidad para almacenar ambas copias.

Replicación

Los datos son copiados de un nodo a otro u otros; es mucho más simple y rápido, pero consume mayor capacidad.

Fuente: TechTarget.

Hewlett Packard Enterprise

Recuperarse después del desastre

La **recuperación ante desastres** se enfoca en cómo las organizaciones restauran y actualizan sus copias de seguridad después de cualquier inconveniente. Las mecánicas de recuperación más eficientes se basan en ***snapshots* y replicación**, además de que no requieren la interrupción de los sistemas. Este es el proceso ideal:

1. A partir de un *snapshot*, se crea una unidad diferenciada.
2. Los datos originales se utilizan para lectura, mientras que la unidad diferenciada se usa para escritura
3. El almacenamiento se reconstruye y se replican los datos.
4. La unidad diferenciada se fusiona en el almacenamiento del servidor.

Nuevas tendencias en protección de datos

Por supuesto, todos los procesos de protección de datos están sujetos a mejoras que optimicen la protección. Algunas **tendencias a las cuales prestar atención son**:

Hiperconvergencia

Este marco combina almacenamiento, recursos y redes con capacidades de protección de datos en un sistema único que asegura escalabilidad y seguridad.

Almacenamiento en cintas LTO

Este medio es cada vez más popular para realizar copias de seguridad, pues es el más confiable, costo-eficiente, y ofrece una *air gap* que mantiene lejos los ataques del *malware* y *ransomware*.

Manejo de copias de datos (CDM)

El *copy data management* reduce la cantidad de copias a guardar para bajar los gastos operativos a través de la automatización, inteligencia artificial y control centralizado.

Hewlett Packard
Enterprise

¡Cuéntale a tus clientes las principales estrategias y medios de protección de datos y ayúdales a asegurar su activo más importante con las soluciones de HPE!

Si tienes alguna duda o comentario, comunícate conmigo:

Lisdy Mara Hinestroza
G. Segment Sales Specialist Latam
57 31 7517 9898