# EL RESPALDO DE LOS DATOS

Cristina López Albarrán

**Las soluciones de backup y disaster recovery en el entorno del data center son cada vez más críticas. Las organizaciones se mueven hacia entornos híbridos y el dato está cada vez más fragmentado, lo que hace que su protección sea también una tarea cada vez más compleja. Las compañías deben hacer frente al persistente ransomware a la par que aseguran el cumplimiento de normativas y salvaguardan la continuidad de su negocio.**

La realización de copias de seguridad y de planes de recuperación de la información almacenada por una compañía son procesos críticos en el ecosistema de los centros de datos; y dada su criticidad, no están exentos de desafíos. Más bien al contrario. Los volúmenes de datos siguen creciendo, las aplicaciones se vuelven más dinámicas y las amenazas como el ransomware aumentan de manera exponencial. Con este panorama, un rendimiento lento de una solución de este calado se presenta como un gran problema para muchas empresas. Mientras tanto, los métodos tradicionales de backup y recovery están cambiando aceleradamente, pasando de cinta a repositorios de disco y nube. Además de los quebraderos de cabeza que suponen los sistemas on-premise, debemos añadir que las aplicaciones alojadas en plataformas IaaS y externalizadas en SaaS exigen niveles iguales de protección. Estos requisitos tan plurales y diversos están llevando a las organizaciones a buscar propuestas que puedan proteger todo (servidores virtuales y físicos, aplicaciones en nubes IaaS públicas y una lista creciente de aplicaciones SaaS), en lugar de adoptar soluciones de múltiples puntos. Como resultado, la selección de un producto de respaldo que pueda satisfacer las necesidades del negocio durante los próximos tres a cinco años se ha convertido en una labor importante y estratégica.

Y harto complicada. Como hemos mencionado, los repositorios de datos corporativos están más fragmentados que nunca dada la proliferación de almacenamiento en la nube, dispositivos móviles, software como servicio e innovaciones de código abierto. Muchas organizaciones también están recurriendo a entornos de nubes híbridas y multicloud. De hecho, una investigación de IDC señala que más del 80% de las nuevas implementaciones de aplicaciones incluirán un elemento de nube. El resultado es un panorama de protección de datos más complejo que nunca. Independientemente de dónde residan los datos o quién administre la aplicación, las empresas TIC se hallan en la tesitura de proteger todas las fuentes de datos de acuerdo con los requisitos corporativos. En muchos casos, estas obligaciones incluyen requisitos de nivel de servicio de pro-

> Asegurar la continuidad de los servicios de TI es una parte esencial de la tríada de seguridad: confidencialidad, integridad y disponibilidad

## Principales acuerdos SLA

**RPO (Recovery Point Objective).** Es la cantidad de datos que puede perder una compañía en caso de un incidente en los sistemas de información. Por ejemplo, si hacemos un backup diario a las 23h, el RPO del escenario de backup será de 24 horas, ya que en el peor de los casos, si los sistemas fallaran a las 22:59h, la pérdida de datos sería de un día completo.

**RTO (Recovery Time Objective).** Se trata del tiempo que una compañía puede estar sin servicio en sus sistemas IT sin poner en riesgo la continuidad del negocio. Es una decisión que se debe realizar conjuntamente entre el departamento de IT y dirección general con el objetivo de encontrar una ventana de tiempo adecuada que equilibre los costes de la solución y el tiempo sin productividad (cuanto menor sea el tiempo previsto para la pérdida de productividad, mayor será el coste de la solución).

tección de datos cada vez más estrictos. Los dos acuerdos SLA más comunes en este campo incluyen los objetivos de punto de recuperación (RPO, del inglés recovery point objective) y de tiempo de recuperación (RTO, del inglés recovery time objective). Es decir, RPO se refiere a la cantidad tolerable de pérdida de datos en caso de una interrupción, mientras que RTO se refiere a la cantidad tolerable de tiempo de inactividad en caso de una interrupción. Actualmente, el RPO de mejores prácticas es de 15 minutos y el RTO es de cuatro horas. Por lo tanto, las compañías buscan herramientas de protección y recuperación de datos que puedan cumplir o superar estos SLA, incluso frente al crecimiento masivo de datos y los requisitos de recuperación más cortos.

