Backup, inmutabilidad y ciberresilencia: tridente para la protección del dato

La aceleración de los procesos de digitalización de las empresas, el crecimiento exponencial del volumen de información, la necesidad de reforzar la resiliencia frente a los ciberataques y fallos de sistemas, y la obligatoriedad de cumplir con las normativas siguen posibilitando la plena vigencia del *backup*. Una tecnología, último fortín frente al *ransomware*, que se mantiene a la cabeza de las amenazas, pero que debe entenderse, para ofrecer una estrategia de ciberseguridad completa, con soluciones de prevención, detección y recuperación, para garantizar a las empresas su continuidad del negocio.

Marilés de Pedro

Se trata de una tecnología que, a pesar de su madurez, ha recuperado todo su glamour tecnológico. Ha dejado de ser un gasto operativo para convertirse en un pilar estratégico de continuidad y ciberresiliencia. Ahora bien, los expertos coinciden: no basta con almacenar copias de seguridad; la clave está en garantizar la recuperación rápida y fiable de los servicios críticos. Se prevé que el tamaño del mercado global de software de respaldo y recuperación empresarial alcance los 8.960 millones de dólares este año y crezca hasta los 17.960 millones en 2035 con una tasa anual compuesta del 7,2% de 2026 a 2035.

> "Hoy es impensable que una copia de seguridad pueda modificarse o eliminarse; hace años no se consideraba crítico"

Backup versus *ransomware*

Las copias de seguridad, tradicionalmente observadas como un mecanismo técnico de recuperación, se han transformado en un elemento central de la continuidad del negocio. "No se trata solo de almacenar copias, sino de garantizar que la organización pueda seguir operando cuando ocurre un incidente. Una copia tradicional devuelve los datos, pero las soluciones modernas permiten la recuperación casi inmediata, minimizando las pérdidas", explica Eduardo García, director general de Acronis en España y Portugal, que insiste en que el *backup* por sí solo no es suficiente. "No evita el ataque, no bloquea el *malware* ni impide la exfiltración de información. La protección real exige un enfoque integrado donde se conjugue que la prevención, la detección y la recuperación trabajen juntas".

El crecimiento y la evolución del *ransomware* ha fortalecido el papel del *backup* como tecnología clave para hacerle frente. Ya no se trata de ataques masivos y oportunistas, sino de operaciones mucho más dirigidas, que estudian en profundidad el entorno de la víctima y buscan maximizar el impacto. "Los ataques dirigidos buscan exfiltrar datos de forma silenciosa: estos se roban sin cifrarse, aumentando el daño reputacional y legal", recuerda Víctor Pérez de Mingo, presales manager para España y Portugal de Veeam. Solo el 29 % de los responsables de TI confía plenamente en su capacidad de recuperar los datos críticos. "El desafío no es tener copias, sino poder demostrar que la recuperación es efectiva bajo una presión real".

Un *ransomware* al que también ayuda la inteligencia artificial. "Los ataques no buscan solo cifrar datos: uno de sus principales objetivos son las copias de seguridad, precisamente para impedir una recuperación fiable", alerta David Sanz, senior director sales engineering Europe South de Commvault. Aunque las copias son el "mecanismo" más

eficaz para asegurar la recuperación en caso de ataque, deben integrarse en una estrategia de ciberresiliencia que incluya gobernanza, protección de identidades y restauraciones rápidas de copias limpias. "Operar en entornos híbridos y multicloud complica diseñar una política de protección coherente y disfrutar de una visibilidad completa de dónde residen los datos ya que las empresas manejan herramientas que no se comunican entre sí, lo que crea puntos ciegos y una mayor exposición al riesgo".

Eduardo García destaca que la inmutabilidad y la replicación en entornos aislados han marcado un cambio decisivo en la evolución del *backup*: "Hoy es impensable que una copia de seguridad pueda modificarse o eliminarse, algo que hace unos años no se consideraba crítico. Además, la replicación en entornos lógicos y físicos aislados refuerza la protección frente a ataques dirigidos específicamente contra los sistemas de recuperación".

David Sanz subraya el papel de la inteligencia artificial en esta evolución: "Las copias modernas protegen no solo contra fallos, sino contra ataques sofisticados e intencionados. La IA permite recuperaciones limpias y completas después de un ciberataque".

