



**NO TEMA
POR SUS DATOS**

PRIMERA PARTE
Libro blanco – IDC

El cambio de paradigma
en el archivado, la
protección de datos y la
recuperación ante
desastres

SEGUNDA PARTE
Libro blanco – Bull

Las 7 reglas de oro de la
protección de datos

PRIMERA PARTE

El cambio de paradigma en
el archivado, la protección
de datos y la recuperación
ante desastres



LIBRO BLANCO

Nuevas estrategias de archivado, protección de datos y recuperación ante desastres para el cliente

Patrocinado por: Bull

Carla Arend - Enero de 2008

LA OPINIÓN DE IDC

En la actualidad estamos experimentando un cambio fundamental en el mercado del almacenamiento de la información. Aunque el crecimiento acelerado del volumen de datos sigue siendo la dinámica subyacente, nuestra apreciación del valor de los datos está cambiando. Los datos de distinto tipo cobran relevancia y un número cada vez mayor de personas necesitan acceder a ellos por distintos motivos, pero los presupuestos destinados al almacenamiento de datos se siguen mirando con lupa pese a los crecientes desafíos que plantea su gestión. Hoy en día, la gestión de datos de acuerdo con su valor se ha convertido en la clave para compensar la proliferación de los datos y los gastos asociados de almacenamiento.

Tradicionalmente, los datos estructurados eran los que poseían mayor valor para la empresa y se encontraban bien gestionados y protegidos en el centro de datos. Los datos semi-estructurados, como los correos electrónicos, o los datos sin estructurar, como las presentaciones, los ficheros almacenados en SharePoint y las copias personales de documentos, empiezan a ser considerados por las organizaciones como datos de gran valor y, en algunos casos, también como factores potenciales de riesgo. Sin embargo, dichos ficheros suelen almacenarse en ordenadores portátiles, en teléfonos móviles, o en sucursales más allá de las fronteras del centro de datos y de la protección y gestión centralizadas.

El cambio fundamental en la percepción del valor de los datos ha llevado a un cambio de paradigma en diversas tareas de gestión de datos como la protección, recuperación y archivo de datos, la continuidad de negocio y la recuperación ante desastres. No se trata de conceptos nuevos, sino de conceptos que están mejorando gracias a una inyección de nuevas e innovadoras tecnologías y de buenas prácticas que permiten al administrador de almacenamiento crear una infraestructura de almacenamiento que mantenga un compromiso adecuado entre el valor de los datos y el nivel servicio requerido a un coste competitivo.

El renovado interés en las estrategias de protección y recuperación de datos eleva la demanda de este mercado, impulsado por el aumento continuo del volumen de datos, los ajustados costes de almacenamiento, la necesidad de recuperar los datos con mayor rapidez y la creciente atención que la dirección presta a las implicaciones en el negocio derivadas de procesos inadecuados de protección de datos.

EN ESTE LIBRO BLANCO

Este documento, redactado por IDC y patrocinado por Bull, describe los cambios de paradigma de los que estamos siendo testigo en las áreas de protección y recuperación de datos, archivo, continuidad de negocio y recuperación ante desastres. Está dirigido a los administradores de almacenamiento que intentan entender la dinámica actual del mercado y su impacto en el diseño de sus propias infraestructuras de almacenamiento.

UNA VISIÓN GENERAL

¿Por qué es necesario cambiar las estrategias de almacenamiento?

Desde varios años atrás se manifiestan las dinámicas subyacentes que imponen un cambio en las estrategias de almacenamiento, pero ahora se han acelerado y suponen tal presión en los sistemas de almacenamiento y en los presupuestos, que el cambio es inevitable.

- . **Proliferación de los ficheros de datos no estructurados.** Comprender el valor de negocio de la cantidad masiva de distintos tipos de ficheros de datos y almacenarlos en los sistemas de almacenamiento más rentables es uno de los mayores desafíos a los que se enfrentan los administradores de almacenamiento. La presión proviene de la reducción del tiempo disponible para realizar backups debido al funcionamiento continuo 24/7 y a las bases de datos distribuidas.
- . **Requisitos de tiempos de recuperación más cortos.** Los acuerdos de nivel de servicio (SLA) de la mayoría de las aplicaciones requieren tiempos de recuperación (RTO) cada vez más cortos y puntos de recuperación (RPO) más granulares. Por consiguiente, las organizaciones necesitan rediseñar su arquitectura de protección de datos para poder estar a la altura.
- . **Mayor visibilidad en la organización.** El almacenamiento adquiere cada día mayor importancia estratégica en las organizaciones. Las razones son de doble sentido: el almacenamiento recibe una porción mayor del presupuesto de TI, por lo que el servicio que presta recibe a su vez una mayor atención. Además, crece el interés en los datos y en las potenciales responsabilidades legales que la organización almacena en su infraestructura de almacenamiento sin supervisión y sin control, lo cual es especialmente evidente en determinados sectores, como el financiero, el de las telecomunicaciones o el farmacéutico, que se enfrentan a normativas europeas cada vez más exigentes.
- . **Presión continua en los presupuestos de almacenamiento.** En muchas organizaciones el almacenamiento todavía se percibe como un gasto a soportar y el presupuesto destinado al almacenamiento no puede crecer al mismo ritmo que los datos a proteger. Es imprescindible incrementar la eficiencia de los procesos de protección de datos.

Al mismo tiempo, y como reacción ante estas dinámicas, constantemente surgen en el mercado del almacenamiento nuevas tecnologías y mejores prácticas, lo que supone un desafío para las organizaciones, que deben comprender en qué casos estas tecnologías son un valor añadido y cómo pueden utilizarlas bajo la misma interfaz de gestión. En los apartados siguientes se discuten las tecnologías surgidas en el mercado del almacenamiento como una reacción a las dinámicas del mercado.

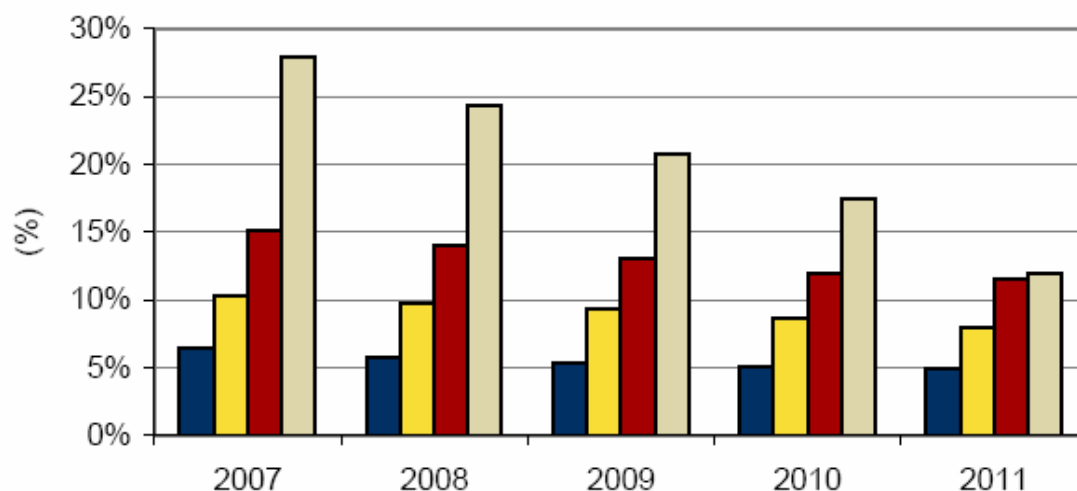
PREVISIONES FUTURAS

Mientras estos factores de cambio se intensifican, el mercado del almacenamiento en Europa Occidental está creciendo a un ritmo mucho más rápido que el gasto medio en TI. En la figura 1 se muestran las tasas de crecimiento del almacenamiento en tanto por ciento.

