arcserve®

eBook

MUY RESILIENTES O MUY EXPUESTAS:

La disponibilidad continua en industrias de alto riesgo

arcserve®

SIEMPRE DISPONIBLE. CONTINUA. TODAS LAS INDUSTRIAS NECESITAN QUE LOS SISTEMAS Y APLICACIONES CRÍTICOS ESTÉN DISPONIBLES SIN INTERRUPCIONES.

Hoy en día, las empresas están globalizadas y tienen operaciones ininterrumpidas que sencillamente no pueden dejar de funcionar. Cuentan con aplicaciones y sistemas que almacenan software propietario sujeto a derechos de propiedad intelectual, mantienen en funcionamiento sitios de comercio electrónico y sistemas aeroportuarios, además de herramientas de logística y de planificación de recursos empresariales (ERP), y hacen posible las transacciones financieras. En estos casos, un período de inactividad no planificado, aunque se trate de minutos, podría afectar de manera irreparable los ingresos y la productividad. Honestamente, ya no alcanza con una solución de backup y recuperación.

Para proteger estos sistemas y aplicaciones, las organizaciones deben cambiar su enfoque y pasar del backup a la protección de datos continua. Deben dejar atrás los objetivos de tiempo y punto de recuperación (RTO/RPO) para nunca más necesitar recuperarse.

Entonces, ¿cómo sería alcanzar una verdadera continuidad del negocio?

¿Qué sucedería si los sistemas y las aplicaciones nunca fallaran? ¿Qué sucedería si pudiera eliminar los RPO/RTO por completo de sus sistemas, para olvidarse de una vez por todas de la recuperación?

Veamos una serie de industrias donde podremos identificar la necesidad de contar con una empresa siempre disponible, el escenario ideal donde las operaciones nunca se interrumpen y los sistemas críticos nunca fallan.

arcserve®

PROTEGER LAS TECNOLOGÍAS DE IoT CONTRA CIBERATAQUES EN LA INDUSTRIA DE LA FABRICACIÓN

Las organizaciones de fabricación rara vez descansan, ya que suelen operar en producción las 24 horas del día, los siete días de la semana y los 365 días del año. Esto requiere una infraestructura de TI con una alta capacidad de respuesta: muchas de ellas buscan mejorar el crecimiento y la eficiencia operativa adoptando la Internet de las Cosas (IoT) para automatizar y administrar en forma remota más herramientas y sistemas en el proceso de producción. Sin embargo, a medida que se acelera el gasto en IoT y la adopción pasa de proyectos piloto a la implementación a escala completa, surgen riesgos mayores.

En el sector de fabricación, la automatización de las líneas de producción por medio de la IoT ofrece beneficios tangibles, como una mayor producción a un costo reducido.

Pero también las vuelve susceptibles, ya que crea vulnerabilidades que los atacantes cibernéticos pueden aprovechar. Los ciberataques paralizan infraestructuras y frenan las operaciones de los fabricantes, y así causan pérdidas irreparables en sus finanzas y su productividad.

VEAMOS UN EJEMPLO:

CUANDO NORSK HYDRO, UNO DE LOS PRINCIPALES FABRICANTES DE ALUMINIO A NIVEL MUNDIAL, FUE ATACADO POR EL RANSOMWARE LOCKERGOGA, LA RECUPERACIÓN LE COSTÓ $41 MILLONES, PRINCIPALMENTE POR EL TIEMPO DE PRODUCCIÓN PERDIDO[1]. EN POCAS PALABRAS, LOS FABRICANTES NO PUEDEN PERMITIRSE QUE LOS SISTEMAS LOCALES QUEDEN INACTIVOS DEBIDO A CIBERATAQUES, ERRORES HUMANOS O DESASTRES NATURALES.

En una industria donde muchas empresas fabrican productos sin parar, los ingresos y la prestación de servicios dependen de la disponibilidad de sistemas críticos. Y en las complejas infraestructuras de TI de hoy en día, la interconexión de sistemas individuales implica que la falla de uno puede afectar a todos. Los ejecutivos de TI en el sector de fabricación deben concentrarse en brindar operaciones confiables manteniendo sistemas y aplicaciones clave en funcionamiento ante un error humano o un desastre natural. Las soluciones de alta disponibilidad local y/o remota son la clave para preservar las operaciones empresariales y ofrecer ventajas competitivas manteniendo una disponibilidad ininterrumpida de los sistemas críticos.

arcserve®

MANTENER UNA OPERACIÓN CONTINUA EN LA INDUSTRIA DE VIAJES Y TRANSPORTE

Todos los días, más de 2,6 millones de pasajeros transitan por los aeropuertos de EE. UU. y 3.480 aviones despegan por hora[(2)]. Cualquier problema técnico en cualquier sistema, con en la emisión de pasajes, el manejo de equipaje y las operaciones de vuelo, puede provocar un efecto dominó y atascar todo el proceso.

