Converse con un consultor ¡Prueba gratuita de 30 días!

Exhibición de la solución

El portafolio de Protección de Datos de IBM Spectrum es 'algo que no puede perderse'

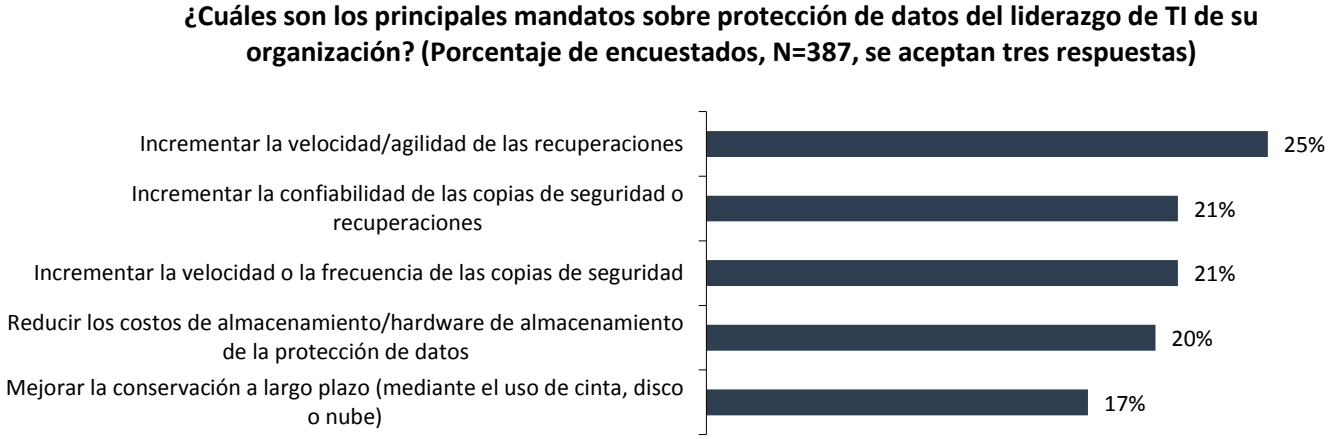
Fecha: Octubre 2017 **Autores:** Jason Buffington, Analista principal; y Monya Keane, Analista sénior de investigación

Resumen: La oferta IBM Spectrum Protect cuenta con más de 20 años de logros en la protección y recuperación de sistemas de TI clave. Por lo tanto, resultaría fácil suponer que las nuevas ofertas de software "Spectrum Protect" y "Spectrum Copy Data Management" de IBM representan solamente a "Spectrum Protect con características adicionales". Esta suposición sería incorrecta. Se trata de estrategias independientes y reinventadas que apuntan a resolver un desalentador reto de TI –la protección/recuperación de la virtualización– y que aspiran a obtener un codiciado resultado de TI –la gestión y habilitación efectiva de datos (DM&E, por sus siglas en inglés), que muchos denominan "gestión de copia de datos" (CDM, por sus siglas en inglés)–.

Introducción

La investigación de ESG demuestra que los líderes sénior de TI están emitiendo mandatos dentro de sus organizaciones para, simplemente "*mejorar*" en sus iniciativas de protección de datos (ver la Figura 1).[1]

Figura 1. Los cinco principales mandatos del liderazgo de TI para la protección de datos