Se prevé que el mercado del software de archivado sea el de mayor crecimiento hasta el 2011, con un crecimiento del 18,6%, debido a que las empresas necesitan descargar y bloquear los datos almacenados en sus sistemas de producción. Le sigue el mercado de la replicación, que crece un 12,7% y que representa un componente clave de las soluciones de recuperación ante desastres y de continuidad del negocio. Debido a su madurez, el mercado del software de protección y recuperación de datos es el que presenta un crecimiento medio más lento en Europa Occidental, con un 5,3%, donde el mercado del software de almacenamiento representa un 8,9%. Las dinámicas subyacentes se discuten detalladamente en los apartados siguientes.

FIGURA 1

Previsión para el software de almacenamiento en Europa Occidental



por segmentos de mercado, 2007-2011 (Crecimiento anual en %)

- Software de protección y recuperación de datos
- Mercado del software de almacenamiento (Europa Occidental)
- Software de replicación de almacenamiento
- Software de archivado y HSM

Fuente: IDC, 2008

Nuevas estrategias para la gestión de datos: el valor para el negocio

Las organizaciones han ampliado su definición de datos valiosos y empiezan a buscar formas de gestionar los datos de acuerdo con su valor para la empresa en lugar de por tipo de fichero o antigüedad. Comprender su valor para el negocio sigue siendo clave para gestionar su almacenamiento de forma eficiente: no todos los datos se crearon iguales, por lo que no deben recibir el mismo tratamiento en la infraestructura de almacenamiento. Con las actuales herramientas de gestión de datos, se pueden implantar políticas que posicionen los datos en el nivel de almacenamiento más rentable y los trasladen a medida que van envejeciendo y se utilizan con menor frecuencia.

Nuevas estrategias para la protección y recuperación de datos: aprovechar la innovación

El mercado de la protección y recuperación de datos es el mercado del almacenamiento de mayor madurez. Todas las empresas tienen implantado algún tipo de proceso de protección de datos. A pesar de su madurez, se han producido numerosas innovaciones en el mercado, como la deduplicación, el backup de disco a disco (B2D), las librerías de cinta virtual (VTL), y la protección continua de datos (CDP). Las organizaciones se enfrentan ahora al desafío de aprovechar las nuevas tecnologías para mejorar las estrategias de backup y recuperación existentes sin aumentar la complejidad ni perturbar los procesos ya establecidos. Además, dado que estas nuevas tecnologías suponen un gasto añadido, los administradores de almacenamiento deben decidir qué nuevas tecnologías son las más apropiadas para

cada tipo de datos, relacionando así el coste de almacenamiento con el valor para el negocio de los datos almacenados.

Muchas organizaciones han alcanzado los límites de su estructura de protección y recuperación de datos y se enfrentan constantemente a problemas relacionados con los objetivos de tiempo de recuperación (RTO) y de punto de recuperación (RPO). La duración de las copias de seguridad (*backup*) se reduce debido al funcionamiento continuo 24 X 7 y la mayoría de las aplicaciones no pueden permitirse unos tiempos de inactividad prolongados debido a operaciones de mantenimiento o tras un fallo del sistema. La implementación de nuevas tecnologías de protección y recuperación de datos bajo un solo marco de gestión puede ser la solución a estos problemas.

El objetivo global de las innovaciones en materia de protección y recuperación de datos es aumentar el rendimiento de los procesos de almacenamiento, de los administradores y de la capacidad de almacenamiento. Una de las mayores innovaciones en cuanto a protección y recuperación de datos es la compresión de datos, que aumenta la eficacia de la protección de datos. La compresión de datos suele utilizarse conjuntamente con las tecnologías de B2D y VTL. Debido al descenso del precio de los discos, las empresas desean aprovechar al máximo el rendimiento mejorado de los backup con el fin de hacer frente a la reducción de los tiempos de backup y cumplir los cada vez más ajustados objetivos de tiempo de recuperación (RTO). No obstante, la protección continua de datos se utiliza para proteger aplicaciones que necesitan un nivel de puntos de recuperación más granular que un backup diario.

Virtualización

Una de las innovaciones contemporáneas más importantes en el campo de la TI es el nacimiento y la implementación de las tecnologías de virtualización. A fin de sacar el máximo partido a la virtualización de los servidores, las organizaciones necesitan entender cómo proteger adecuadamente los entornos virtualizados. Uno de los principales desafíos a la hora de proteger las máquinas virtuales es que en lugar de instalar un agente de backup en cada servidor físico las organizaciones han de implementar un agente en cada servidor virtual, lo que aumenta el número de agentes implementados, los costes y, aún más importante, la sobrecarga que el proceso de backup consume en cada servidor virtual. Como consecuencia, la virtualización es uno de los mayores motores de la transformación del almacenamiento directamente conectado (DAS) al almacenamiento en red (SAN o NAS).

Web 2.0

Web 2.0 es cada vez más popular en las empresas y añade más volumen a las crecientes cantidades de datos que las organizaciones necesitan gestionar y proteger. Web 2.0 surge con la llegada a la empresa de blogs, wikis y demás tecnologías de redes sociales. Su finalidad es compartir información y mejorar la red de empleados y clientes. Además, las herramientas de colaboración, como SharePoint, están proliferando en todos los departamentos. Sin embargo, si las organizaciones desean aprovechar estas innovaciones necesitan establecer estrategias adecuadas de protección y gestión de datos, así como llegar a comprender tanto el valor como el patrón de uso de las ingentes cantidades de ficheros de datos no estructurados. Definir una arquitectura por niveles es primordial para mantener bajo control los costes asociados de almacenamiento.

TI ecológica

Cuando las organizaciones adoptan estrategias de protección de datos inteligentes y tecnologías innovadoras están también fomentando su imagen "verde". La gestión adecuada de los datos aumenta la eficacia del hardware de almacenamiento y un mejor uso de los recursos de almacenamiento. La TI "verde" va más allá de la eficiencia energética del hardware de almacenamiento, pues supone la automatización mediante software de los procesos de gestión de datos, que serán mucho más eficientes.

Estas innovaciones en el mercado de la protección y recuperación de datos proporcionan importantes beneficios si se implementan correctamente. No obstante, es imprescindible entender el valor de los datos para poder identificar la tecnología adecuada de protección de datos y justificar la inversión en tecnologías innovadoras.

Nuevas estrategias de archivado: de la eficiencia a la conformidad legal y la gestión de riesgos

El mercado del archivado está experimentando un cambio fundamental. Las organizaciones europeas, en particular, han utilizado el archivado para descargar datos de sus sistemas de almacenamiento primarios a fin de aumentar la eficiencia de los sistemas de producción. Esta tendencia seguirá intensificándose, ya que el volumen de los datos en fichero crece mucho más rápido que el de los datos estructurados.

