WHITE PAPER

TRANSFORMAR LA ATENCIÓN MÉDICA

Salvar vidas con cero tiempo de inactividad: 6 pautas para conseguir disponibilidad

EL SECTOR SANITARIO REPRESENTA UNA PARTE IMPORTANTE DE LA ECONOMÍA: . Este sector se encuentra bajo la presión constante de una amplia gama de condicionantes (gobierno, trabajadores, consumidores y socios), para transformar los procesos basados en documentos impresos, reducir los costes y proteger los datos de los pacientes. El objetivo de convertir todo a formato digital requiere de una disponibilidad siempre activa que satisfaga las expectativas del negocio, la administración y los consumidores, y a su vez mantenga la información a buen recaudo.

Todos los sectores están experimentando los inconvenientes y tribulaciones que suponen la transformación digital, pero en el caso particular del sector de la sanidad, es mucho lo que está en juego. Proveedores, pagadores, pacientes y funcionarios del gobierno tienen todos ellos sus propias prioridades. Los equipos de TI de la atención sanitaria se ven desbordados por la demanda de los usuarios de un acceso 24/7 desde cualquier tipo de dispositivo, una tolerancia cero para los tiempos de inactividad y una gestión de los datos en entornos híbridos que abarque los recursos de las instalaciones locales, la nube privada y la nube pública.

A su vez, la rápida innovación que se está produciendo en las tecnologías de diagnóstico y tratamiento está incrementando significativamente los volúmenes de datos, lo que conlleva a una demanda de accesibilidad por parte de profesionales y consumidores que esperan un acceso rápido a esta información. Mientras tanto, el incremento en las normativas gubernamentales, imponen cargas adicionales y sanciones potenciales por violaciones de estas normativas.

A pesar de los avances producidos en la atención sanitaria, la gestión de toda esta información parece estar quedando por debajo de las expectativas. Los analistas McKinsey & Co. observaron a mediados de 2014 que las organizaciones del sector sanitario tenían serias dificultades para gestionar la infinidad de grupos de interés, regulaciones y cuestiones de seguridad necesarias para desarrollar un sistema de TI integrado para el sector sanitario, acumulando un retraso importante con respecto a otros sectores a la hora de conseguir la digitalización completa.

La tormenta perfecta

En un entorno en el que los datos deben conservarse en algunos casos hasta incluso 100 años, y sin tolerancia para tiempos de inactividad, el desafío para la TI es muy pronunciado.

Si a esto añadimos los problemas derivados del cibercrimen, nos encontramos antes una "tormenta perfecta" virtual de proporciones catastróficas.

Durante el pasado año, sin embargo, las instituciones de la salud se han convertido en el objetivo de un nuevo peligro: el ransomware. Este software malicioso está diseñado para impedir el acceso a los sistemas informáticos hasta que la organización pague una suma económica para desbloquear los datos.

LOS EQUIPOS DE TI DE LA ATENCIÓN SANITARIA RECIBEN POR TODOS LADOS LA DEMANDA DE ACCESO 24/7 PARA CADA USUARIO Y DESDE CUALQUIER TIPO DE DISPOSITIVO, TOLERANCIA CERO PARA LOS TIEMPOS DE INACTIVIDAD Y UNA GESTIÓN DE LOS DATOS EN ENTORNOS HÍBRIDOS QUE ABARQUE LOS RECURSOS DE LAS INSTALACIONES LOCALES, LA NUBE PRIVADA Y LA NUBE PÚBLICA.

En enero de 2016, los hackers bloquearon los sistemas informáticos de un hospital de Los Angeles y el personal se vio forzado a trabajar durante más de una semana "con bolígrafos y papel para conservar los registros". Finalmente la institución pagó 17 000 $ en bitcoins como rescate. Pocos meses después, lo que pareció ser un ataque de ransomware forzó la parada de los equipos informáticos y el correo en el sistema de salud del área de Washington, D.C. incluyendo a 10 hospitales y 250 centros ambulatorios, al cuidado de cientos de miles de pacientes.

Accenture predice que entre 2015 y 2019, 25 millones de pacientes sufrirán el robo de sus datos de pago y/o información médica de los registros digitales de sus proveedores de atención sanitaria. . En el caso de la atención médica, no solo la pérdida de ingresos es lo que corre peligro: Una pérdida de datos o un retraso en el acceso a los mismos puede resultar en los casos más extremos en una pérdida de vidas.

El cibercrimen es solamente una parte de la historia. A medida que el sector sanitario ha ido adoptando los registros médicos electrónicos (EHR por sus siglas en inglés), el acceso 24/7 se ha convertido en un asunto crítico. Según el informe de Department of Health and Human Services inspector en EE.UU. sobre una encuesta realizada a 400 hospitales en 2015, "Más de la mitad de los hospitales informaron de una interrupción no planificada en el acceso a los EHR, y cerca de un cuarto de estos experimentaron como resultado problemas y retrasos en el cuidado de los pacientes". Como señala el informe, "La regla de seguridad requiere que cada entidad cubierta posea un plan de contingencia para responder a eventos que puedan interrumpir los sistemas que contienen la información electrónica sanitaria."