Las empresas de la industria de viajes y transporte generan datos constantemente. No solo las aerolíneas monitorean cada movimiento de sus pasajeros: las empresas ferroviarias deben monitorear sus cronogramas, el contenido de las cargas y el mantenimiento de trenes y vías, y las autoridades portuarias deben contar con datos en tiempo real sobre los embarques, los activos y el personal. Mantener estos sistemas en funcionamiento sin interrupciones es crucial para las operaciones, y constituye la principal prioridad para los ejecutivos de esta industria junto con la protección de datos críticos de individuos y empresas.

La complejidad de las organizaciones de viajes y transporte pone en relieve otras vulnerabilidades en el desarrollo de planes de continuidad del negocio. Por ejemplo, un desastre natural, como un huracán, puede afectar los cronogramas y sistemas. Además, la forma en la que una organización se recupera de un desastre muchas veces puede influir sobre la percepción que tiene el cliente de la empresa en el largo plazo.

Los aviones no paran de volar, los trenes cumplen sus cronogramas y los buques cargueros continúan navegando: la industria de viajes y transporte está siempre en movimiento. Lo mismo se aplica a los sistemas críticos para el negocio que la respaldan. Para estas organizaciones, la continuidad del negocio implica satisfacer las expectativas de los consumidores sobre la disponibilidad, mediante el funcionamiento sin problemas de las operaciones en cada punto de su viaje.

arcserve®

PROTECCIÓN DE DATOS CONTINUA PARA LAS CONSTANTES TRANSACCIONES DE LA INDUSTRIA DE SERVICIOS FINANCIEROS

En la economía global actual, estar «siempre disponible» significa realizar transacciones sin parar, y la industria bancaria y de servicios financieros siente esa presión todos los días.

La transformación digital para la industria de servicios financieros exige modernizar y automatizar las infraestructuras de TI, sin dejar de garantizar la más alta calidad de experiencia del cliente a través de la disponibilidad continua de las aplicaciones bancarias.

Como en cualquier industria, las violaciones de seguridad de los datos pueden resultar devastadoras. La sufrida por Equifax en 2017 puso en riesgo los datos personales de 145 millones de personas en los Estados Unidos. Se expuso información como fechas de nacimiento, licencias de conducir y números de seguridad social[(3)]. Los eventos de este tipo afectan los ingresos y la reputación de las organizaciones, y hacen que los clientes pierdan la confianza en su capacidad de mantener la seguridad de sus datos.
Como parte del camino hacia la transformación digital, la incorporación de un plan de continuidad del negocio que esté a la altura de la innovación y las expectativas del cliente será fundamental para las organizaciones de servicios financieros. Con tecnologías más nuevas, como las criptomonedas y la inteligencia artificial (IA), la protección de datos continua con mejoras en monitoreo y alertas es fundamental para las instituciones bancarias y financieras, a medida que surgen nuevas formas de ataques de hackers.

arcserve®

MEJORAR LA EXPERIENCIA DEL USUARIO EN APLICACIONES CON ALTA DISPONIBILIDAD

En la economía de las experiencias de hoy en día, el consumidor es la base de todo. Y este espera acceder a lo que desee cuando lo desee. Si no puede solicitar una entrega directa al auto en su tienda habitual o compartir sus selfies con el filtro que desea, se frustrará. Además, su voz es más fuerte si se manifiesta en línea: las redes sociales son el lugar perfecto para compartir todas sus experiencias (en gran parte negativas), ya sea con tuits, reseñas y publicaciones en Reddit.

La cantidad de datos en el sector de tecnología puede resultar abrumadora. Solo para hacerse una idea: se envían 6.000 tuits por segundo[4], se suben 300 horas de video a YouTube por minuto[5], y se realizan 3.500 millones de búsquedas en Google por día[6]. Si esas aplicaciones no están disponibles, los usuarios pierden la cabeza.