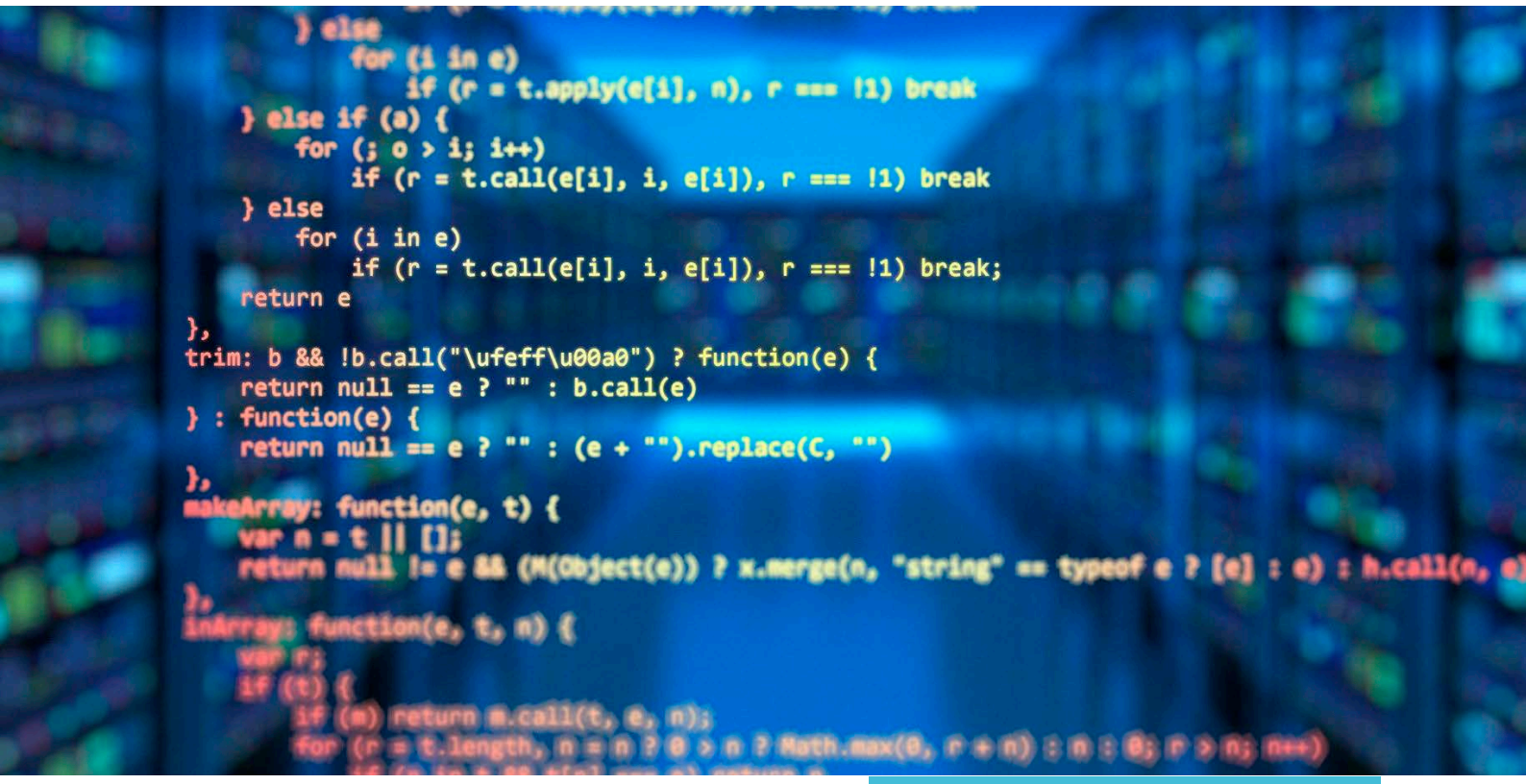
Desde otra perspectiva, la firma de análisis europea KuppingerCole en su informe Cloud Backup and Disaster Recovery de mayo de 2020

