# La Alta Disponibilidad no es un lujo.
## Eliminación del tiempo de inactividad en organizaciones pequeñas y medianas

Si bien la tecnología de la información (TI) ofrece un enorme valor a las empresas pequeñas y medianas, también representa para ellas un gran punto de debilidad. Debido a la globalización de los mercados, los empleados trabajan constantemente y el negocio está permanentemente activo; toda interrupción en la disponibilidad de las aplicaciones puede conducir rápidamente a la pérdida de ingresos, productividad, valor de la marca y generar problemas regulatorios. Llevado al extremo, el tiempo de inactividad prolongado puede incluso amenazar la supervivencia de su empresa.

Entonces, ¿de qué forma debería su organización enfrentar este tipo de amenaza que pone en riesgo la existencia misma de su empresa? La triste realidad es que la mayoría de las organizaciones no la enfrenta apropiadamente.

La continuidad del negocio, que implica la planificación, la preparación y la implementación de sistemas empresariales más resistentes que prevean el tiempo de inactividad no programado, es algo que la mayoría de las organizaciones considera un problema de la TI. Esto conduce invariablemente a la implementación de una amplia gama de soluciones tácticas, pero sin una estrategia general que sirva de guía. En realidad, tal como el término lo indica, la continuidad del negocio es un tema empresarial y requiere de un enfoque empresarial para resolverlo.

**A continuación, se presenta una forma rápida de saber si su plan de continuidad del negocio actual expone a su organización:**

- Si su plan requiere de una significativa intervención manual, su organización está expuesta;
- Si su plan acepta la pérdida de datos más allá de unos pocos segundos para sistemas críticos, su organización está expuesta;
- Si su plan no puede restaurar el acceso a sistemas críticos en pocos minutos, su organización está expuesta;
- Si su plan depende de tecnología de backup y recuperación de hace 30 años, su organización está definitivamente expuesta.

Durante 30 años, la técnica de backup y recuperación ha sido la más utilizada para la protección de sistemas de TI, pero fue desarrollada en una época de menor complejidad. Hacer un backup de datos en cinta o en disco, o realizar copias instantáneas – el equivalente moderno del backup –, crea una imagen de los datos de las aplicaciones en un momento determinado en el tiempo. La recuperación de datos a partir de una copia en un momento determinado en el tiempo nunca permitirá que se recuperen los datos almacenados con posterioridad al backup más reciente. Aunque la copia sea de hace quince minutos o dos días, la recuperación desde un backup implica enfrentar la pérdida de datos. Esto puede ser aceptable para algunos sistemas. Sin embargo, para muchas de las aplicaciones empresariales más importantes, la pérdida de datos será catastrófica.

Las técnicas de backup y de recuperación fueron desarrolladas para procesos informáticos relativamente poco sofisticados, en la época en que existían períodos de tiempo programados regularmente en los que el sistema no se estaba utilizando. Las aplicaciones empresariales, siempre activas, de las que depende actualmente su organización para realizar las operaciones diarias requieren una tecnología que garantice la disponibilidad continua del sistema y que elimine la amenaza de pérdida de datos, sin tener que depender de una ventana de backup.

La tecnología moderna de alta disponibilidad (HA) envía cambios de datos y aplicaciones en forma continua a una ubicación remota. Cuando ocurre un desastre, ya sea un terremoto, un corte en el suministro eléctrico o una falla en la instalación de algún software, se activa la función de failover y el traspaso a una copia actualizada de su sistema es automático e instantáneo. HA elimina tanto el tiempo de inactividad como la pérdida de datos.

## Alta Disponibilidad para todos

Aunque durante muchos años, la HA tuvo una mala reputación, es la solución perfecta para proteger sus sistemas frente a tiempos de inactividad y pérdida de datos. Se consideraba que la tecnología de la HA era demasiado compleja y costosa para las pequeñas y medianas organizaciones. Se creía que sólo las organizaciones grandes con alto poder adquisitivo y con amplios recursos de TI podían acceder realmente a las soluciones ofrecidas por la HA. Esta crítica parecía ser real hasta hace poco tiempo.

