

La gestión eficiente del dato en un entorno híbrido es el gran reto del sector

Datos, historia de una continua revalorización al alza

Que actualmente los datos son el activo más importante para las empresas no es ningún secreto. De hecho, para la mayoría la gestión de estos activos críticos es una prioridad, pero también un desafío debido al incremento desorbitado de datos que se genera y a problemáticas relacionadas con la normativa o la seguridad. Sin embargo, la adecuada gestión y administración de este preciado bien puede traer grandes beneficios a las organizaciones.

Entonces, ¿en qué punto se encuentran los datos y su gestión en España? Y, especialmente, ¿qué papel juegan dentro de las estrategias de las organizaciones?

Olga Romero



"Los datos se han vuelto cada vez más valiosos para las empresas por la información valiosa que proporcionan, pero, por desgracia, muchas de ellas no realizan un seguimiento adecuado de su difusión y carecen de visibilidad sobre dónde se almacenan, cómo se utilizan o cómo se accede a ellos", comenta Candid Wuest, vicepresidente de Investigación sobre Ciberprotección en Acronis. Además, recuerda que "la evolución de la tecnología ha facilitado la recopilación, almacenamiento y análisis de grandes cantidades de datos, especialmente en la nube".

David Benito, director de canal de Commvault Iberia, también hace referencia al volumen global de datos: "se ha multiplicado por 30 en los últimos 10 años". Mismo ritmo de crecimiento que ha seguido la revalorización del valor de estos activos. El directivo comenta también que existe una "brecha de integridad del negocio", es decir, las empresas son conscientes de que hay una brecha entre la ubicación real de los datos y dónde deberían estar realmen-

Los datos se han convertido en un activo imprescindible debido a las ventajas competitivas que aportan a las empresas

te para dar los servicios requeridos. Por ello, se está viendo "una evolución en la percepción que tienen las empresas del *backup*".

Destaca también el papel de los datos Jaime Balañá, director técnico de NetApp para Iberia y LATAM. "Son un bien imprescindible y el futuro de la innovación reside en nuestra capacidad para aprovechar el potencial de los datos y trabajar en torno a ellos", explica. Esta realidad convertirá, según Balañá, la seguridad y fiabilidad de los datos en prioridades para las empresas, así como su gestión y la ex-

tracción del valor competitivo de los mismos. También habla de prioridades Carmen Delinchán, *senior systems engineering director* de Pure Storage Iberia. "Encontrar soluciones más óptimas y sostenibles para gestionar y almacenar los datos es una necesidad urgente para las empresas españolas", indica. Una finalidad relacionada con las previsiones de Gartner y es que, según la consultora, los datos no estructurados tienen un crecimiento del 30 % anual y se prevé que para 2027 este crecimiento se haya cuadruplicado.

"La evolución de los datos ha estado marcada por las necesidades de las compañías y el rol que ha ido cogiendo el entorno digital en nuestras vidas", asegura Rafael Quintana, director regional de Qlik en Iberia. Una digitalización que, como explica, ha dado como resultado el recibir, capturar y analizar los datos para tomar mejores decisiones y, por ende, "crecer, actuar con agilidad en tiempo real y diferenciarse de la competencia". Además, recuerda que a pesar de la evolución en Es-

paña aún queda camino por recorrer y señala como fundamental el papel del programa Kit Digital, el plan España Digital 2026 y los fondos NextGenerationEU.

También resalta la importancia que ha tenido la digitalización, junto con la globalización, en la revalorización de los datos Víctor Pérez de Mingo, *senior systems engineer* de Veeam. Igualmente, subraya la necesidad que tienen las empresas hoy en día de tomar decisiones basadas en datos actualizados y "ser capaces de protegerlos". Razón por la que, según un estudio de la compañía, "las organizaciones en España y Portugal esperan aumentar su presupuesto en protección de datos un 7 % este año".

Por último, Ignacio de Pedro, *country manager* Iberia en Veritas Technologies LLC, asegura que "todavía hay mucho margen de mejora ya que hay muchas organizaciones que, aunque entienden el valor del dato, aún no disponen de planes

ni de herramientas para su gestión y que les permita manejar de forma adecuada los diferentes retos". Para de Pedro los datos "han dejado de ser el petróleo del siglo XXI para convertirse en el agua necesaria para vivir".

La soberanía del dato a debate

2022 fue el año en el que numerosas compañías se decantaron por España para instalar sus nuevas regiones *cloud*. Elección que celebran Benito, Balañá, Quintana y de Pedro ya

que facilita el control y la soberanía del dato. Los cuatro directivos coinciden en destacar la importancia y repercusión que estas decisiones tendrán, tanto a nivel económico como social, en España y, además, resaltan otros aspectos fundamentales como la garantía que supone para las empresas europeas de cara al cumplimiento normativo.