reconfirma que existe un mercado maduro con muchas soluciones de respaldo y recuperación ante desastres disponible, pero que la forma en la que se prestan los servicios TI está cambiando a medida que las organizaciones se mueven hacia un modelo de entrega híbrido. Esto está dando lugar al surgimiento de mercados emergentes para estos sistemas que protegen datos en SaaS (Software como Servicio) e IaaS (Infraestructura como Servicio), así como para soluciones que utilizan servicios en la nube para hacer backup. Algunos usuarios de servicios cloud creen que el servicio en sí proporciona toda la continuidad que necesitan. Esto puede ser cierto o no, pero está en manos del cliente el comprobar que el SLA satisface sus necesidades.

No obstante, la mayoría de los proveedores existentes están adaptando sus propuestas a este nuevo modelo, pero a la mayoría todavía le queda camino por recorrer, especialmente en el área de SaaS. Además, los nuevos actores, incluidos los propios suministradores de nube, están ofreciendo recursos que no sólo cubren su nube, sino también el almacenamiento de datos on premise o en otras nubes. Para SaaS, y especialmente para Microsoft Office 365, varios fabricantes de nuevo cuño proporcionan soluciones para que los clientes realicen copias de seguridad de los datos almacenados en los servicios SaaS que utilizan. Las capacidades esenciales que los usuarios deben buscar deben estar alineadas con sus requisitos comerciales para la continuidad del servicio. Esto incluye considerar cuán críticos para el negocio son los diversos sistemas y los datos y, por lo tanto, la protección que se necesita (objetivos de recuperación). En general, cuando una organización ya está utilizando una solución existente para la protección local, se preferirá a la adición de otras, siempre que satisfaga sus necesidades comerciales en evolución. KuppingerCole considera que agregar nuevas soluciones no solo aumenta los costes, sino que también incrementa la complejidad de uso y mantenimiento. Sin embargo, actualmente algunas de las soluciones existentes en el mercado no brindan una cobertura integral para el modelo de TI híbrido. Ante este hecho, cuando un sistema existente no cumple con los requisitos productivos de una empresa, ésta debe considerar las nuevas ofertas del mercado, aunque solo sea como una opción provisional.

> El mercado de software de protección y recuperación de datos es maduro y competitivo

Sea como sea la transformación digital no va a detenerse. Y más con la Covid-19 que ha impulsado su despegue de forma precipitada llevando



a muchas compañías a cumplir el objetivo de convertirse en una organización basada en datos, en otras palabras, que utiliza datos para crear una ventaja competitiva en el mercado. Para estas organizaciones, la disponibilidad, la precisión y la ubicación de los datos son primordiales.

Visto lo visto, la premisa no admite réplica: los datos críticos necesitan estar protegidos, ya sea en la nube, en el data center, en las aplicaciones o en el perímetro. Las compañías necesitan productos que no solo aseguren la disponibilidad de protección de datos, sino que también adopten la cloud para asegurar esos datos, tanto en las instalaciones como en cualquier repositorio en la nube.

## Capacidades críticas

Recientemente Gartner ha publicado un informe sobre las capacidades críticas que deben tenerse en cuenta a la hora de elegir una solución de backup y disaster recovery para CPD. El estudio saca a relucir hallazgos interesantes como que la protección integral contra rasomware es un aspecto clave para muchos clientes que están considerando reemplazar estos sistemas. También indica que disco a disco a cloud es la arquitectura de copia de seguridad preferida a medida que las empresas adoptan la nube pública; y que las compañías buscan alternativas que sean coherentes con capacidades on-premise o locales. Asimismo, desvela

### Diseñados para...

Las soluciones de backup y recovery para data center son productos diseñados para:

-Capturar una copia puntual (point-in-time copy) de datos en cargas de trabajo empresariales heterogéneas, independientemente de dónde se hospede. Toman instantáneas o snapshots regulares de manera que permiten que esos datos se restauren rápidamente.