La columna vertebral de la experiencia del usuario hoy depende de la disponibilidad de los datos, no únicamente de brindar productos de calidad. Esas experiencias, impulsadas en gran parte por las empresas de tecnología y sus aplicaciones, pueden ser tan valiosas (si no más) que los productos tangibles. Es vital garantizar que su negocio funcione sin interrupciones. Esta es la razón por la cual evitar cualquier tiempo de inactividad con protección de datos continua es un elemento crítico para la estrategia de TI de toda empresa de tecnología.

arcserve®

LA SEGURIDAD DE LOS DATOS, UNA DE LAS PRINCIPALES INQUIETUDES DE LOS PROFESIONALES DE TI PARA LA SALUD

Los datos son activos clave en cualquier organización de salud. La información y los antecedentes de un paciente pueden determinar el tipo de tratamiento y aportar datos importantes para lograr un diagnóstico. Además, según una encuesta de Health Data Management (HDM), la seguridad sigue siendo la principal preocupación para los profesionales de TI para la salud, que están redoblando esfuerzos para proteger la información sobre la salud de sus pacientes y defenderse ante ciberataques. En esta encuesta, orientada a los ejecutivos de TI para la salud, el 93% afirmó que la protección de la información sobre salud y la seguridad de los datos eran muy importantes o extremadamente importantes.[7]

Asimismo, como las leyes de privacidad y las normas de cumplimiento son cada vez más estrictas, proteger los datos de los pacientes no es un buen gesto, sino una obligación. La innovación en la salud moderna implica contar con las tecnologías más recientes para la atención al paciente y también para la protección de datos.

En lo que respecta a garantizar la continuidad de las operaciones, los profesionales de TI para la salud dependen de soluciones que mantengan los consultorios, las salas de emergencia o los hospitales funcionando en todo momento. Es sencillo: si se cae un sistema o una aplicación de salud, puede llegar a ser cuestión de vida o muerte.

Los pacientes son la prioridad número uno de los profesionales de la salud. Por eso, es inaceptable dejar de atenderlos ante un desastre natural o provocado por el hombre. Gracias a la tecnología de alta disponibilidad, las organizaciones de salud pueden confiar en que estarán "siempre disponibles" para prestar servicios a sus pacientes cuando ellos lo necesiten.

arcserve®

ALCANZAR UNA VERDADERA CONTINUIDAD DEL NEGOCIO CON SOLUCIONES DE REPLICACIÓN Y ALTA DISPONIBILIDAD

Sea cual sea la industria, toda empresa tiene sistemas y aplicaciones que deben mantenerse en funcionamiento. Para protegerlos, los equipos de TI suelen usar tecnología diseñada para minimizar el tiempo de inactividad y la pérdida de datos ante una interrupción inevitable.
Arcserve Replication and High Availability (RHA) justamente logra eso: garantizar la continuidad del negocio con tecnologías comprobadas que tienen un propósito en común, mantener su negocio operativo y en funcionamiento. Gracias a la tecnología de replicación asincrónica, Arcserve RHA es la única solución que brinda alta disponibilidad, conmutación por error automática respaldada por tecnología de latido y protección de datos continua para aplicaciones y sistemas on-premise, remotos y en la nube. Alcance una verdadera disponibilidad de sistemas y aplicaciones:

Replique datos en tiempo real y pase de objetivos de tiempo y punto de recuperación (RTO/RPO) a una protección continua.

La tecnología basada en registros replica cambios a nivel de bytes, en archivos, aplicaciones y sistemas completos, para que pueda retornar a cualquier punto en el tiempo y restaurar todo a como estaba antes de la falla.

Brinde una conmutación por error automática, impulsada por la tecnología de latido, para eliminar demoras entre las tareas de detección y mitigación.

Compatibilidad con servidores físicos y virtuales y entornos de nube con cifrado y pruebas no disruptivas para aumentar el costo total de propiedad (TCO).

Cuando se produce una interrupción, cada momento cuenta. Alcance un tiempo de actividad ininterrumpido y gane en tranquilidad con **Arcserve RHA**.

Referencias

1. How to neutralize the impact of ransomware, **https://www.manufacturing.net/article/2019/05/how-neutralize-impact-ransomware**
2. Air traffic by the numbers, **https://www.faa.gov/air_traffic/by_the_numbers/**
3. Top Bank Tech Trends for 2018, **https://www.americanbanker.com/slideshow/top-bank-tech-trends-for-2018**
4. Internet Live Stats, **https://www.internetlivestats.com/twitter-statistics/**
5. YouTube by the Numbers: Stats, Demographics & Fun Facts, **https://www.omnicoreagency.com/youtube-statistics/**
6. Internet Live Stats, **https://www.internetlivestats.com/google-search-statistics/**
7. Providers and Progress: Baby Steps for Healthcare's Top Challenges, Health Data Management, accessed 5/13/2019.

Descubra mucho más en **www.arcserve.com/la**