Además, un número cada vez mayor de organizaciones necesitan manejar datos a efectos de cumplimientos legales. En el sector financiero, por ejemplo, la Directiva de los Mercados de Instrumentos Financieros (MLFID) exige desde noviembre de 2007 que las instituciones financieras almacenen cada una de las transacciones con el cliente para documentar las conductas y el asesoramiento apropiados. Asimismo, las empresas de telecomunicaciones también necesitan almacenar todos sus datos de conexión durante al menos un año para que el gobierno pueda rastrear cualquier tipo de actividad delictiva. Debido a las normativas en materia de privacidad, las organizaciones empiezan a ser cada vez más conscientes de los riesgos potenciales asociados a los datos almacenados. También buscan mejorar el control y conocer el número de copias que poseen para backup y archivado a fin de garantizar que toda la información irrelevante pueda ser borrada cuando transcurran los períodos de retención obligatorios.

Funciones de búsqueda

Una de las claves para garantizar el cumplimiento legal y poder encontrar los datos relevantes en caso de una auditoría o un juicio es una funcionalidad de búsqueda implementada en las copias de archivado y backup.

Dicha funcionalidad también aumenta la productividad de los usuarios finales que ahora pueden realizar búsquedas de todos los datos a los que tienen acceso en todos los archivos de la empresa.

Nuevas estrategias para la continuidad de negocio/recuperación ante desastres: minimizar riesgos de forma eficaz

Las estrategias de continuidad de negocio y de recuperación ante desastres resultan fundamentales para la supervivencia de toda empresa. Sin embargo, también son caras y necesitan de un cuidadoso diseño que permita obtener la máxima protección con una mínima inversión.

En la actualidad, vemos cómo numerosas organizaciones analizan sus planes de continuidad de negocio/recuperación ante desastres cuando planean consolidar sus centros de datos. Muchas organizaciones están reduciendo sus centros de datos a dos o tres grandes centros en lugar de tenerlos esparcidos por toda Europa. Esto forma parte de la tendencia a minimizar riesgos a cualquier precio y encauzar los esfuerzos a hacerlo de forma eficaz e inteligente, normalmente en el seno de un proyecto de consolidación de mayor envergadura.

¡Cambiar las estrategias de almacenamiento es todo un reto!

Mantener el ritmo de la dinámica del mercado del almacenamiento puede ser una tarea abrumadora para muchas organizaciones, sobre todo porque existe un amplio abanico de tecnologías entre las que elegir y que todavía tienen que demostrar su valor y su rendimiento en las operaciones del día a día. Además, la implementación de distintas tecnologías que solucionan diversos problemas desde una

perspectiva parcial puede incrementar la carga que soporta el administrador de almacenamiento si dicho esfuerzo no forma parte de un marco general de gestión del almacenamiento.

GUÍA BÁSICA: 5 PASOS HACIA EL ÉXITO

Las organizaciones y los administradores de almacenamiento se enfrentan en la actualidad a importantes cambios y desafíos. Sin embargo, existen cinco pasos para guiar a las organizaciones y a los administradores de almacenamiento en su viaje:

- . Clasifique sus datos y sus aplicaciones de acuerdo con su importancia para el negocio. Este es el paso más importante para conseguir una estrategia de almacenamiento eficaz y duradera.
- . Decida cuál es la tecnología de almacenamiento más adecuada para cada tipo de datos. La mayoría se pueden almacenar en un almacenamiento secundario y terciario, sin necesidad de ocupar almacenamiento primario, que es mucho más caro.
- . Para los datos más importantes procure utilizar nuevas tecnologías que mejoren los RTO y los RPO, ya que la mejora en los niveles de servicio de los datos vitales para la organización justifican la inversión.
- . Para los datos menos importantes, utilice las tecnologías de almacenamiento más económicas posibles para reducir los costes de almacenamiento. Un almacenamiento "suficiente" es una estrategia viable para esta clase de datos.
- . ¡Concéntrese en la gestión de datos y de almacenamiento! La posibilidad de gestionar entornos heterogéneos de fuentes de datos y tecnologías de almacenamiento le aportará una mejor visión de conjunto además de mejorar el rendimiento. Tenga presente que implementar nuevas tecnologías en sus servidores, como, por ejemplo, la virtualización, requiere una nueva configuración de la infraestructura de almacenamiento. Es más, encuentre una solución que pueda gestionar tanto a través de entornos virtualizados como físicos.

Aviso de Copyright

Publicación externa de IDC Information and Data. Toda información de IDC que vaya a ser utilizada en anuncios publicitarios, comunicados de prensa o material promocional deberá contar con el consentimiento previo por escrito del vicepresidente o del Country Manager de IDC pertinente. Cualquier petición de este tipo deberá ir acompañada de un borrador del documento. IDC se reserva el derecho de denegar el uso externo.

© 2008 IDC. Queda prohibida la reproducción total o parcial sin el consentimiento previo por escrito.

2º PARTE

Las 7 reglas de oro de la protección de datos



Architect of an Open World™

Resumen	3
¿Cuál es el problema?	4
¿Qué impacto tiene?	5
Ampliar la perspectiva.....	6
Siete prácticas maneras de mejorar la protección de datos	7
1. Clasifique sus conjuntos de datos y defina métricas de protección de datos	7
2. Reduzca el volumen de los datos protegidos utilizando niveles de almacenamiento	
7	
3. Reduzca el RTO y el TCO mediante Virtual Tape.....	7
4. Reduzca el RPO y el RTO mediante copias instantáneas	8
5. Reduzca el riesgo mediante soluciones de recuperación ante desastres de bajo coste	
8	
6. Amplíe el ámbito de la protección de datos para incluir los datos de ficheros	9
7. Reduzca los volúmenes de almacenamiento primario y secundario mediante la	
deduplicación	9
Cómo Bull puede ayudarle a proteger sus datos	10
Tecnologías de almacenamiento completas e innovadoras	10
Servicios y sólida experiencia técnica	10
Soluciones enfocadas hacia la empresa	11
Productos de almacenamiento StoreWay	12
StoreWay Optima	12
StoreWay Calypso	12
StoreWay Virtuo.....	13
StoreWay DPA (Data Protection Appliance).....	13
Clientes	14
La gestión del ciclo de vida en Sonepar	14
Almacenamiento y cumplimiento de normas en Saltgate	14
Conclusión	15

El incesante y acelerado crecimiento del volumen de datos corporativos, la cada vez mayor dependencia en estos datos para realizar operaciones clave en la empresa y la naturaleza cambiante de la información suponen una carga para cada área de la infraestructura de almacenamiento, desde el presupuesto de los costes crecientes de almacenamiento hasta el cumplimiento de objetivos de nivel de servicio cada vez más exigentes, pasando por la gestión del riesgo de la pérdida de datos, el cumplimiento con los requisitos obligatorios de archivado de los datos o el mantenimiento de una flexibilidad suficiente dentro de la infraestructura de almacenamiento que permita adaptarse a necesidades futuras.

La aplicación de una estrategia de protección de datos eficaz es de vital importancia. Si se implementa correctamente, no sólo permite reducir el riesgo de pérdida de datos, sino también la presión en el presupuesto, los objetivos de nivel de servicio, el cumplimiento de normas y la flexibilidad. Por desgracia, los mecanismos de protección de datos implantados hoy día en muchas organizaciones a menudo no se ajustan al ritmo de los cambios y ofrecen una protección parcial e inadecuada de los recursos de información de la empresa. Es necesario adoptar nuevos enfoques para responder a estos nuevos desafíos.

