CONTINUIDAD DEL NEGOCIO DENTRO DEL PRESUPUESTO

7 preguntas clave que su empresa debe hacerse sobre cómo superar la pérdida de datos y el tiempo de inactividad

Debido a la gran complejidad de los entornos informáticos actuales, podemos decir que hemos ingresado a una nueva era. Sin embargo, es probable que los planes de continuidad del negocio de su empresa hayan sido implementados en una época en que el camino hacia la continuidad del negocio y la recuperación de desastres (BCDR) era mucho más claro y simple. Esto amenaza a su empresa ya que, si utiliza un modelo viejo que asigna un precio fijo a la recuperación, es posible que su empresa esté destinada al fracaso. Las preguntas a continuación pueden ayudar a identificar rápidamente si su empresa está en riesgo: un primer paso esencial para tomar las medidas necesarias.

1 ¿Será víctima de los predadores del ransomware y su extorsión por USD 11 500 billones?

Se espera que los ataques de ransomware se disparen en los próximos 12 a 14 meses, por lo que es probable que muchas empresas los sufran.

14 SEGUNDOS
SERÁ LA FRECUENCIA DE ATAQUES DE RANSOMWARE HACIA FINES DE 2019

CONSEJO: **¡La recuperación a un punto en el tiempo (o rebobinado de datos) puede evitar esta amenaza por completo!**

2 En caso de ciberataque, ¿quedará a merced de los clientes y colegas más críticos?

Con demasiada frecuencia, el daño de los ciberataques no se limita a los sistemas de TI. Sus colegas pueden usarlo de chivo expiatorio o los clientes enojados pueden hablar muy mal de su empresa. Además, como buen profesional de TI que conoce el campo de batalla, es posible que hasta usted mismo cuestione su desempeño.

CONSEJO: **Defienda sus aplicaciones y sistemas con soluciones comprobadas en décadas, no días. Al ser la empresa proveedora de BCDR más experimentada del mundo, nunca enfrentamos un desafío de protección de datos que fuera demasiado difícil de resolver.**

3 ¿Un desastre natural será lo que destruirá su plan de DR?

Más de la mitad de las empresas no cuentan con un plan de recuperación de desastres. Entre las que sí tienen uno, menos del 15 % confían en el proceso de recuperación.

50% DE LAS EMPRESAS NO TIENEN UN PLAN DE RECUPERACIÓN DE DESASTRES

CONSEJO: **Evite todas las consecuencias de los desastres causados por el tiempo de inactividad con soluciones en la nube que ofrecen RTO y RPO rentables de menos de un minuto.**

4 ¿Cuál es la forma más segura de tirar por la borda sus SLA? (Una pista: piense en la tecnología obsoleta).

La tecnología obsoleta agrega un grado importante de imprevisibilidad a su operación. Cuando esa tecnología falla o no funciona adecuadamente, es posible que sus SLA alcancen un punto de quiebre y no pueda cumplirlos.

CONSEJO: **Transforme su infraestructura de TI de forma segura con protección de datos en múltiples nubes y entre nubes.**

5 ¿Puede un error humano causar un desastre de pérdida de datos que hunda su costo total de propiedad (TCO)?

Al ser una de las principales causas del tiempo de inactividad no planificado, el error humano representa un desafío cada vez más costoso: las cifras estimativas van

DESDE **USD 100,000**

A MAS DE **USD 300,000** POR HORA.

CONSEJO: **Agregue el costo del tiempo y soporte necesarios para recuperarse de un error humano y verá que los costos son aún más alarmantes. Recupere desde y hacia cualquier ubicación, cumpla todos los RTO/RPO y ahorre hasta un 50 % de tiempo sin múltiples proveedores, herramientas e interfaces de usuarios.**

6 ¿Es posible que algo tan simple como un corte de energía pueda llevar sus obligaciones de cumplimiento al lado oscuro?

Los cortes de energía son una amenaza cada vez mayor para las empresas actuales; en promedio, se prolongan el doble de tiempo respecto del año pasado. No importa cuál sea la causa, pueden hacer mucho más que paralizar su organización

81 MINUTOS
ES LA DURACIÓN PROMEDIO DE UN CORTE DE ENERGÍA

A menudo, su empresa no puede cumplir con normas gubernamentales e industriales que regulan muchas industrias.

CONSEJO: **Evite multas elevadas y posibles repercusiones entre sus clientes con backup externo de sus datos en la nube. ¡La recuperación de desastres como servicio (DRaaS) es una forma efectiva de alcanzar la recuperación de desastres sin el costo de infraestructuras y sitios secundarios!**

7 ¿Cómo puede una falla destrozar sus planes de asignación de TI sin previo aviso?

Las cosas fallan. Si bien es tentador culpar a los sistemas obsoletos de TI por las fallas, la realidad es que cualquier elemento de su infraestructura de TI puede fallar, sin importar hace cuánto tiempo está funcionando.

CONSEJO: **Asegúrese de que su solución de protección de datos pueda defenderlo frente al tiempo de inactividad y la pérdida de datos en toda su infraestructura de TI de varias generaciones, desde hardware no basado en 86x al uso de múltiples nubes. Así, estará protegido independientemente de qué sistema falle.**

MÁS INFORMACIÓN

Obtenga "Continuidad del negocio dentro del presupuesto: guía interna" en **arcserve.com/la**

arcserve®