Generalmente, la HA utiliza una combinación de tecnologías de replicación y pulsación de servidor para mantener los sistemas de TI en una ubicación remota sincronizada con las aplicaciones en el centro de datos principal. En el pasado, esto significaba disponer de redes con un gran ancho de banda entre dos ubicaciones físicas y copias redundantes de servidores, almacenamiento y redes de hardware con aplicaciones especiales y software operativo. El costo de esta redundancia siempre colocó a la tecnología de HA fuera del alcance de las organizaciones más pequeñas.

En la actualidad, las redes con gran ancha de banda a bajo costo son de uso generalizado, al punto de ser una necesidad empresarial.

Además, una gran variedad de proveedores de servicios facilitan el acceso a servidores virtuales a pedido, a muy bajo costo. Como consecuencia de estos avances en la infraestructura, la tecnología HA está disponible para más organizaciones a un costo mucho más bajo.

La caída drástica de los costos de infraestructura de HA significó un punto de inflexión para los planes de continuidad del negocio de muchas organizaciones. Abundan las soluciones de backup descoordinadas y, con frecuencia, superpuestas en el centro de datos. Si su organización siempre dependió del backup y de la recuperación para la continuidad de su negocio, probablemente notará que estas soluciones aisladas son una pesadilla al momento de realizar el mantenimiento, afectan la productividad y, lo que es peor, complican mucho la recuperación de desastres. Las soluciones que ofrece la tecnología moderna de HA aportan un enfoque universal hacia la continuidad del negocio que reduce el costo de la protección de datos, simplifica la recuperación de desastres y elimina tanto la pérdida de datos como el tiempo de inactividad.


Figura 1 –Los riegos ocultos respecto de la complejidad en el uso de soluciones de backup desactualizadas.

La HA puede ser apropiada para su negocio, pero si no se realiza un análisis detallado de los sistemas empresariales para determinar cuáles son sus necesidades de recuperación, es imposible saber qué aplicaciones se beneficiarán con esa tecnología. Lo cierto es que las restricciones que limitaban la implementación de HA fueron eliminadas y eso le permitirá ocuparse de otros problemas que pueden afectar sus planes de continuidad del negocio.

## Las 10 cosas que debe saber para mantener la continuidad del negocio

Todo el mundo habla sobre cuál es la mejor manera para recuperarse de los desastres, pero también ayuda echar un vistazo a los peligros que conlleva hacerlo mal. A continuación, incluimos una lista de las 10 cosas más importantes a tener en cuenta al momento de planificar la recuperación de desastres y la continuidad del negocio.

**1 ¡Lo importante es el negocio, no la tecnología!**

Cualquiera sea la opción (recuperación de desastres, alta disponibilidad, backup y recuperación, continuidad del negocio), el objetivo es siempre el mismo: mantener el negocio funcionando sin importar las circunstancias. Con demasiada frecuencia, las organizaciones permiten que la tecnología tome la palabra y domine la conversación. Lo que suele olvidarse, pero es esencial recordar, es que la recuperación de desastres implica satisfacer una necesidad empresarial y, por eso, debe ser impulsada por las necesidades de la empresa.

Antes de intentar resolver la forma de implementar la recuperación de desastres, es necesario tomarse el tiempo para preguntar ¿por qué? Hable con los líderes de la empresa para comprender sus prioridades. Para algunos, la prioridad será el correo electrónico; para otros, el sistema de ingreso de pedidos en línea; y para otros, Microsoft SharePoint. El problema es que no sabrá qué sistemas son los más importantes si no se lo pregunta a los usuarios empresariales. Comprender las necesidades de la organización le permitirá establecer prioridades que determinarán sus opciones respecto de la tecnología de recuperación de desastres.

**2 Puede ser una catástrofe o no**

Cuando se habla de recuperación de desastres, probablemente se piensa en huracanes, inundaciones, ataques terroristas o eventos similares, y no en una actualización de software mal realizada con un proceso inadecuado de reversión o en un error de hardware en un equipo de red crítico. Planificar para evitar el peor escenario y enfrentarse a errores triviales todos los días es lo más común. Su planificación de recuperación de desastres debe tener en cuenta cualquier eventualidad, desde lo ordinario hasta el cataclismo.