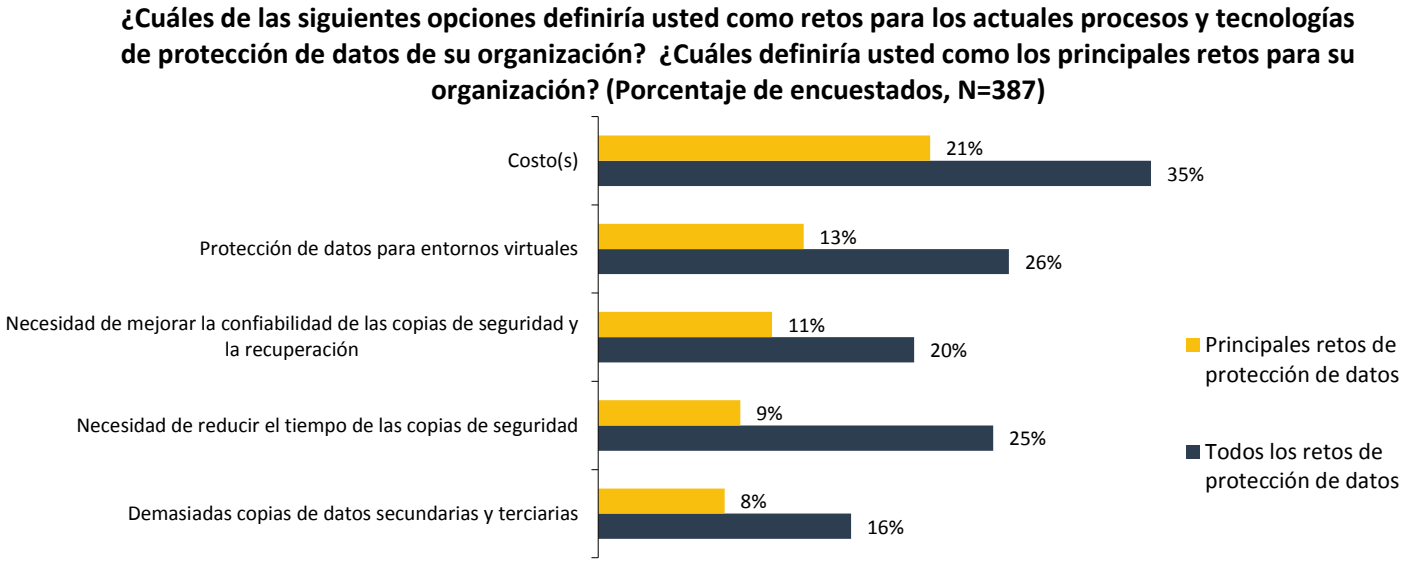
Fuente: Enterprise Strategy Group

De manera notable, los profesionales de TI cuya tarea es la protección de datos, están enfocados en acciones similares relacionadas con la mejora/reducción, a la vez que tratan de gestionar los costos y los retos relacionados con la protección y recuperación de entornos virtualizados (ver la Figura 2).[2]

[1] Fuente: Encuesta de investigación de ESG, *2017 Trends in Data Protection Modernization (Tendencias 2017 en la Modernización de la Protección de Datos)*, diciembre 2016.

Este trabajo de ESG fue encargado por IBM y se distribuye bajo licencia de ESG.
© 2017 por The Enterprise Strategy Group, Inc. Todos los derechos reservados.

Figura 2. Los cinco retos principales para los actuales procesos y tecnologías de protección de datos



Fuente: Enterprise Strategy Group

Los retos modernos requieren soluciones modernas

Para el 2017, muchas organizaciones mencionaron el aumento en el uso de la virtualización de servidores y la mejora en las copias de seguridad y la recuperación de datos como las áreas de inversión significativa para la modernización de los centros de datos.[3]

Pero como muestran los datos citados en la Figura 2, la virtualización crea desafíos relacionados con la protección. Del mismo modo, las numerosas copias de datos creadas en el curso de la búsqueda de iniciativas de protección y no protección también presentan desafíos.

Con tanta presión para reducir los costos de almacenamiento a la vez de incrementar la flexibilidad y la agilidad de recuperación, sería fácil llegar a la presunción equivocada de que las dos iniciativas siempre entran en conflicto entre sí. En realidad, se puede lograr una mejor flexibilidad de recuperación a la vez que se reducen costos (o se incrementa el valor empresarial proveniente de esos costos), que es exactamente lo que las organizaciones deberían tener como meta.

- Mejora en la recuperabilidad y el aseguramiento de la virtualización.
- Gestión y habilitación de datos más eficiente y más rentable.

Mejora en la recuperabilidad y el aseguramiento de la virtualización.

En 2017, ya no debería ser una simple cuestión de *si* uno puede brindar copias de seguridad de manera adecuada a una máquina virtual o a un conjunto de VM residentes en un "host". Aunque ese esfuerzo fue admitido alguna vez como un reto, las APIs de protección de datos actuales de VMware, Microsoft y otros proveedores de hipervisores brindan ahora mecanismos confiables para las copias de seguridad de prácticamente cualquier VM.