Backup y ciberseguridad: un rol estratégico

El *backup*, a juicio de los principales proveedores tecnológicos, es una tecnología esencial en la estrategia de ciberseguridad y para garantizar la continuidad del negocio. "La ciberseguridad previene y mitiga muchos incidentes, pero cuando falla, es imprescindible contar con un plan de respaldo sólido que permita volver a la normalidad con rapidez.

Es aquí donde el *backup*, combinado con una recuperación ante desastres eficiente, cobra su verdadero valor", asegura Eduardo García.

David Sanz añade que la copia de seguridad se convierte en la última línea de defensa dentro de una arquitectura por capas: "Permite volver a un estado seguro cuando todo lo demás falla". Ahora bien, no basta por sí solo. "Es fundamental complementarlo con tecnologías de prevención y detección para detectar el ataque antes de que cause daños".

El directivo también alerta de la resiliencia de la identidad: nueve de cada diez ataques se dirigen a sistemas como Active Directory, "las llaves del reino" de una empresa. "Cuando se detecta un cambio sospechoso, los equipos pueden revisarlo en detalle y revertirlo para anularlo inmediatamente, lo que permite corregir rápidamente los cambios no autorizados o accidentales, manteniendo disponibles sus servicios de identidad críticos".

Víctor Pérez de Mingo insiste en que el *backup* no puede ser una tecnología aislada; algo crítico en entornos *multicloud*, SaaS y de trabajo distribuido, donde casi el 60 % de los responsables de TI ha reconocido haber perdido visibilidad sobre dónde se encuentran realmente sus datos. "En este escenario, el *backup* debe integrarse con soluciones de detección y respuesta, con arquitecturas como XDR o SASE y con políticas claras de gobernanza, cumplimiento y soberanía del dato".

> "La copia de seguridad permite volver a un estado seguro cuando todo lo demás falla"

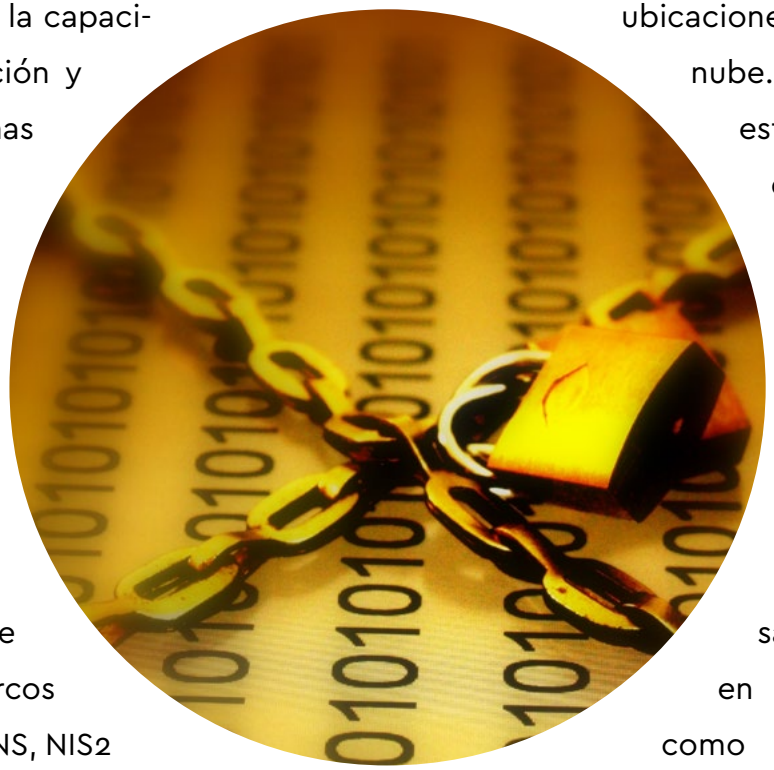
Implantación del *backup* en España

En España, el *backup* está ampliamente presente, aunque los especialistas coinciden en que su nivel de actualización frente a amenazas modernas aún deja margen de mejora. Santiago Sánchez, *sales engineer Iberia* de Cohesity, asegura que prácticamente todas las organizaciones realizan copias de seguridad, pero muchas siguen apoyándose en arquitecturas tradicionales que no están diseñadas para enfrentar ataques persistentes y sofisticados. "Durante los últimos años hemos observado un cambio claro: sectores como la banca, la industria o la Administración pública están apostando por plataformas más avanzadas, impulsados por regulaciones como DORA o NIS2 y por la necesidad de garantizar continuidad operativa incluso ante un ataque", explica. Aun así, cree que "la ciberresiliencia todavía está en proceso de maduración".