Un cumplimiento normativo que, en el caso de compañías con sedes en Europa, la lógica, según Quintana, "indica que han de regirse por el marco legal que establece la Unión Europea (GDPR) y el proyecto Gaia-X". Una lógica que de seguirse favorecería a España ya que "aunque tener los datos en el mismo país no es una obligación explícita, es una tendencia cada vez más visible en los requisitos de los clientes", afirma Tsvetomira Godinova, *Compliance Specialist* en Acronis. Y es que reducir la incertidumbre, así como los posibles costes legales y de cumplimiento, rigiéndose por



El *backup* es la última línea de defensa contra el *ransomware* y se ha vuelto objeto de deseo para los *hackers*

normativas de países afines es una máxima para las empresas.

Sin embargo, la elección de España para albergar nuevas regiones *cloud* supondrá también una prueba para las empresas. Las cuales tendrán que demostrar su nivel de concienciación en soberanía del dato y la importancia que le dan a estos activos. "Entendemos que las organizaciones tienen cierta conciencia normativa sobre dónde deben residir los datos, pero quizás no tienen tan interiorizado la problemática de los modelos de responsabilidad compartida de la información al movernos a entornos *cloud*", profundiza el directivo de Veritas Technologies LLC.

Por su parte, el director de canal de Commvault Iberia reflexiona sobre la seguridad y advierte de que "los proveedores *cloud* tienen

la obligación de proteger su servicio e infraestructura, pero la protección de los datos del cliente es responsabilidad de éste, por lo que deben contar también con soluciones de protección y de gestión de datos".

En cuanto a las estrategias de protección de datos, desde Veeam prevén que el 81 % de las empresas de EMEA se decante por soluciones en la nube. Unas estrategias de protección que, según Pérez de Mingo, están muy consolidadas y extendidas al igual que el uso de proveedores de alojamiento en la nube.

¿Y los retos legales?

Cada 28 de enero, desde 2006, se celebra el Día Europeo de la Protección de Datos. Una fecha dedicada a aumentar la concienciación de los ciudadanos sobre el derecho a la pro-

tección de datos. Actualmente "España es uno de los países europeos que más avanzados está en normativas para la protección de los datos personales", destaca Benito. Y es que, como recuerda, nuestro país ha sido el primero en adoptar una Carta de Derechos Digitales.

Asimismo, el responsable de canal de Commvault Iberia añade que en pocas semanas estará listo el texto final de la Ley de Resiliencia Operativa Digital (DORA). Una normativa a nivel europeo que entrará en vigor en los próximos años y que "obligará a revisar los sistemas informáticos heredados para garantizar que cumplen con la normativa", explica. Una revisión y ajuste que, según de Pedro, será uno de los grandes retos, junto a las fugas de información, en este 2023. "En los últimos años hemos visto una actividad frenética en materia regulatoria respecto a la privacidad, especialmente en Europa, y esto obliga a las empresas y organizaciones españolas a ajustarse a esas normativas", comenta.

Para Godinova el "denso panorama normativo es el principal reto legal" que tienen por delante las empresas españolas a corto, medio y largo plazo. Tal y como asegura, "las leyes e iniciativas legislativas relacionadas con la ciberseguridad y la protección de datos van en aumento y esto obligará a las empresas a mantener programas de cumplimiento flexibles y sujetos a mejoras constantes".

Papel del *backup* en la protección del dato

Según datos de un estudio de Veeam, el 78 % del tejido empresarial español sufrió, en 2023, un ciberataque. Detrás de este resultado está el crecimiento imparable del *ransomware*, el cual obliga a las organizaciones a estar alerta y establecer sólidas estrategias de protección del dato. En esta ardua tarea "las copias de seguridad son cruciales para cualquier empresa hoy en día", defiende el vicepresidente de Investigación sobre Ciberprotección en Acronis. Para Wuest el plan de negocio debe incluir las copias de seguridad, así como su

revisión periódica, y recuerda que "aunque la mayoría de las empresas son conscientes de la importancia de estas copias, muchas olvidan que los ciberdelincuentes intentarán borrarlas durante sus ataques".

Misma opinión comparte Benito. El directivo de Commvault Iberia explica que "el *backup* es la última línea de defensa contra el *ransomware*, pero también es objetivo de los cibercriminales". Ante este escenario, la solución es disponer de *backups* aislados y definir el plan de seguridad desde diferentes puntos,

es decir, utilizar una estrategia multicapa.