Lo que sigue siendo una verdadera área de diferenciación es la capacidad de recuperación y el logro de una protección *integral* dentro de los entornos virtuales, un objetivo que a menudo sigue afectando a las organizaciones (ver la Figura 3).[4]

[2] ibid.
[3] Fuente: Informe de Investigación de ESG, *2017 IT Spending Intentions Survey (Encuesta de Intenciones de Inversiones en TI para 2017)*, marzo 2017.
[4] Fuente: Expediente ESG, *Reliable Virtualization Protection Continues to Elude Many Organizations (La protección confiable de la virtualización continúa eludiendo a muchas organizaciones)*, octubre 2017.

© 2017 por The Enterprise Strategy Group, Inc. Todos los derechos reservados.

Figura 3. Los diez retos principales para la protección de un entorno de servidores virtualizados

¿Cuáles de las siguientes opciones definiría usted como retos para la protección del ambiente de servidores virtuales de su organización? ¿Cuál definiría como el principal reto para la protección de esos servidores? (Porcentaje de encuestados, N=400)

Fuente: Enterprise Strategy Group

Como lo demuestra la Figura 3, el principal reto para la protección de datos específica de la virtualización sigue siendo, a criterio de los encuestados, la recuperabilidad de los datos (lo que realmente no debería ser el caso, pero lo es). Pero también son notables los otros retos citados frecuentemente. Como lo indican las palabras resaltadas de la Figura 3, todos ellos se relacionan, de alguna manera con la *visibilidad*. Muchos de estos retos relacionados con la visibilidad existen todavía porque algunas soluciones para la protección de datos, simplemente carecen de "habilidades en virtualización". En otras palabras, les faltan la instrumentación y la consciencia contextual para ser capaces de demostrar a los administradores de virtualización, a los administradores de operaciones de TI y a otras partes interesadas, el verdadero estatus de protección y recuperación de su entorno virtual.

En el futuro, las organizaciones incrementarán aún más su nivel de virtualización. Así que los profesionales de TI afectados necesitan buscar soluciones modernas de protección de datos que estén equipadas con buena instrumentación y diseñadas teniendo en cuenta la agilidad de un entorno altamente virtualizado.

Gestión y habilitación de datos (DM&E) eficiente y rentable

La clave para entregar eficazmente los millares de resultados de recuperación que las organizaciones requieren es desbloquear el valor empresarial de los datos secundarios. Cuando la organización de TI desbloquea ese valor, puede también justificar mejor los mecanismos de protección en uso. Como lo demuestran los datos ilustrados en la Figura 2, el costo –sobre todo el costo de tener demasiadas copias de datos– es uno de los principales retos que enfrentan actualmente los profesionales de protección de datos. De manera similar, la reducción de los costos relacionados con almacenamiento es un mandato principal del liderazgo de TI (ver la Figura 1). La conflictiva realidad para los profesionales de TI es que el nivel de recuperabilidad y agilidad que las partes interesadas que demandan las partes interesadas de las unidades de negocios no siempre se puede cumplir solo con copias de seguridad.

Es por eso que los administradores de protección de datos, para cumplir con las SLA de sus organizaciones, se encuentran haciendo *más* (en realidad, una gama más amplia de *tipos* de) copias mediante instantáneas; réplicas;

© 2017 por The Enterprise Strategy Group, Inc. Todos los derechos reservados.

y copias de seguridad completas, progresivas y diferenciales. En realidad, la naturaleza parcial y temporal de las instantáneas, combinada con la flexibilidad de replicación, puede reducir el almacenamiento cuando son manejadas holísticamente y apuntaladas por una arquitectura de almacenamiento moderna. Pero, sin esas integraciones y estrategia complementaria, el almacenamiento de protección puede aumentar en respuesta al abordaje de las metas de recuperación, aún cuando la administración ejecutiva exija que se concreten esas reducciones de costos relacionadas con el almacenamiento. Y, para agravar el problema, otros equipos de TI (por ej.: los desarrolladores de aplicaciones y el personal de operaciones de TI) generan todavía más copias para respaldar sus propios esfuerzos de desarrollo y administración de parches.