David Blanqué, *Iberia sales manager* de ExaGrid, alerta, a pesar de esta presencia generalizada, de que en muchos casos se entiende como una tecnología orientada, principalmente, a almacenar datos. "Se prio-

"En escenarios de recuperación, no basta con que la copia esté protegida; hay que validar la consistencia y la limpieza de los datos"

riza el coste frente a la capacidad real de protección y recuperación". Muchas empresas, continúa, lo gestionan como una rutina operativa, y "no como un elemento clave para proteger la continuidad del negocio". Ahora bien, corrobora que las normativas y marcos regulatorios como ENS, NIS2 o DORA están actuando como catalizadores de un cambio de mentalidad.



En la Unión Europea, el 79,2 % de las organizaciones realiza copias de seguridad en ubicaciones separadas o en la nube. Un dato que sitúa esta práctica solo por detrás de la autenticación robusta de usuarios en lo que a medidas de protección se refiere. En España, aunque la mayoría de las empresas —especialmente en sectores regulados como banca, infraestructuras críticas o grandes corporaciones— ya cuenta con plataformas de protección, Antonio Espuela, *director technical sales EMEA Western* de Hitachi Vantara, alerta de que, en muchos casos, el *backup* sigue considerándose una tecnología "heredada", y no como una estrategia activa de resiliencia. "La brecha más relevante se observa en la adopción de modelos avanzados orientados a la protección frente al *ransomware* mediante aislamiento lógico, inmutabilidad y verificación, así como arquitecturas híbridas y *multicloud* que integren el *backup* en un tejido de protección unificado".

Errores que siguen debilitando el *backup*

A pesar de que el *backup* está ampliamente implantado en las organizaciones, los especialistas coinciden en que los errores no suelen estar en la tecnología, sino en la forma de utilizarla y en el enfoque estratégico con el que se aborda.

> "El desafío no es tener copias, sino demostrar que la recuperación es efectiva bajo una presión real"

Desde Mast Storage advierten de que la metodología es tan determinante como la herramienta elegida. "Con la misma tecnología se pueden obtener resultados muy diferentes y niveles de seguridad dispares", señala Loreto Lojo, directora comercial del fabricante. Entre los fallos más habituales destaca la dependencia de procesos manuales —cuando el *backup* depende de una persona concreta y no está automatizado— y la ausencia de copias en múltiples ubicaciones siguiendo esquemas como el 3-2-1 o, sobre todo, 3-2-1+1, que es, a su juicio, la fórmula ideal, "en la que la copia externalizada en el *cloud* está replicada". También las políticas de retención excesivamente cortas que priorizan el ahorro de espacio frente a la capacidad real de recuperación.

A estos problemas se suman prácticas deficientes, como realizar copias de copias que impiden la deduplicación, almacenar datos sin cifrar o gestionar incorrectamente las claves de cifrado, utilizar herramientas básicas sin controles de acceso avanzados como el doble factor de autenticación, o confiar únicamente en copias locales fácilmente accesibles en caso de *ransomware*. Lojo también alerta sobre un error crítico que sigue repitiéndose: la falta de simulacros de restauración. "Muchas empresas creen que el *backup* funciona hasta que lo necesitan. Cuando descubren que los datos no estaban realmente protegidos ya no hay margen de maniobra". De ahí la importancia de auditorías periódicas y de un seguimiento continuo del estado de las copias.

Desde una perspectiva más estratégica, David Blanqué considera que el principal error sigue siendo conceptual. "Durante años, el *backup* ha sido tratado como una extensión del almacenamiento o como un gasto necesario, rara vez estaba integrado en los proyectos estratégicos del negocio, ni era una parte esencial de la protección del dato". En un contexto de *ransomware* y de ataques dirigidos, "el *backup* determina si una organización puede seguir operando o no tras un incidente", subraya. Sin embargo, muchas decisiones siguen basándose en métricas incompletas —como una capacidad bruta o en ratios de eficiencia— sin cuestionar si la arquitectura está realmente preparada para ofrecer una recuperación fiable y controlada frente a ataques modernos. "El *backup* ha dejado de ser un coste asumido para convertirse en un pilar de la resiliencia cibernética de las empresas", concluye.