**3 ¿Cómo realizar un presupuesto sin saber el costo del tiempo de inactividad?**

A menudo, las organizaciones asignan un valor dólar a la recuperación de desastres antes de determinar el riesgo financiero del tiempo de inactividad y la pérdida de datos para el negocio. A menos que se pueda cuantificar cuánto se puede perder en una interrupción de los sistemas críticos, será difícil determinar cuánto gastar para evitar estas pérdidas. El enfoque a adoptar hacia la recuperación de desastres debe estar alineado con las necesidades de su negocio, lo que significa evaluar el costo financiero del tiempo de inactividad antes de asignar un presupuesto. No olvide incluir los gastos derivados del cumplimiento normativo en sus cálculos de tiempo de inactividad. Con frecuencia, se imponen sanciones financieras en caso de incumplimiento con obligaciones legales.

**4 Se trata de medir el riesgo**

Los acontecimientos que califican como desastres pueden variar de una organización a otra e incluso de un departamento a otro. Algunos eventos, como los terremotos, son potencialmente catastróficos y, por eso, es esencial que la organización se proteja por si ocurren. Otros eventos pueden ser comunes, como un error en el hardware de red, pero pueden tener un impacto financiero fuera de toda proporción. Al pensar en la recuperación de desastres, es necesario preguntarse: ¿de qué queremos protegernos? No debemos olvidar los lugares comunes. Las pequeñas pérdidas causadas por problemas comunes pueden acumularse rápidamente.

**5 ¿Tiene un plan?**

Si su plan de recuperación de desastres es una nota autoadhesiva en las cintas de backup que se encuentran debajo de la cama de su administrador de sistemas, hay un problema. Por extraño que suene, una cantidad sorprendente de organizaciones no tiene un plan de recuperación de desastres. Es de suma importancia que redacte un documento formal en el que se detallen todas las aplicaciones, el hardware, las instalaciones, los proveedores de servicios, el personal y las prioridades de la empresa y que, además, obtenga la aprobación del documento por parte de todas las partes interesadas en la organización. El plan debe representar a todas las áreas funcionales y servir de guía para el antes, el durante y el después de un desastre.

**6 Tenemos un plan, pero no está probado**

Tener un plan de recuperación de desastres sólo es útil si funciona. La única manera de asegurarnos de que el plan funciona es probándolo. Probar el plan en condiciones de desastre simuladas es esencial y, a su vez, presenta todo un desafío. Realizar pruebas de recuperación de desastres es costoso, y demanda tiempo y recursos de las operaciones diarias. Sin embargo, a menos que el plan haya sido completamente probado al nivel de las aplicaciones, será inevitable enfrentar problemas en caso de que ocurra un desastre real. Busque soluciones para la protección de datos que le permitan crear entornos para pruebas sin interrupciones de su plan de recuperación de desastres.

**7 ¿Quién es responsable y de qué?**

Un desastre en la realidad de su empresa puede ser caótico y generar confusión. Si el personal clave no tiene en claro cuáles son sus responsabilidades en el plan de recuperación de desastres, el proceso de recuperación será largo y estará repleto de problemas. Su plan no sólo debe indicar claramente los roles y las responsabilidades de cada una de las personas involucradas, sino que además debe definir los pasos a seguir en caso de que el personal clave no se encuentre disponible. Estas personas también deben participar en las pruebas del plan de recuperación.

**8 ¿Punto de recuperación? ¿Tiempo de recuperación?**

Es fundamental entender cuánto puede afectar el tiempo de inactividad y la pérdida de datos a cada sector de su organización. Esta información es crucial para las selecciones de tecnología de recuperación de desastres, crea las bases para la planificación de una recuperación de desastres y le permite conocer las consecuencias de la falta de recuperación de cada aplicación empresarial. Existen dos sistemas de medición para registrar la tolerancia de una aplicación al tiempo de inactividad y a la pérdida de datos: el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO). Ambos sistemas se miden en unidades de tiempo. El RPO se calcula hasta el momento en que ocurre el desastre y RTO a partir del momento en que éste ocurre.