- Escribir los datos en una ubicación secundaria independiente, como disco, cinta, dispositivo óptico o servicio en la nube. Es decir, para proteger los datos respaldados contra pérdidas o daños, estos deben almacenarse por separado y la nube está siendo una alternativa muy utilizada hoy en día para esta función.

- También es necesario realizar una copia de seguridad de los datos almacenados en los servicios en la nube. A menudo se asume que esto es responsabilidad del proveedor de servicios, pero las organizaciones deben verificar sus SLA. Especialmente para SaaS.

- Proporcionar la capacidad de buscar y restaurar conjuntos de datos específicos en el sistema o ubicación original o alternativo. Los servicios de recuperación de desastres brindan servicios administrados para ayudar a las organizaciones con los procesos involucrados en lo anterior.

que el backup de los datos almacenados en aplicaciones SaaS no está disponible, excepto para las plataformas más comunes, como Office 365.

De acuerdo con la consultora, en 2022, el 40% de las organizaciones sustituirán o complementarán sus aplicaciones de copia de seguridad, en comparación con lo que desplegaron en 2018. Y es que, proteger y recuperar activos empresariales independientemente del modelo de infraestructura subyacente y la ubicación es fundamental. Este requisito, tal y como sostiene la firma de análisis, se vuelve más difícil cada año debido a la creación e incorporación de más datos, aplicaciones y modelos de implementación de las mismas.

**40%**
de las organizaciones sustituirán o complementarán sus aplicaciones de backup en 2022

Para ayudar a los clientes en su elección, Gartner valora a los proveedores en función de tres casos de uso: entornos de nube física, virtual y pública. La capacidad de los fabricantes para abordar estos casos se mide evaluando cada caso con nueve capacidades críticas: soporte de aplicaciones, soporte de plataforma, rendimiento y eficiencia, seguridad y cumplimiento, experiencia del usuario, capacidad de administración, informes y análisis, integración de ecosistemas y escalabilidad.

## Elaborar un buen plan de contingencia

Para elaborar un buen de plan de contingencia en el centro de datos, lo primero que debemos hacer es identificar los activos que hay que proteger: qué equipos son más importantes y qué medidas aplicamos en cada uno para proteger la seguridad y privacidad nuestra empresa. Esta protección ha de llevarse a cabo tanto de forma activa (técnicas para evitar o reducir los riesgos que amenazan al sistema) como pasiva (herramientas que se implantan para, una vez producido el incidente, minimizar su repercusión y facilitar la recuperación).