Al habilitar "escenarios sin protección" (tales como DevOps, informes o analítica) a la vez de eliminar, comprimir y optimizar conscientemente el almacenamiento *y* utilizar mecanismos más inteligentes de protección de datos, una organización realmente puede:

- Lograr sus resultados de recuperación y agilidad de negocios.
- Establecer un enfoque holístico a largo plazo para la administración y reutilización de datos.
- Administrar exitosa y responsablemente el presupuesto de TI disponible.

Como tal, cualquier organización que se esfuerce por poseer una protección de datos moderna, debería buscar soluciones que proporcionen una gama exhaustiva de capacidades de recuperación a la vez de desbloquear un valor empresarial progresivo al habilitar casos de uso sin protección.

Protección exhaustiva con el portafolio de almacenamiento definido por software de IBM

IBM y su software Spectrum Protect (antes conocido por algunos como "Tivoli Storage Manager" o TSM) ha sido un líder innovador en la protección de datos empresariales durante muchas décadas. Sin embargo, sería un error suponer que la oferta se ha vuelto rancia como ha sucedido con otras soluciones de copias de seguridad antiguas. El producto básico Spectrum Protect ha seguido evolucionando para satisfacer las necesidades de las empresas modernas, e IBM ha expandido su portafolio de almacenamiento con IBM Spectrum Copy Data Management (Spectrum CDM) e IBM Spectrum Protect Plus (SPP).

IBM Spectrum Copy Data Management

Spectrum CDM es una nueva incorporación al portafolio de protección de datos de IBM Spectrum. Ha sido diseñado para habilitar casos de uso no relacionados con la -protección para datos secundarios –por ejemplo, DevOps, pruebas de parches e informes/analítica–.

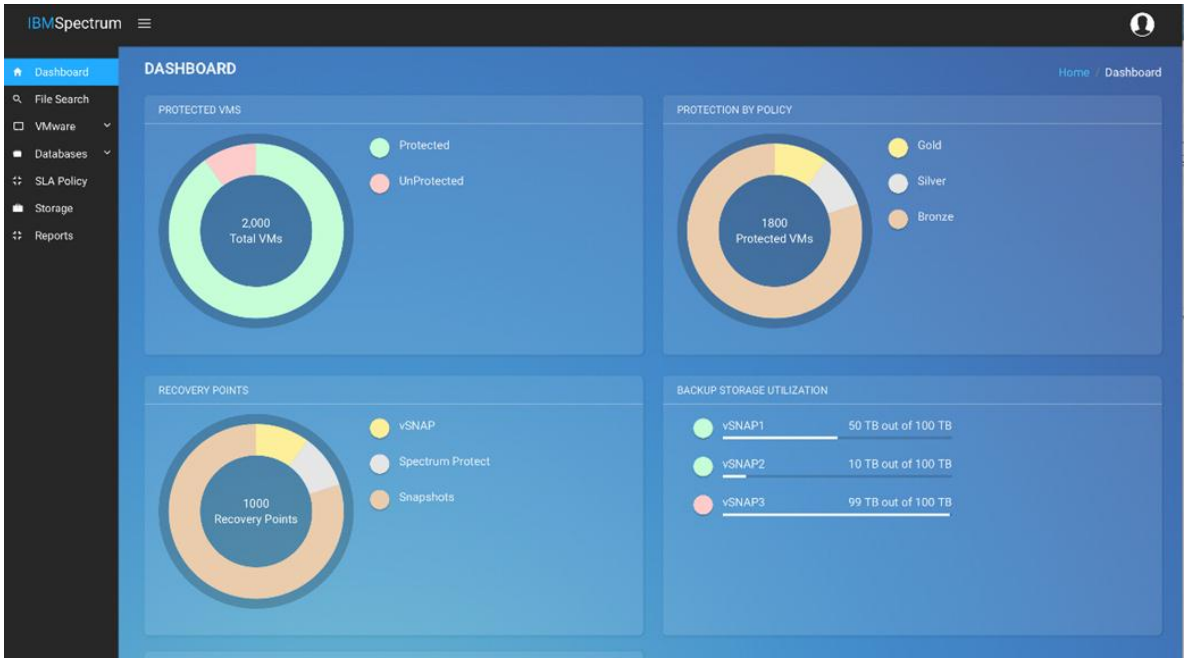
Al igual que las otras (si bien son pocas) ofertas de administración de copias de datos en el mercado actual, la meta principal de Spectrum CDM es facilitar el acceso a "datos de producción" sin comprometer, sobrecargar o alterar los conjuntos reales de datos de producción. Al aprovechar Spectrum CDM, los empleados de unidades de negocios, los codificadores/desarrolladores y varias otras partes interesadas podrán desbloquear valor empresarial progresivo de esos datos. Y esa capacidad hace que sea más fácil para la organización, como un todo, justificar otras inversiones en la protección y recuperación de datos moderna.