El RPO mide la pérdida de datos. Cuanto más alto sea el RPO, mayor será la pérdida de datos que una aplicación puede soportar antes de convertirse en un problema para el negocio. Sería el momento en el tiempo hasta el que pueden recuperarse los datos exitosamente. Toda la información entre ese momento y aquel en que se produce el desastre se perderá.

El RTO mide la importancia de una aplicación para las operaciones de un negocio en curso. Cuanto más bajo sea el RTO, más rápido se deberá trabajar para lograr que la aplicación vuelva a estar en línea antes de que la organización comience a sufrir pérdidas significativas.

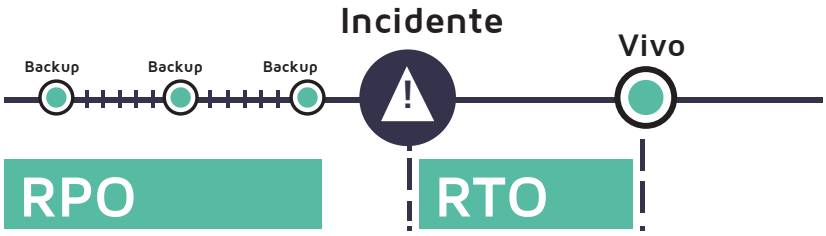


Figura 2 – Comprender la frecuencia con la que deben realizarse los backups de las diferentes aplicaciones y fuentes de datos (Objetivo de punto de recuperación – RPO) y la rapidez con la que deben recuperarse (Objetivo de tiempo de recuperación – RTO) es un componente fundamental para su plan de continuidad del negocio.

Si no conoce el RPO y el RTO de cada aplicación, está trabajando a ciegas en la recuperación de desastres. Todo lo que haga para asegurar una recuperación luego de un desastre estará basado en conjeturas. El RPO y el RTO permiten definir niveles de servicio con los que se debe cumplir.

Tecnologías como la protección continua de datos son fundamentales para asegurar que se cumplan estos objetivos.

**9 La recuperación tomará más tiempo de lo que cree**

Muchas organizaciones dejan de pensar en la recuperación de desastres cuando se retiran las cintas de backup del centro de datos. Sin embargo, es esencial comprender cuánto tiempo se necesita para recuperar los sistemas principales del negocio y cuántos datos críticos se perderán luego de un desastre. Aun si se tiene acceso a copias de backup fuera de las instalaciones, no hay garantías de que se puedan recuperar las aplicaciones a tiempo ¿Tiene acceso a equipos que pueden leer los datos? ¿Puede restaurar los datos y rehacer los sistemas de las aplicaciones a tiempo para satisfacer a los usuarios empresariales? ¿Tiene el ancho de banda necesario para recuperar datos desde un proveedor de servicios de nube? Comprender cuánto tiempo se necesita para recuperar las aplicaciones y el efecto del tiempo de inactividad en el negocio puede obligarlo a tomar decisiones diferentes sobre tecnología.

**10 Regresar al servidor primario**

Regresar al servidor primario luego de transmitir los datos al sitio de recuperación es un elemento que suele pasarse por alto en la planificación de recuperación de desastres. Es fácil saber la razón: al pensar en un posible desastre, nos enfocamos en proteger los activos de valor y no pensamos demasiado en lo que le sucede a esos activos una vez que ha ocurrido el desastre.

La capacidad de realizar un failback a los sistemas de producción es tan importante como la capacidad de realizar un failover. A menos que se lo planifique con mucho cuidado, es poco probable que un centro de datos de backup tenga la misma capacidad o rendimiento que el sitio de producción.

Sin un plan para realizar un failback, podrá implementar un failover inicial con éxito, pero luego las pérdidas se acumularán a medida que su negocio avance con dificultades durante semanas debido a un sitio de backup planificado de manera inadecuada.

## Comprensión del riesgo

Con excepción de los correos electrónicos, es casi imposible saber qué aplicaciones representan el mayor riesgo de tiempo de inactividad para el negocio sin obtener información de parte de los usuarios empresariales. Los RPO y RTO ofrecen medidas para calcular ese riesgo e indican qué aplicaciones son prioritarias para sus dirigir sus esfuerzos de recuperación de desastres.