En el informe de IDC solicitado por Bull, IDC identifica los principales motores de cambio en el almacenamiento y los retos clave relacionados con la protección de datos, y destaca una serie de estrategias y tecnologías que pueden jugar un papel decisivo para responder a estos retos. Este informe de IDC se complementará con un análisis minucioso de las principales organizaciones europeas, realizado por IDC a petición de Bull, en el que se examinarán detalladamente los problemas relacionados con la protección de datos a los que se enfrentan los departamentos de TI.

En este Libro Blanco se analizan las exigencias que obligan a las organizaciones a reconsiderar sus estrategias de protección de datos, y las principales deficiencias que genera una protección de datos inadecuada. Su objetivo es ayudar a los responsables de TI a categorizar sus necesidades de protección de datos y a establecer un conjunto de medidas de evaluación de la protección de datos. Identifica 7 prácticas maneras de mejorar los niveles generales de protección de datos. Por último, ofrece una descripción de la cartera de productos de protección de datos Bull StoreWay y algunos ejemplos de las soluciones que los clientes de Bull han implementado para responder a los retos de la protección de datos.

Soluciones de protección de datos

Bull StoreWay

La organización StoreWay de Bull es un integrador de soluciones de almacenamiento abierto de reconocida trayectoria, que permite a empresas de todos los tamaños en toda Europa y en otros continentes implementar infraestructuras de almacenamiento personalizadas en función de sus necesidades individuales, con beneficios económicos y empresariales demostrados. Basadas en una sólida colaboración con los líderes del sector del almacenamiento, su propia gama StoreWay de productos de hardware y software y una amplia gama de servicios de asesoramiento e implementación de almacenamiento, las soluciones de almacenamiento StoreWay abarcan todos los aspectos de la gestión de la información y el almacenamiento de datos.

Resumen

Todas las empresas se ven obligadas a mejorar sus medidas de protección de datos como consecuencia inevitable de un entorno empresarial en constante evolución. La desmaterialización, las operaciones 24x7, los servicios electrónicos y las normativas son algunos ejemplos de factores externos que tienen un impacto en la manera de gestionar y proteger la información electrónica. El fuerte crecimiento del volumen de datos y las restricciones presupuestarias sólo agravan el problema.

Para los departamentos de TI, supone tener que enfrentarse a una serie de retos específicos: reducir el coste total de propiedad (TCO, *Total Cost of Ownership*), cumplir los objetivos de nivel de servicio (SLO, *Service Level Objectives*), gestionar el riesgo, cumplir con la normativa y conservar la flexibilidad de la infraestructura de almacenamiento.

Una estrategia de protección de datos eficaz consiste en una combinación de diversas técnicas de protección de datos que representa un equilibrio entre, por una parte, la naturaleza y el valor de la información junto con los riesgos específicos a los que están expuestos los datos y, por otra parte, el presupuesto disponible para proteger la información.

¿Cuál es el problema?

Los procedimientos de protección de datos son tan antiguos como la informática. Durante décadas, las empresas han dependido de las copias de seguridad que se realizaban de noche para almacenar los datos en una cinta; aún hoy sigue siendo un procedimiento estándar en los centros de datos. Sin embargo, por diversos motivos, la copia de seguridad en cinta ya no es suficiente y es necesario sustituirla o combinarla con otros métodos de protección de datos. Estos son los principales motivos:

Reducir los tiempos de backup. La copia de seguridad en cinta es un proceso que se realiza tradicionalmente con las aplicaciones offline durante el proceso de almacenamiento. Sin embargo, la necesidad de que las aplicaciones estuvieran disponibles durante períodos más largos (por ejemplo, para ofrecer servicios de internet) supone una reducción del tiempo dedicado a la copia de seguridad. Además, el crecimiento de los datos primarios implica la necesidad de almacenar más datos en un período de tiempo más corto.

Reducir el RPO/RTO. Las 2 medidas estándar que se utilizan en la protección de datos son el objetivo de punto de recuperación (RPO, *Recovery Point Objective*) y el objetivo de tiempo de recuperación (RTO, *Recovery Time Objective*). El RPO es el intervalo entre la última copia de seguridad de los datos y el momento en que se produce la pérdida de los datos; refleja la cantidad de datos que se ha perdido irremediamente. El RTO es el tiempo necesario para restablecer los datos y hacerlos disponibles para las aplicaciones tras una pérdida de datos. Por ejemplo, una copia de seguridad que se realice diariamente en cinta tiene un RPO de 24 horas (se podrían perder las modificaciones de todo un día) y un RTO que varía de varias horas a varios días. El empleo cada vez mayor de recursos de TI en los procesos empresariales pone de manifiesto la necesidad de reducir el RPO y el RTO.

La naturaleza cambiante de la información. La copia de seguridad en cinta se centra tradicionalmente en proteger los datos utilizados en las aplicaciones clave de la empresa y que se almacenan generalmente en bases de datos. La información crítica se está almacenando cada vez más en datos no estructurados (correos electrónicos, ficheros, vídeo, audio, etc.) fuera del ámbito de los procesos existentes de copia de seguridad. La copia de seguridad tradicional a menudo no está optimizada para los datos no estructurados, que generalmente son voluminosos y difíciles de clasificar e indexar.

Gestión de riesgos. Aunque en la práctica no siempre es así, los procesos tradicionales de copia de seguridad deben incluir un almacenamiento de seguridad remoto de los datos. No obstante, en caso de incidentes graves en las instalaciones centrales se proporcionaría un soporte muy limitado de la recuperación ante desastres.

Conformidad legal. Cada vez más, las empresas tienen la obligación legal de almacenar los datos. La copia de seguridad no debe considerarse como una solución de archivado. La copia de seguridad es una copia que se utiliza para recuperar los datos en caso de pérdida. El archivado es el almacenamiento a largo plazo de información importante por motivos de referencia y la conservación de recursos de información a largo plazo.

Por último, las operaciones de copia de seguridad y restauración son un método *correctivo* que permite recuperar los datos en caso de pérdida. No aborda el problema de cómo evitar la pérdida de datos. Es necesario tener en cuenta la protección *preventiva* junto con la protección correctiva como parte de una estrategia global de protección de datos.

En conclusión, la copia de seguridad tradicional sigue ofreciendo una primera línea de defensa para la protección de datos y aún juega un papel en la mayoría de las estrategias de protección de datos. Pero debe formar parte de una estrategia más amplia en la que se combinen las técnicas de protección de datos preventivas y correctivas. A continuación, veremos cómo se clasifican las necesidades de protección de datos y cómo definir los criterios de medición.

¿Qué impacto tiene?