IBM Spectrum Protect Plus

SPP ha sido diseñado teniendo en cuenta a los generalistas de operaciones y administradores de virtualización de TI. Proporciona un marco centrado en SLA para garantizar la protección y recuperación ágiles de entornos altamente virtualizados, y tiene una interfaz de usuario (ver la Figura 4) que es suficientemente elegante y contemporánea para sorprender a los incondicionales usuarios de IBM.

© 2017 por The Enterprise Strategy Group, Inc. Todos los derechos reservados.

Figura 4. IBM Spectrum Protect Plus–Panel de Informes



Fuente: IBM

También posee las "habilidades de virtualización" descriptas anteriormente, según las cuales las políticas de SLA son definidas inicialmente por el administrador de TI correspondiente y luego simplemente activadas –ya sea en VM o en "hosts"– según lo dicten las necesidades empresariales.

Y como uno podría esperar, SPP y Spectrum CDM se integran con el software básico Spectrum Protect y con el resto del portafolio de almacenamiento de IBM, proporcionando de esta manera una agilidad empresarial todavía mayor.

La mayor verdad

La protección de datos debe continuar evolucionando si alguna vez va a abordar los retos que tantas organizaciones están enfrentando. Pero lo que es interesante, es que los mecanismos de copias de seguridad discretos, independientes –e incluso los administradores de copias de seguridad exclusivos– probablemente tengan menos prominencia a medida que los profesionales de operaciones de TI continúan profundizando su participación en la definición e implementación de las estrategias de protección de datos de sus organizaciones.

Con esa probabilidad en mente, las empresas continuarán confiando, casi con certeza, en mecanismos exhaustivos de protección de datos, tales como IBM Spectrum Protect, aunque sigan buscando mecanismos que sean accesibles y construidos a la medida de sus cargas de trabajo más importantes –mecanismos que sean capaces de desbloquear valor empresarial progresivo para respaldar una estrategia de administración de datos con base amplia.

Si se considera la manera en que estas tendencias se están desplegando, es positivo comprobar que IBM, innovadora de larga data en la protección de datos, continúa expandiendo y enriqueciendo su portafolio con ofertas adaptadas para los administradores de VA y generalistas de TI. Está dando los pasos correctos para habilitar los casos de uso que requieren las empresas actuales.

Todas los nombres comerciales son propiedad de sus respectivas compañías. La información contenida en esta publicación ha sido obtenida de fuentes que The Enterprise Strategy Group (ESG) considera confiables, pero no es garantizada por ESG. Esta publicación puede contener opiniones de ESG, que están sujetas a cambios. Los derechos de autor de esta publicación han sido registrados por The Enterprise Strategy Group, Inc. Cualquier reproducción o redistribución de esta publicación, parcial o total, ya sea en formato impreso, electrónicamente, o de otra manera a personas no autorizadas para recibirla, sin el expreso consentimiento de The Enterprise Strategy Group, Inc., será una violación de la ley de derechos de autor de EE. UU. y será pasible de demanda por daños civiles y, si corresponde, de acción penal. En caso de tener alguna duda, contactar a ESG Client Relations llamando al 508.482.0188.

© 2017 por The Enterprise Strategy Group, Inc. Todos los derechos reservados.