Tanto el RPO como el RTO funcionan como un continuo. Imagine una línea de tiempo donde el evento de interrupción se encuentra en el centro. El punto RPO se encuentra antes de tal evento e indica la cantidad de pérdida de datos que una aplicación puede soportar. A medida que el punto se mueve hacia atrás en el tiempo, alejándose del evento de interrupción, la cantidad de pérdida de datos aumenta, al igual que el posible costo para la organización.

El punto RTO se encuentra en el lado opuesto al del RPO en la línea del tiempo. El RTO muestra cuánto tiempo de inactividad puede soportar una aplicación antes de que comiencen a acumularse pérdidas para el negocio. En otras palabras, con cuánta rapidez es necesario volver a hacer funcionar una aplicación luego de una interrupción.

Si se puede restablecer la información en el sistema por otros medios, perder algunos datos durante un desastre podrá ser un dolor de cabeza, pero no causará demasiados problemas. Por ejemplo, si se pierden facturas del sistema de cuentas a pagar, éstas pueden recuperarse si se solicita a los proveedores que vuelvan a presentar una solicitud de pago. Sin embargo, si los datos no pueden volver a generarse fácilmente – por ejemplo, pedidos en línea de los clientes – la pérdida de esa información puede afectar directamente los ingresos, la productividad de los usuarios, la reputación de la empresa y su marca, como así también el cumplimiento regulatorio.

De igual manera, el impacto en la organización por tiempo de inactividad respecto de los sistemas de negocios no críticos – por ejemplo, los informes mensuales de una aplicación de análisis de negocio– es distinto al impacto que tienen los sistemas que involucran operaciones diarias, como una aplicación de punto de venta (POS). El RTO mide el impacto en el negocio que genera el tiempo de inactividad de una aplicación y ayuda a determinar las herramientas de recuperación de desastres que deben implementarse para esa aplicación. Realizar backups en forma periódica puede ser aceptable para una aplicación de análisis de negocio, pero como es probable que un sistema POS sea relevante para el negocio, éste exigirá una solución de alta disponibilidad.

La diferencia entre las mediciones RPO y RTO y los resultados reales de las pruebas periódicas de recuperación de desastres muestran si existe una brecha en la disponibilidad de la aplicación. Debemos tener en cuenta que una brecha de disponibilidad no siempre indica que se esté adoptando un enfoque incorrecto para la continuidad del negocio. Con frecuencia, las organizaciones cuentan con un rango amplio de tecnologías de recuperación de desastres de diferentes proveedores, muchas de las cuales se superponen, se duplican y complican la recuperación. Las pruebas pueden eliminar problemas e incongruencias en las tecnologías de continuidad del negocio existentes y también pueden destacar aquellos sectores donde la consolidación basada en un único enfoque o en un único proveedor de soluciones puede mejorar el RTO.

## ¿Qué características tiene una HA exitosa?

Las características de una alta disponibilidad exitosa no tienen ningún secreto: inexistencia de tiempo de inactividad e inexistencia de pérdida de datos para las aplicaciones. Pero, ¿es viable para las pequeñas y medianas organizaciones?

La tecnología HA ya no involucra un enfoque complejo y esotérico para la continuidad del negocio como lo hizo alguna vez. Las grandes empresas han estado utilizando durante años las técnicas de alta disponibilidad para proteger las aplicaciones más importantes de sus negocios. La tecnología ha sido probada y es ampliamente aceptada como una herramienta estándar para evitar desastres. Es simple, repetible, medible y automatizada. Tecnologías como la protección continua de datos, la replicación, el failover y el failback automatizados son fundamentales.

La maduración de los productos de HA permitió que su precio sea accesible para las pequeñas y medianas empresas. Este hecho, junto con la reducción de los costos de infraestructura– banda ancha, virtualización de servidores, proveedores de servicios múltiples – y una mejora considerable en la facilidad de uso hacen que la HA sea una alternativa de continuidad del negocio real para todo tipo de organización.