La información es un recurso clave de cualquier empresa. Procesada mediante aplicaciones empresariales, la información es la base de la actividad empresarial y permite ofrecer detalles de las operaciones comerciales. Sin embargo, el almacenamiento y la gestión de los datos son esencialmente un coste para la empresa, y no generan beneficios directos. De hecho, lo que más preocupa en las soluciones de almacenamiento es la optimización de los costes implicados. Bull considera que las estrategias de gestión del almacenamiento se pueden analizar o validar desde una perspectiva de costes y define cuatro áreas de costes importantes:

- . **El coste total de propiedad de los recursos de almacenamiento.** El coste total de propiedad (TCO, *Total Cost of Ownership*) engloba la inversión inicial (inversión de capital o CAPEX) y los costes recurrentes, como el mantenimiento y la administración (gastos operativos, u OPEX), y abarca el hardware de almacenamiento y el software que se utiliza para administrar y gestionar los datos. La protección de datos forma parte del TCO general "por GB". Puesto que la piedra angular de la protección de datos consiste en copiar datos a un número de dispositivos de almacenamiento cada vez mayor, puede representar un coste significativo.
- . **El coste de suministro de niveles de servicio.** Los objetivos de nivel de servicio (SLO, *Service Level Objectives*) a menudo se describen dentro de los acuerdos de nivel de servicio (SLA, *Service Level Agreements*), y para el almacenamiento generalmente se expresan en términos de disponibilidad de los datos para las aplicaciones y el rendimiento de las operaciones de transferencia de datos. El rendimiento no es un factor que aborde directamente la protección de datos, aunque algunas técnicas de protección de datos, como las copias instantáneas (*snapshots*), pueden tener un impacto negativo en el rendimiento. Sin embargo, la disponibilidad de los datos es una preocupación básica. La protección preventiva y correctiva tienen un impacto directo en los niveles de disponibilidad.
- . **El coste de gestión del riesgo y el cumplimiento legal.** Un problema puramente empresarial es el impacto de la pérdida de datos, ya sea temporal o permanente, o la imposibilidad de proporcionar la información necesaria a efectos de cumplimiento legal (con la legislación gubernamental o del sector, o para presentar pruebas ante una demanda judicial). El nivel de protección de datos es una consecuencia directa de estos posibles impactos.
- . **El coste de conservar la flexibilidad.** Lo más difícil de cuantificar es el impacto de no poder adaptar la infraestructura de almacenamiento a los cambios tecnológicos y empresariales. La flexibilidad puede aumentarse, por ejemplo, mediante la consolidación y el uso de tecnologías de virtualización. Sin embargo, la protección de datos generalmente impone ciertas limitaciones en la flexibilidad del almacenamiento. A menudo, la protección de datos está basada en "silos", con diversas técnicas de protección de datos estáticamente asignadas a diversos conjuntos de datos, lo que genera infraestructuras de almacenamiento complejas y rígidas.

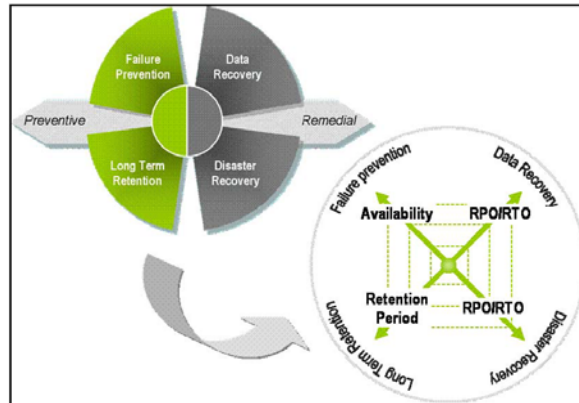
Cabe destacar que las tecnologías existen para proporcionar casi cualquier objetivo de nivel de servicio, responder a virtualmente cualquier riesgo y ser completamente flexibles. Sin embargo, los costes son prohibitivos y el cálculo del ratio coste/beneficio debe realizarse en función del valor de los datos para la empresa. Puesto que las empresas tienen varios tipos de datos, y que todos los datos no son iguales, deberá calcularse el ratio coste/beneficio para cada clase de dato. La protección de datos está claramente centrada en el problema de la gestión de riesgos. Sin embargo, también tiene un impacto directo en las demás áreas de coste. La restauración rápida de datos puede contribuir a cumplir los objetivos de nivel de servicio. También debe tenerse en cuenta que cada elemento de datos individual se replica generalmente varias veces dentro de la infraestructura de almacenamiento, habitualmente por motivos de protección de datos. La optimización de la protección de datos optimiza a su vez el coste total de propiedad (TCO) general. Por último, la implementación fragmentada e improvisada de una protección de datos insuficiente puede afectar negativamente a la flexibilidad de la infraestructura de almacenamiento.

Ampliar la perspectiva

Como se ha descrito previamente, existen dos medidas para la protección de datos: preventiva – “¿cómo evitar la pérdida de datos?” y correctiva – “he perdido los datos, ¿cómo los recupero?”. En la práctica, ambas medidas preventiva y correctiva son necesarias. Aunque se tomen todas las medidas oportunas para evitarlo, resulta inevitable sufrir alguna pérdida de datos.

En el ámbito de la prevención, Bull identifica dos áreas principales:

Protección contra fallos aislados de hardware y software. La protección contra los fallos de componentes individuales como discos, controladores de almacenamiento y switches de red, los mecanismos de arquitecturas redundantes con copia de seguridad en cliente (*hot backup*) y recuperación ante fallos (*failover*) son ampliamente conocidos y están implementados en todo el mundo en las arquitecturas de almacenamiento corporativo. La protección de discos RAID y el enrutamiento múltiple (*multi-pathing*) pertenecen a esta categoría.



Archivado. Aunque puede resultar sorprendente, Bull considera que el archivado de datos forma parte de una estrategia preventiva de protección de datos. Guardar los datos durante un largo período representa un auténtico reto: identificar la información que es necesario archivar, definir la duración del almacenamiento junto con los niveles de seguridad y autenticación, clasificar e indexar la información para poder buscar y recuperarla posteriormente, y conservar la capacidad de acceso a la información a medida que cambia la tecnología y se deterioran los soportes de almacenamiento.

En el ámbito de la protección de datos correctiva:

Recuperación de datos. Para afrontar la pérdida de datos debida a diversos factores, la recuperación de datos restablece los datos perdidos a partir de una copia. Las causas más frecuentes son la eliminación accidental de los datos, aunque también se incluyen los virus y los fallos de software o de hardware. Las técnicas de recuperación de datos incluyen el ya tradicional restablecimiento/backup de datos, pero también técnicas más recientes como las copias instantáneas (*snapshot*), la replicación de datos y la protección continua de datos (CDP, *Continuous Data Protection*).

Recuperación ante desastres. Es la implementación informática del plan de continuidad de negocio que describe cómo se mantendrán activos los procesos clave del negocio en caso de amenaza para las operaciones clave de la empresa. Para los sistemas informáticos, consiste habitualmente en dar respuesta a la pérdida de un centro de datos (*Data Center*) completo provocada por acontecimientos como un incendio, inundación, fallo del suministro eléctrico, actos de terrorismo o disturbios. Las modernas arquitecturas de recuperación ante desastres incluyen la replicación de datos en tiempo real a un segundo y, con mayor frecuencia, a un tercer centro de datos, lo que permite trasladar rápidamente las operaciones de TI en caso de que se produzca un incidente grave.

Uno de los mayores retos para los departamentos de TI es tener que considerar estas cuatro áreas como piezas de un mismo puzzle de protección de datos y dejar de gestionarlas como unidades independientes.

Siete prácticas maneras de mejorar la protección de datos

1. Clasifique sus conjuntos de datos y defina métricas de protección de datos

Para optimizar la protección de datos ya existente y dar cabida a futuras estrategias de protección de datos, primero es necesario clasificar toda la información corporativa y establecer métricas concretas de cada conjunto de datos. Los conjuntos de datos incluyen, normalmente, bases de datos ERP, ficheros de datos de PC, etc. Las métricas más importantes son los objetivos RPO/RTO y el periodo de conservación.

El análisis del valor de la información identificará los puntos débiles del procedimiento actual. Es posible implementar mejoras inmediatas si se cambian las políticas de backup y archivado existentes para abarcar los datos que en la actualidad no se incluyen en los procesos de copia de seguridad, y en cierta medida optimizar los objetivos RPO/RTO.