Santiago Sánchez apunta que uno de los errores más extendidos es creer que dispo-

ner de copias es estar protegidos. A ello se suma no blindar el propio sistema de *backup*, que hoy se ha convertido en un objetivo prioritario para los atacantes, y la falta de pruebas periódicas de restauración. "Muchas compañías descubren si sus copias funcionan precisamente el día que más las necesitan". Además, señala que todavía abundan estrategias incompletas que no combinan de forma coherente *backup*, inmutabilidad, copias *off-site*, análisis de anomalías y validaciones continuas.

Por su parte, Antonio Espuela alerta de que muchos ataques buscan directamente la destrucción o corrupción de los repositorios de *backup*, lo que invalida el supuesto de que tener copias sea sinónimo de estar protegido. Otro fallo recurrente es confiar en que el *backup* "funciona" sin realizar pruebas de restauración realistas, algo especialmente crítico en un contexto en el que las organizaciones deben demostrar RTO y RPO —o, como empieza a denominarse, *Return to Operations*

> "Europa tiene ante sí un auténtico reto de abordar este problema potenciando la aparición de fabricantes europeos"

(recuperación rápida del servicio) y *Recovery Point Objective* (pérdida nula o mínima de datos)— tanto a nivel interno como para cumplir normativas europeas como DORA o NIS2. A esto se añade la dependencia excesiva de infraestructuras tradicionales que no escalan frente al crecimiento exponencial de los datos, especialmente los no estructurados, que ya superan el 70 % del total; encareciendo y ralentizando los procesos de *backup* si no se adoptan arquitecturas modernas orientadas a objeto y *multicloud*. "Muchas organizacio-

La aportación diferencial del *backup* a la ciberseguridad

Los fabricantes especializados en *backup* y resiliencia de datos, que ya integran una estrategia de ciberseguridad, reivindican una aportación diferencial en relación a los proveedores con un foco exclusivo en la protección: no se trata "solo" de evitar el ataque, sino de garantizar la continuidad cuando el incidente se ha producido.

Eduardo García explica que esta perspectiva marca una diferencia clara frente a los fabricantes de seguridad clásicos, históricamente más centrados en la prevención y la detección. "Un proveedor de *backup* diseña sus soluciones pensando también en la recuperación real del negocio, en cómo volver a operar cuando el ataque ya ha tenido éxito". En este sentido, la compañía subraya la importancia de integrar de forma nativa copia de seguridad, ciberseguridad y recuperación ante desastres, de manera que "prevención, detección y restauración funcionen como un mismo sistema, y no como piezas desconectadas que luego hay que coordinar manualmente".

Daviz Sanz sitúa los datos y las identidades en el centro de la resiliencia cibernética. "La seguridad es un deporte de equipo", destaca, subrayando la necesidad de colaborar estrechamente con otros proveedores y socios de ciberseguridad.

Víctor Pérez de Mingo señala que la principal aportación de un fabricante especializado en resiliencia de datos parte de una premisa clara: los incidentes no son una posibilidad remota, sino una certeza. "Más allá de bloquear amenazas, el foco está en garantizar que la organización pueda volver a operar con rapidez, confianza y control". Ese enfoque se apoya en un conocimiento profundo del dato, de su ciclo de vida y, sobre todo, de su capacidad real de recuperación.

Además, pone el acento en que la resiliencia ha dejado de ser solo una cuestión técnica para convertirse en un factor regulatorio y de negocio, impulsado por normativas como NIS2 o DORA. "La resiliencia de datos no solo permite cumplir con los requisitos legales, sino que puede convertirse en una ventaja competitiva". Según un análisis realizado por Veeam junto a McKinsey, las organizaciones con mayor madurez en resiliencia de datos registran un crecimiento medio de ingresos superior al de aquellas que no la han priorizado.

nes aún no integran adecuadamente *backup* y ciberseguridad, cuando capacidades como la detección de anomalías, el análisis de comportamiento o la validación previa a la recuperación ya son requisitos esenciales frente a ataques cada vez más sofisticados".