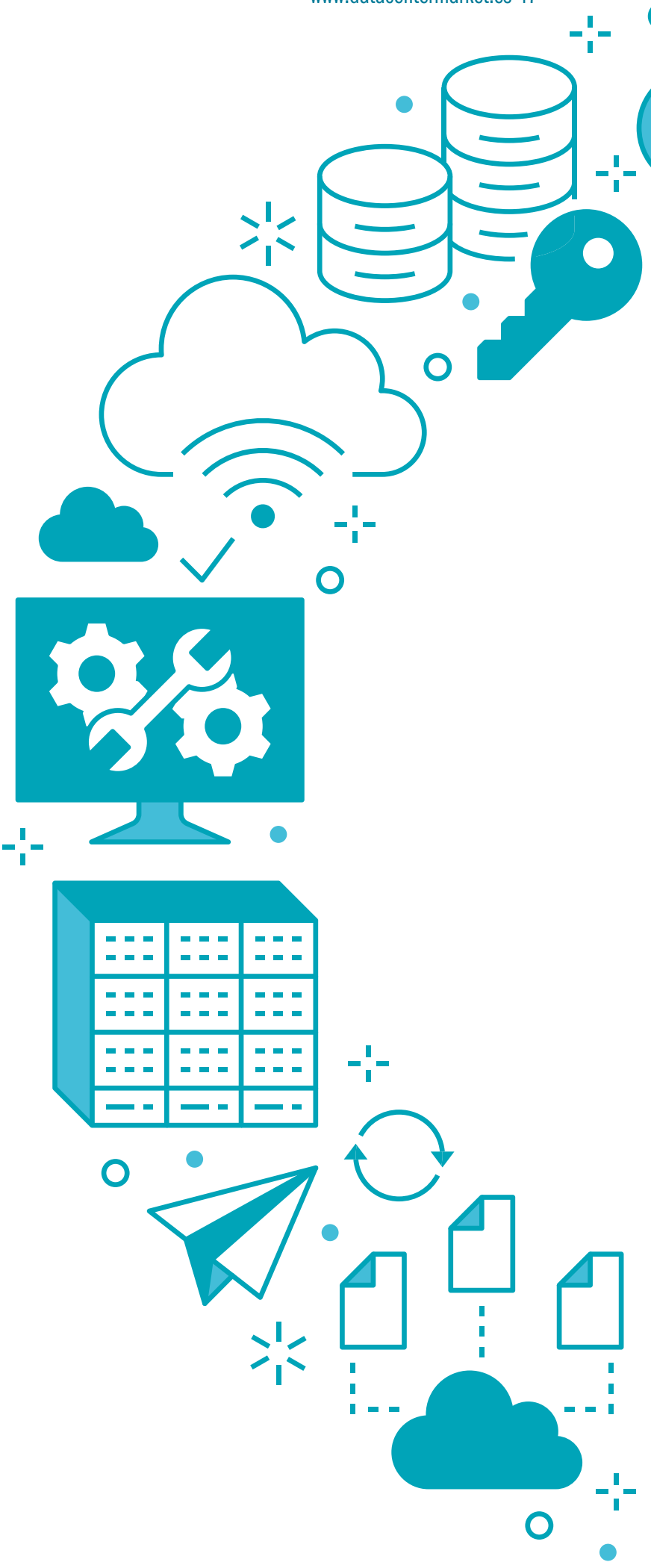
El proceso de análisis de riesgo consiste en hacer inventario y valoración de los activos, identificando y valorando las amenazas que puedan afectar a la seguridad de los mismos y los protocolos de protección existentes, así como los objetivos en la materia que ha definido la organización. Tras tener claros estos aspectos, se debe determinar sistemas que midan los riesgos y el impacto que produciría un ataque. Como precaución, se aconseja no instalar nada que no sea estrictamente necesario, por si estamos otorgando más permisos de los imprescindibles, y, por encima de todo, dar formación a los usuarios para que utilicen la seguridad y la vean como una ayuda.

## Recomendaciones

Gartner ofrece una serie de recomendaciones para los responsables de infraestructura y operaciones encargados de modernizar sus soluciones de backup y disaster recovery en los centros de datos:

- Actualice o reemplace las arquitecturas de copia de seguridad existentes para admitir soluciones en la nube y ubicaciones edge, así como nuevas cargas de trabajo en el centro de datos y aplicaciones SaaS.
- Elija un software de backup que permita la organización en niveles (tiering) y la replicación de datos en proveedores de nube pública, incluido el almacenamiento de archivos de bajo coste, como Amazon Glacier.
- Seleccione el software de copia de seguridad que ofrezca una protección de datos coherente, independientemente de si la aplicación se implementa en el centro de datos, la nube pública o la infraestructura de proveedores SaaS.
- Elija programas de backup de terceros cuando sea necesario para complementar el software de copia de seguridad empresarial y proteger las aplicaciones SaaS, como Office 365 y Salesforce.
- Haga de la protección contra ransomware y el soporte para el cumplimiento normativo una parte clave de cualquier proceso de selección y evaluación de la plataforma de copia de seguridad haciendo hincapié en estas capacidades en sus criterios de adquisición.

**Fuente:** Gartner (julio 2020).



Con todos estos aspectos sobre la mesa, una estrategia de DRP (Diasaster Recovery Plan) consiste en un centro de datos configurado activo-pasivo, es decir, toda la información está respaldada en un data center completamente configurado con la información crítica replicada en un sitio remoto. Otra opción también utilizada en el mercado es una configuración activa-activa donde toda la información de la compañía se mantiene en dos o más CPD.

Estas soluciones han de estar preparadas para cualquier tipo de incidentes como incendios, sabotajes o caída de servidores. Y desde 2020 para pandemias.