Al no disponer de un análisis profundo del valor de la información corporativa, muchas empresas tratan la información como una masa homogénea y la protección de datos se ajusta a las necesidades de los datos más críticos, lo que supone un coste adicional.

2. Reduzca el volumen de los datos protegidos utilizando niveles de almacenamiento

La gestión del ciclo de vida de la información (o ILM, *Information Lifecycle Management*, por sus siglas en inglés) es un concepto relativamente claro hoy día: el valor de los datos cambia a lo largo de su ciclo de vida. Normalmente, los datos son activos e importantes al principio de su ciclo de vida, y después pasan a ser inactivos y menos importantes. En esta primera fase activa, los datos se almacenan en sistemas de almacenamiento primarios de coste más elevado, tras lo cual se transfieren a un soporte secundario de bajo coste (disco) y terciario (cinta) como datos de referencia a largo plazo.

En términos de protección de datos, el coste más considerable corresponde a la protección de los datos primarios activos. Es posible reducir los costes de almacenamiento y los tiempos de copia de seguridad si se eliminan periódicamente los datos primarios. Asimismo, tenga en cuenta que algunas fuentes estiman que por cada byte de almacenamiento primario existen al menos 10 copias para la protección de datos.

3. Reduzca el RTO y el TCO mediante las cintas virtuales

Ya se han comentado las limitaciones RPO/RTO de la copia de seguridad tradicional. El principal problema para la mayoría de las empresas es el tiempo de recuperación (RTO). Una manera eficaz de afrontar esta cuestión consiste en realizar copias de seguridad a disco. La restauración de datos desde discos de acceso aleatorio es mucho más rápida que la restauración secuencial desde una cinta.

Las librerías de cinta virtual (VTL) emulan dispositivos de cinta para permitir que la copia de seguridad a disco se integre de forma transparente en la arquitectura de copia de seguridad existente. Normalmente, las librerías VTL ofrecen la posibilidad de realizar la copia de seguridad a disco antes de la transferencia final a cinta (Disco a Disco a Cinta) o bien copiar los datos al disco (Disco a Disco).

Las librerías VTL emulan múltiples librerías de cintas, por lo que también proporcionan beneficios TCO al permitir consolidar diferentes entornos de backup, con el consiguiente beneficio de una administración simplificada y un mejor aprovechamiento de los discos y cintas para copias de seguridad. Por último, con la virtualización del entorno de backup, los recursos de cintas y la caché de disco pueden evolucionar sin tener un impacto en el entorno de backup, lo que proporciona flexibilidad y una mejora en el TCO gracias al uso de modernos equipos de almacenamiento de bajo coste.

4. Reduzca el RPO y el RTO mediante copias instantáneas

La tecnología de copias instantáneas (*snapshot*) permite obtener copias de datos virtuales casi instantáneas y, en la actualidad, se incluye en todos los arrays de almacenamiento corporativos. Al copiar únicamente unos pocos kilobytes de punteros de datos, y no los datos subyacentes, los tiempos de copia de seguridad se acortan considerablemente. Los agentes snapshot para aplicaciones de correo electrónico y base de datos permiten sincronizar los snapshots con la aplicación.

La desventaja de los snapshots es que aunque proporcionan una protección eficaz contra la pérdida de datos, por ejemplo, un borrado accidental, usan el mismo almacenamiento físico que los datos primarios y si se producen daños físicos en el soporte de almacenamiento, se pierden tanto los datos primarios como la copia snapshot.

Lo mejor es una combinación de la copia de seguridad tradicional y del snapshot. La realización de frecuentes copias snapshots permite reducir el RPO/RTO de varios días, para una copia de seguridad tradicional, a algunas horas, para las causas más frecuentes de pérdida de datos. Las copias físicas de datos, mediante la replicación o backup de las copias snapshot, proporcionan una protección adicional.

5. Reduzca el riesgo mediante soluciones de recuperación ante desastres de bajo coste

Durante mucho tiempo, la recuperación ante desastres se ha circunscrito a las grandes empresas capaces de gestionar la complejidad y los costes de la implementación de una replicación síncrona de datos sobre líneas alquiladas de fibra óptica hasta unos centros de datos remotos. Más que la velocidad de transferencia, el mayor reto ha sido la latencia de la red, ya que ha tenido un impacto en el rendimiento en la arquitectura de replicación síncrona y ha limitado la distancia práctica hasta el centro de datos a 100-200 km.

La mejora en la fiabilidad y el rendimiento de las redes IP, el soporte nativo de la conectividad IP que ofrecen los arrays de almacenamiento en disco y la madurez alcanzada por la tecnología de replicación asíncrona han abierto el camino a toda una serie de opciones rentables de recuperación ante desastres. Ya sea a través de la red IP corporativa o de redes IP comerciales, en configuraciones de replicación de cobertura local hasta nacional o internacional, la recuperación ante desastres está en la actualidad al alcance de la mayoría de las empresas.

6. Amplíe el ámbito de la protección de datos para incluir los datos de ficheros

Las empresas de TI disponen de una gran experiencia en la protección y gestión de la información dentro del centro de datos, en particular, de las bases de datos gestionadas por ERP y otras aplicaciones críticas. En cambio, no se gestionan tan bien los datos corporativos en forma de ficheros. A menudo, estos datos se distribuyen a través de los PC y servidores de ficheros de la empresa y la protección de datos suele ser parcial o inconexa. A pesar de la naturaleza no estructurada y poco clara de este tipo de datos, lo que dificulta su clasificación y gestión eficaz, se reconoce cada vez más la importancia de estos datos.

Existen dos enfoques en la gestión de estos datos. Lo ideal sería consolidar los datos dentro del centro de datos en servidores de ficheros corporativos compatibles con los mecanismos de protección de datos ampliamente usados para los datos estructurados, e integrarlos en la estrategia y política corporativas de protección de datos. Si no fuera factible (por ejemplo, cuando existan varias sucursales), la tecnología CDP puede volver a replicar los datos en el centro de datos. Por último, si esto no fuera posible, podrían utilizarse equipos sencillos de backup de bajo coste para conseguir una protección de datos local.

7. Reduzca los volúmenes de almacenamiento primario y secundario mediante la deduplicación

En general, el uso de recursos de almacenamiento supone un derroche considerable. El hecho de que los usuarios no sepan lo que de verdad están almacenando, y que el sector del almacenamiento no aporte una tecnología de gestión eficaz de los datos, hace que la información se esté almacenando de manera repetida e innecesaria.

La deduplicación de los datos está surgiendo como una potente tecnología que ayuda a responder a este problema. La identificación de registros duplicados (deduplicación) se centra inicialmente en los sistemas de correo electrónico, en los que se almacenan repetidamente documentos adjuntos idénticos, y en los entornos de copia de seguridad, en los que las políticas de protección de datos hacen que se realice una copia de seguridad o replicación de los mismos datos de manera innecesaria. Sin duda, la deduplicación de datos se convertirá en una característica estándar incluso en el almacenamiento de datos primario, del mismo modo que la protección mediante RAID actual.

Hoy día existen dos tipos de deduplicación de datos. El almacén de instancias únicas (SIS, *Single Instance Store*), o deduplicación de ficheros, almacena sólo una copia de cada fichero. La deduplicación de bloques, más avanzada, busca coincidencias de secuencias de bloques para evitar, por ejemplo, almacenar datos idénticos de distintas versiones de un documento.