Inmutabilidad: pilar clave, pero no una solución absoluta

La inmutabilidad del *backup* se ha consolidado como uno de los conceptos más citados en las estrategias modernas de protección frente al *ransomware*. Ahora bien, es una condición necesaria, pero no suficiente. Solo cuando se combina con aislamiento, controles de acceso, análisis continuo y pruebas de recuperación, se convierte en una verdadera garantía para la continuidad del negocio.

Loreto Lojo explica que una copia inmutable, al no poder modificarse ni borrarse durante el periodo de retención definido, protege los datos frente al cifrado malicioso, la eliminación accidental o incluso frente a empleados malintencionados. Además, facilita el cumplimiento normativo al permitir demostrar que los datos históricos no han sido alterados.

No obstante, advierte de una confusión habitual: inmutabilidad no es lo mismo que copia *off-site*. "La copia inmutable debería combinarse con una copia *air-gap* para garantizar realmente la integridad de los datos", señala.

David Blanqué recuerda que la inmutabilidad no es un concepto nuevo y que existe desde hace años en tecnologías como *snapshots*, WORM o almacenamiento de objetos. El problema aparece cuando se presenta como una solución definitiva. "Por sí sola no evita que los datos sigan expuestos a través de la red ya que lo que es visible sigue siendo atacable". Desde una perspectiva de ciberseguridad, el objetivo no es solo impedir la modificación del dato, sino reducir al máximo los vectores de ataque, limitando accesos y aislando los repositorios. "La inmutabilidad protege el dato, su aislamiento garantiza la recuperación", resume.

Santiago Sánchez insiste en que la inmutabilidad, siendo pilar de la estrategia de protección, tiene límites claros. "No evita que

un *backup* contenga datos ya comprometidos si la infección se produjo antes de su ejecución, ni sustituye la necesidad de supervisión inteligente, segmentación o análisis de anomalías. Es la base, sí, pero no el techo", señala.

Antonio Espuela señala que su valor se manifiesta cuando se integra en un enfoque más amplio de ciberresilencia. "Permite aislar las copias frente a ataques directos, facilita el cumplimiento normativo y se complementa con capacidades de análisis de anomalías que ayuden a identificar copias potencialmente contaminadas". Sin embargo, también subraya sus límites: la inmutabilidad no protege frente a ataques que alteran los datos antes del *backup*, ni frente a amenazas internas si no existe una correcta segregación de identidades y claves. "En escenarios reales de recuperación, no basta con que la copia esté protegida; es imprescindible validar la consistencia y la "limpieza" de los datos antes de devolverlos a producción".

Propuestas concretas de los fabricantes

Cuando un ciberataque afecta a la organización, la recuperación ya no se mide solo en rapidez, sino en seguridad y fiabilidad. Para lograrlo, Santiago Sánchez apela al concepto de "sala limpia" de recuperación, un entorno aislado y controlado donde los *backups* se inspeccionan cuidadosamente antes de reintegrarlos al negocio. "Se monitoriza el comportamiento del sistema y se comprueba que no existan puertas traseras, *malware* latente o procesos sospechosos.

David Blanqué insiste en que la recuperación fiable no es un evento fortuito, sino un proceso que debe diseñarse y verificarse con antelación. "La integridad de la restauración no se garantiza el día del incidente, sino mucho antes. Es necesario auditar y proteger cada copia de forma sistemática, confirmar que los *backups* se completan correctamente y que no contienen corrupción silenciosa ni amenazas latentes", señala. La estrategia, puntualiza, debe adaptarse al ciclo de vida de los datos. "Los *backups* recientes requieren tiempos de recuperación muy bajos, mientras que los datos más antiguos demandan retención segura y eficiencia".

Desde Hitachi Vantara añaden que garantizar la integridad de una restauración exige un enfoque multinivel que empieza antes del ataque. "Hay que verificar la salud del *backup* mediante la detección de anomalías, el análisis de metadatos y la comparación temporal entre versiones para identificar copias potencialmente comprometidas", aconseja Espuela. No olvida apelar al aislamiento de los procesos de recuperación utilizando entornos protegidos "donde las copias se validan antes de reintroducirlas en producción".