El tiempo de inactividad y la pérdida de datos son hechos que pueden suceder en la vida de un negocio que depende de la TI. En las primeras etapas del desarrollo de software y de los ciclos de vida del producto, debe considerarse la compensación de este riesgo con la tecnología adecuada. Comprender el nivel de protección exigido por cada aplicación permite asignar los recursos apropiados. Cuando una aplicación está en la etapa de uso de producción por parte de los usuarios empresariales, el RPO y el RTO ya debieran haberse identificado con claridad, y las soluciones de continuidad del negocio apropiadas ya debieran haberse implementado para facilitar una recuperación garantizada en caso de que ocurra una interrupción.

Todo enfoque de continuidad de negocio que no pueda confirmar la inexistencia de tiempo de inactividad ni de pérdida de datos no posee alta disponibilidad. Una amplia variedad de soluciones se encuentran disponibles y prometen mejorar la recuperación de desastres, pero si no eliminan la exposición de su organización, no son HA.

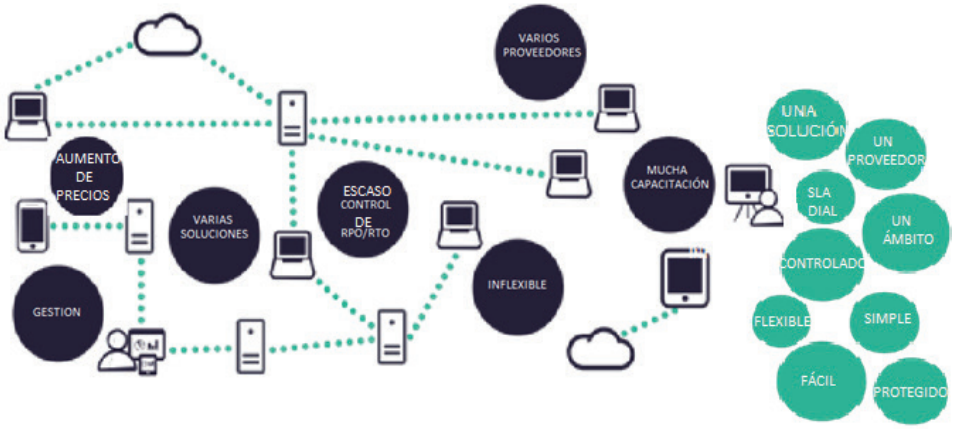


Figura 3 – Una solución de continuidad del negocio unificada.

## Acerca de Arcserve® Unified Data Protection

Arcserve asegura la inexistencia de tiempo de inactividad a organizaciones en todo el mundo desde hace más de 20 años. Actualmente, Arcserve® Unified Data Protection (UDP) ofrece un servicio integral para la protección de datos y las necesidades de alta disponibilidad. Con un control centralizado, Arcserve® UDP unifica la protección de backup, copias instantáneas, replicación y deduplicación para aplicaciones virtuales, físicas, en las instalaciones y en la nube. Arcserve® UDP Assured RecoveryTM ofrece un proceso de prueba completa y en tiempo real de preparación ante desastres para una validación sin interrupciones de los planes de continuidad del negocio. Para obtener más información sobre Arcserve® Unified Data Protection (UDP) y acceder a una prueba gratuita de 30 días, visite http://arcserve.com/availability

Para más información sobre Arcserve UDP, **visite arcserve.com**

Copyright © 2015 Arcserve (USA), LLC, sus afiliadas y subsidiarias. Todos los derechos reservados. Todas las marcas registradas, nombres comerciales, marcas de servicio y logos mencionados aquí pertenecen a sus respectivas compañías. Este documento es sólo a título informativo. Arcserve no asume ninguna responsabilidad por la exactitud o exhaustividad de la información. En la medida permitida por la ley aplicable, Arcserve proporciona este documento "en el estado en que se encuentra" sin garantía de ningún tipo, incluida, sin limitación, cualquier garantía implícita de comerciabilidad, adaptación para un propósito particular o no contravención. En ningún caso Arcserve será responsable por cualquier pérdida o daño, directo o indirecto o, derivado de la utilización de este documento, incluido, sin limitación, lucro cesante, interrupción de negocios, renombre de marca o pérdida de datos, incluso si Arcserve ha sido expresamente notificada de la posibilidad de tales daños.