La deduplicación de datos se incluye como una característica opcional en los arrays de almacenamiento, las librerías de cinta virtual (VTL) y el software de protección de datos, así como en productos específicos (por ejemplo, la deduplicación de correos electrónicos). Por consiguiente, es posible integrarla en las infraestructuras de almacenamiento existentes.

Cómo Bull puede ayudarle a proteger sus datos

Bull StoreWay proporciona productos y soluciones de almacenamiento, y servicios de integración que le ayudan a definir sus requisitos de protección de datos y diseñar una solución adaptada a sus necesidades y a su presupuesto.

Tecnologías de almacenamiento completas e innovadoras

Bull StoreWay combina los productos de almacenamiento de los partners estratégicos de Bull (como EMC, NetApp, Brocade, Sun/StorageTek y Overland, entre otros) con productos propios de hardware y software StoreWay de Bull.

La solución StoreWay cubre todos los aspectos de la infraestructura de almacenamiento y se divide en tres grandes familias de productos: *almacenamiento en disco*, *protección y archivado de datos* y, *por último*, *red de almacenamiento y su gestión*.

El *almacenamiento en disco* cubre todas las necesidades de almacenamiento en red primario y secundario, desde el almacenamiento rentable de gama baja para pequeños grupos de trabajo hasta los arrays de almacenamiento de última generación diseñados para los entornos de centros de datos más exigentes, pasando por el almacenamiento versátil de gama media diseñado para una amplia variedad de necesidades corporativas.

La suite de *protección y archivado de datos* de StoreWay abarca las librerías de cintas y el almacenamiento direccionado por el contenido (CAS, *Content Addressable Storage*), junto con la replicación de datos, copia de seguridad, archivado y almacenamiento HSM para gestionar el movimiento de datos en la infraestructura de almacenamiento.

Al abarcar las infraestructuras de redes de almacenamiento de todos los tamaños, desde las pequeñas redes iSCSI hasta las grandes SAN Fibre Channel de los centros de datos, los productos de *red de almacenamiento y gestión* de StoreWay ofrecen diversas soluciones de redes de almacenamiento autónomas o multisitio.

Servicios y sólida experiencia técnica

Cada familia de productos se apoya en los sólidos conocimientos técnicos, las ofertas de servicios y la amplia red de soporte de Bull. La experiencia y los servicios de integración y consultoría de StoreWay acompañan a las empresas en todas las fases de sus operaciones de planificación, implementación y producción de la arquitectura de almacenamiento.

Esta combinación de productos y experiencia permite a Bull diseñar soluciones que optimizan la tecnología más avanzada existente en el sector y ofrecer el mix de productos que mejor se ajuste a las necesidades particulares de cada empresa.

Bull lleva más de 15 años ofreciendo soluciones abiertas de almacenamiento. Por ejemplo, Bull fue el primer partner OEM a nivel mundial para los arrays de almacenamiento CLARiiON cuando se comercializaron en 1993, y desde entonces ha proporcionado miles de soluciones de almacenamiento basadas en CLARiiON en Europa y en todo el mundo.

La amplitud, solidez y proximidad de la experiencia de Bull StoreWay proporciona un recurso excepcional en el mercado europeo. El Centro de Excelencia de Bull StoreWay (SEC, *StoreWay Excellence Center*) realiza un seguimiento y valora las últimas innovaciones en el mercado del almacenamiento además de mantener contactos técnicos con los principales proveedores de almacenamiento con el fin de integrar la mejor tecnología en las soluciones StoreWay abiertas e integradas.

El SEC pertenece a la red de centros de competencia, que cubren varios sectores de las TI, incluidos Windows, Linux, AIX, base de datos, SAP y alta disponibilidad. En conjunto, estos centros de competencia pueden proporcionar conocimientos en todos los aspectos de las infraestructuras de TI, lo que permite optimizar los sistemas de almacenamiento para el servidor y sus aplicaciones.

Como integrador de almacenamiento, StoreWay ofrece valor a sus clientes mediante soluciones y servicios de almacenamiento basados en varios proveedores a nivel mundial. Gracias a ello, los clientes de StoreWay se benefician de una solución completa de almacenamiento, que integra la mejor tecnología disponible en el mercado y garantiza una funcionalidad abierta con interoperabilidad, junto con un atractivo TCO e interesantes ventajas para el negocio.

Por último, el Customer Briefing Center de StoreWay ofrece a los clientes la oportunidad de colaborar directamente con los expertos de Bull a través de sesiones informativas, demos, estudios comparativos y pruebas de concepto. En el almacenamiento, al igual que en cualquier otro ámbito, no se puede aplicar el mismo rasero para todos los casos. Los clientes de StoreWay se benefician de unas soluciones a la medida de sus necesidades y de los requisitos estratégicos de su empresa.

Soluciones enfocadas hacia la empresa

Los productos y servicios StoreWay se ofrecen con soluciones que proporcionan un valor real. Al aportar una solución para los principales problemas de almacenamiento, como el archivado de correos electrónicos, la recuperación ante desastres y el cumplimiento de la legislación, las soluciones StoreWay no sólo ofrecen un servicio sino que ayudan a las empresas a reducir los costes y gestionar los riesgos.

Productos de almacenamiento StoreWay

Bull cuenta con acuerdos de colaboración a largo plazo con los principales fabricantes de almacenamiento, como EMC, NetApp, Brocade, Sun/StorageTek y Overland Storage, entre otros. A través de estos acuerdos, Bull integra algunos de los productos de almacenamiento más conocidos y mejor valorados del sector, incluidos el almacenamiento SAN de gama media CLARiiON de EMC y los arrays de almacenamiento de última generación de Symmetrix, los arrays de almacenamiento FAS de NetApp para NAS y el almacenamiento unificado SAN, así como los switches SAN y directores de Brocade. Bull ofrece su experiencia en todos estos productos a través del Centro de Excelencia StoreWay.

Como complemento de los productos de almacenamiento de los partners, los productos de la suite StoreWay de Bull completan la gama de productos centrándose particularmente en las soluciones de gran valor añadido en áreas específicas, como protección y gestión de datos.

La suite StoreWay incluye los productos:

StoreWay Optima

La suite StoreWay Optima de arrays de almacenamiento corporativo proporciona redes de almacenamiento Fibre Channel SAN para todas las necesidades corporativas. La familia Optima 1200 proporciona un almacenamiento primario y secundario de bajo coste para entornos Windows y Linux. Optima 1200 es compatible con las tecnologías de disco SATA y SAS, y con la arquitectura RAID de redundancia completa, por lo que es ideal en las aplicaciones de almacenamiento primario y secundario con conexión directa y en entornos de grupos de trabajo SAN. La gama media de almacenamiento de Optima 3000 ofrece prestaciones versátiles de almacenamiento corporativo y es compatible con las funciones de protección de datos, como el soporte RAID6 con doble paridad, las copias snapshot y la replicación síncrona/asíncrona. Los arrays de almacenamiento de gama alta Optima 5000 se dirigen a las necesidades críticas de los centros de datos, y soportan hasta 1200 discos FC/SATA en una arquitectura matricial robusta y de alto rendimiento.

StoreWay Calypso

StoreWay Calypso es la nueva suite de software de protección y gestión de datos de Bull que se encarga de áreas clave de la protección de datos mediante una arquitectura de software integrada y modular. Compatible con las tradicionales copias de seguridad en disco y cinta, Calypso también es compatible con el archivado basado en políticas, el almacén de instancias únicas (deduplicación de ficheros), el almacenamiento en niveles y la protección de datos en tiempo casi real gracias a la función de replicación continua de datos (CDR, *Continuous Data Replication*).