Para Veeam disponer de una copia de seguridad también es la última línea de defensa contra el *ransomware*. En este sentido desde la compañía, como explica su *senior systems engineer*, "recomendamos la regla 3-2-1-1-0, es decir, tener siempre, al menos, tres copias de datos importantes en, al menos, dos tipos de soporte con una *offsite* y otra *offline* y con cero *backups* no verificados o fallidos".

"El *backup* se está consolidando como una pieza clave en las estrategias de protección



del dato y ciberresiliencia", sentencia el responsable de Veritas Technologies LLC para Iberia. Para de Pedro que los ciberdelincuentes hayan puesto en el centro de sus ataques al *backup* es un gran desafío para las organizaciones a las que aconseja disponer de plataformas de *backup* que les permitan sobrevivir a un ataque, "conceptos como bastionado, *zero trust* y almacenamiento inmutable son vitales para diseñar estas plataformas", asegura. En el caso concreto de las empresas españolas, de Pedro cree que en la mayoría de los casos han tomado conciencia. Sin embargo, indica que hace falta "adaptar los entornos a las nuevas características para así garantizar esa última línea de defensa".

Entorno híbrido, ¿cómo conseguir una gestión eficiente?

Destaca Balañá las "enormes ventajas competitivas" que los datos ofrecen a las empresas que los recogen, conservan y explotan. Pero el almacenamiento de esta elevada cantidad

Las brechas de seguridad y el incremento de la normativa en materia de privacidad están entre los principales retos para 2023

de información también puede ocasionarles muchos problemas. ¿Cómo hacerles frente? Con anticipación, agilidad y control. "En NetApp apostamos por modelos de gestión basados en un concepto híbrido, donde la nube pública nos ofrece la posibilidad de ser ágiles y la privada el control de los datos allí donde sea necesario", detalla.

Para Derlinchán la clave para conseguir una gestión eficiente en un mundo cada vez más complejo es adoptar soluciones sencillas y flexibles. En cuanto al desafío que supone el entorno híbrido y *multicloud* actual, la directiva de Pure Storage Iberia indica que "las empresas deben asegurarse de que pueden utilizar la mejor nube para cada caso de uso y evitar así el bloqueo". Para ello deben apoyarse en el uso de contenedores de las aplica-

ciones e impulsar "la gestión de aplicaciones a través de plataformas de kubernetes con la flexibilidad, velocidad, rentabilidad y seguridad necesarias para garantizar el éxito en un entorno neutral de nube".

Planificación. Este es el aspecto que Quintana señala como fundamental para la gestión del dato en los entornos híbridos. El directivo subraya la importancia de conocer el punto de partida, las necesidades y los objetivos. Asimismo, recuerda que no todo tiene que estar en la nube ni gestionarse de la misma manera. "Es crucial evaluar lo que requieren la empresa y los empleados para elegir el entorno más adecuado y garantizar la efectividad".

Sobre cómo combatir la complejidad del entorno, el responsable de Qlik en Iberia apela a la necesidad de "simplificar la infraestructura,

capacitar a los equipos dotándoles de agilidad y flexibilidad, monitorizar bien los activos y asegurar el cumplimiento legal".

En cuanto a los errores a evitar en la gestión del dato, Quintana vuelve a señalar a la planificación, sin la cual no hay éxito posible. Además, recuerda que, al realizar un cambio de paradigma en la empresa, ésta debe darles tiempo a los empleados para adaptarse a los

cambios realizados. También hace referencia a la planificación Derlinchán. La directiva de Pure Storage Iberia asegura que "los planes tienen que responder rápidamente para satisfacer nuevas e imprevistas demandas y la tecnología debe ser capaz de adaptarse al unísono".

Por su parte, Balañá defiende que "por lo general, las empresas saben muy bien lo que

quieren y son absolutamente conscientes de la necesidad de tener una estrategia clara y bien definida desde el principio".

Retos para 2023

La gestión del dato en un entorno cada vez más híbrido dejará, en este 2023, algunos retos relacionados con los costes, la gestión, la adquisición de talento, compatibilidad e interoperabilidad. Además, los directivos coinciden en señalar otros desafíos como el ajuste a las nuevas normativas, el aumento del cibercrimen o las brechas de seguridad que facilitarán la fuga de información.

Las organizaciones también deberán enfrentarse a otros obstáculos como la sostenibilidad, la capacitación de los empleados o la integración de la inteligencia artificial en el canal de datos. Tampoco hay que olvidarse del reto que supone, ante el aumento de datos no estructurados, poder acceder a la información en cualquier momento o la gestión de los datos sintéticos y derivados.