Calypso también mira al futuro al incluir funciones como la clasificación de datos no estructurados, la búsqueda y extracción electrónica de datos archivados y en copias de seguridad, y la búsqueda y restauración para usuario final. Gracias a su enfoque unificado de la gestión y protección de datos, Calypso reduce los costes, aumenta la flexibilidad y facilita la administración de los recursos de información de la empresa.

StoreWay Virtuo

La suite StoreWay Virtuo de librerías de cinta virtual (VTL, *Virtual Tape Libraries*) reduce los costes y optimiza la administración de la protección de datos en todos los niveles de la empresa. Al consolidar y optimizar las operaciones de backup existentes, StoreWay Virtuo proporciona inmejorables niveles de rendimiento, fiabilidad y flexibilidad en entornos de servidor abiertos y Mainframe.

Compatible con las arquitecturas de backup de Disco a Disco y de Disco a Disco a Cinta, la suite Virtuo cubre las necesidades de cualquier empresa, desde los entornos de PYMEs y departamentos hasta los exigentes centros de datos.

Las soluciones StoreWay Virtuo se integran fácilmente en los entornos de backup ya existentes, protegen la inversión en el software de backup existente y ofrecen beneficios inmediatos, como unos reducidos tiempos de backup y restauración, una fiabilidad mejorada de las operaciones de backup y restauración y la recuperación ante desastres.

StoreWay DPA (*Data Protection Appliance*)

Ideal para entornos de oficina/sucursal remota (ROBO, *Remote Office/Branch Office*), StoreWay DPA proporciona una solución de copia de seguridad práctica, de bajo coste y fácil de usar materializada en un equipo que integra tanto el software de backup como el soporte de almacenamiento. StoreWay DPA se basa en un backup eficiente de disco a disco con soporte para cinta para el almacenamiento de seguridad remoto de los datos, y es compatible con los principales entornos de Windows, Linux y Unix.

Entre las funciones opcionales se incluyen el soporte para copia de seguridad automática para MS SQL Server, Oracle, MS Exchange y Lotus Notes, el soporte de recuperación ante desastres, y la protección continua de datos (CDP, *Continuous Data Protection*) basada en bloques, ofreciendo una protección completa de los datos para las islas de información distribuidas en todos los niveles de la empresa.

Clientes

La gestión del ciclo de vida en Sonepar

Presente en 29 países y con ingresos superiores a 9.000 millones de euros, Sonepar GmbH es uno de los principales distribuidores europeos de material eléctrico. Ofrece más de 350.000 artículos en su catálogo en línea y su proceso de logística permite entregar cualquiera de las 80.000 referencias en stock directamente a sus clientes en un plazo de 24 horas desde sus 4 centros logísticos. Como usuario experimentado en TI y con una dilatada experiencia en el almacenamiento EMC Symmetrix en una configuración de recuperación ante desastres, Sonepar se enfrenta al reto que supone una cantidad creciente de datos no sólo en el entorno tradicional de las bases de datos sino también en nuevos tipos de datos, como los datos de ficheros y el correo electrónico. Esta problemática, amén de la obligación legal de proteger y archivar los datos, y reducir los costes de almacenamiento, ha llevado a Sonepar a adoptar una estrategia para implementar una arquitectura de almacenamiento en niveles que emplea los principios de la gestión del ciclo de vida de la información (o ILM, *Information Lifecycle Management*, por sus siglas en inglés). Bull se encarga del diseño general, la integración y el soporte de la infraestructura de almacenamiento, el despliegue progresivo de los arrays de almacenamiento CLARiiON de EMC para el almacenamiento secundario, Celerra para el archivado de ficheros y Centera para el archivado, lo que proporciona a Sonepar la infraestructura de hardware capaz de responder a sus necesidades de ILM. El archivado automatizado de los ficheros y la deduplicación de los datos adjuntos a los correos electrónicos han permitido a Sonepar cumplir con las directivas alemanas de archivado GDPdU, eliminar los datos inactivos del soporte de almacenamiento primario y reducir los tiempos de copia de seguridad. Los resultados son sorprendentes: el espacio de almacenamiento se ha reducido en un 70% para el correo electrónico y en un 85% para los servidores de ficheros. Aunque la optimización de los gastos de almacenamiento, la gestión del crecimiento de la información, el cumplimiento con los requisitos legales y la reducción del riesgo se han unificado ahora en una misma infraestructura de almacenamiento, aún quedan cambios por realizar en Sonepar con otros proyectos en curso, como el archivado a largo plazo.

Como explica Jurgen Bartling, Director de TI de Sonepar, “La gestión del ciclo de vida de la información no es un producto sino una estrategia que se compone de una multitud de proyectos individuales. Para llevarla a cabo, se necesitan conceptos concretos y sobre todo partners valiosos que, como Bull, estén orientados 100% hacia el cliente.”

Almacenamiento y cumplimiento de normas en Saltgate

Saltgate, una nueva empresa del sector financiero que ofrece gestión de fondos en Luxemburgo y Jersey (Reino Unido), ha confiado la gestión completa de sus sistemas de TI a Bull, incluido el cumplimiento con la normativa local en materia de protección de datos.

La experiencia de Bull ha permitido a Saltgate centrarse en sus actividades principales al especificar, entregar y gestionar una solución subcontratada que abarca la infraestructura de aplicaciones, servidor y almacenamiento, cumpliendo a la vez los objetivos de nivel de servicio exigidos. Al suministrar el archivado y la continuidad de negocio, Bull garantiza que la solución cumple por completo con la normativa en materia de conservación y trazabilidad de datos de la “Comisión de Vigilancia del Sistema Financiero de Luxemburgo” (CSSF), que está en proceso de convertirse en la norma de calidad en el sector financiero europeo. La infraestructura de almacenamiento se basa en las soluciones Bull StoreWay con el almacenamiento en disco Optima y la protección y archivado de datos Calypso.

Conclusión

El desarrollo, la diversidad y la importancia de la información corporativa presenta importantes retos económicos y de gestión de riesgos para el departamento de TI. Las metodologías tradicionales de protección de datos han puesto de manifiesto sus limitaciones en muchos casos, ofreciendo unos niveles de protección que ya no se ajustan a los entornos empresariales actuales, y que no logran responder al desafío de proteger nuevos tipos de información no estructurada.

Se pueden combinar los nuevos productos y tecnologías con las copias de seguridad existentes para mejorar radicalmente la protección de datos dentro de un marco de protección de datos global que suponga una evolución y no una revolución.

Con su dilatada experiencia y saber hacer en la integración de sistemas abiertos de almacenamiento empresarial mediante su organización StoreWay, Bull acompaña a las empresas de cualquier tamaño y en todos los sectores de mercado en la transformación de su estrategia de protección de datos para responder a estos retos.

©Bull SAS 2008 Bull reconoce el derecho de las marcas comerciales propietarias contenidas en este documento. Bull se reserva el derecho de modificar este documento en cualquier momento sin previo aviso. Algunas ofertas o parte de ellas contenidas en este documento pueden no estar disponibles. Por favor, contacte con su representante de Bull para obtener información de las ofertas disponibles en su país.

Bull – rue Jean Jaurès - 78340 Les Clayes sous Bois (Francia)
Bull España, S.A. Paseo de las Doce Estrellas, 2. 28042 Madrid

W4DCBullStorage_va1