Otros países se enfrentan a problemas regulatorios de igual índole. El hospital Centre for Addiction and Mental Health (CAMH) es el más grande de Canadá dedicado a la salud mental y las adicciones. "Durante una auditoría tenemos que demostrar que podemos volver a prestar servicios de TI en un periodo de tiempo razonable tras un desastre" comenta Alan Tang, jefe de equipo del grupo de gestión de información del portal y Web del CAMH. Además, comenta, "Para cumplir nuestro compromiso de atención centrada en el paciente, nuestros médicos y personal necesitan acceso a las aplicaciones y los datos, las 24 horas, los 7 días de la semana ".

La firma de investigaciones de mercado IDC estima que el coste medio de una hora de interrupción para organizaciones grandes de entre 1000 y 4999 empleados es de aproximadamente 225 000 dólares. "En consecuencia, las empresas no pueden tolerar los mismos niveles de interrupciones planeadas y no planeadas que aceptaban antes de comenzar su viaje hacia la transformación digital, y para muchas empresas, la ventana de tiempo de inactividad está cercana a cero", afirma la analista Carla Arend de IDC.

El impacto de la TI en la atención sanitaria

Las demandas técnicas para el sector sanitario se están redefiniendo rápidamente, y la gestión de los datos continúa siendo la principal prioridad en las instalaciones de la atención médica. La demanda creciente de los clientes, y el incremento en la complejidad de las infraestructuras de TI, hacen que la salvaguarda adecuada de la creciente cantidad de información sensible que deben almacenar y proteger, se convierta en todo un desafío para estas instalaciones.

Al igual que ocurre en otras industrias, el sector de la salud se enfrenta a un crecimiento explosivo en la movilidad y analítica, así como al impacto aún desconocido de los dispositivos conectados al Internet de las Cosas (IoT). Según un informe, existen 165 000 apps móviles orientadas a la salud, y el 10 % de ellas están vinculadas directamente a un dispositivo o sensor. Es más, en 2014 había en marcha más de 300 estudios clínicos para examinar el efecto de las apps móviles en la salud del paciente.

Luego están las aplicaciones de seguimiento de forma física y salud que están acumulando información. . . Se espera que los hospitales adopten rápidamente el Internet de las Cosas para capturar y compartir datos de las aplicaciones, que van desde equipos de monitorización en las salas de los hospitales, a la monitorización remota de los pacientes en casa.

Como resultado, el cuidado de la salud es una de las fuentes de información digital de más rápido crecimiento, con un aumento estimado anual del 48 % según un estudio de IDC y EMC.

LAS FILTRACIONES O VIOLACIONES EN LA SEGURIDAD DE LOS DATOS SE ESTIMA QUE CUESTAN AL SECTOR DE LA SANIDAD 6200 MILLONES DE DÓLARES ANUALES, Y LA MITAD DE DICHAS VIOLACIONES DE DATOS SON PRODUCTO DE ACTIVIDADES CRIMINALES.

— El Instituto Ponemon

El acceso, la retención y la protección de datos son vitales para organizaciones que ya se encuentran sobrecargadas con los enormes volúmenes de datos. Esos volúmenes seguirán creciendo, especialmente a la luz de los archivos de imágenes digitalizadas. "La suma total de los datos de imagen asociados a los pacientes a lo largo de muchos años puede alcanzar el nivel de petabytes," según un informe de la Society for Imaging Informatics in Medicine. Y esos archivos de imagen pueden estar sujetos a distintos requisitos de retención, que van desde la disponibilidad inmediata al archivado.

Por si las aplicaciones médicas y científicas no fueran de por sí suficiente, los proveedores de la atención médica y los pagadores también deben gestionar datos de tarjetas de crédito, que están sujetos a los estándares de cumplimiento de la industria de las tarjetas de pago (Payment Card Industry o PCI) para la gestión de la información sensible de las tarjetas. Los estándares de seguridad de datos PCI (PCI DSS) tienen estrictos requisitos para el almacenamiento y protección de la información.

Estado de preparación

La transformación digital está impulsando estrategias de negocio que dependen de la facilidad de disponibilidad de los datos. Pero una reveladora encuesta mundial llevada a cabo por *MIT Sloan Management Review* y Deloitte encontró que aunque cerca del 90 % de los directores y ejecutivos creen que sus negocios sufrirán algún tipo de interrupción como consecuencia de la evolución digital, solo el 44 % afirma que sus organizaciones se están preparando de forma adecuada para enfrentarse a los problemas que puedan producirse.

La tecnología de TI está generando una gran cantidad de aplicaciones y datos críticos que deben protegerse y mantenerse disponibles en todo momento. En 2013, se estimó que el 90% de todos los datos del mundo habían sido generados en los dos años anteriores, y los del sector de la atención sanitaria representaban una parte importante de ellos. Un informe apunta que "el tamaño y complejidad de la información de la investigación social, biomédica y de la salud recopilada por científicos en el mundo académico, de la administración, agencias de seguros y la industria se duplica en el transcurso de 12 o 14 meses."

A medida que las organizaciones incrementan su nivel de digitalización, estas se ven más expuestas a posibles interrupciones y mayores tiempos de inactividad causados por ataques criminales, errores humanos, fallos informáticos o fenómenos naturales.

Por ejemplo, Catalent Pharma Solutions sufrió tres desastres naturales en solo un año. Primero un terremoto seguido por un tsunami causó una inundación que produjo un corte de larga duración del suministro energético en sus operaciones en Japón. Posteriormente, un incendio dañó los servidores del sitio en Reino Unido donde máquinas virtuales (VMs) críticas para el negocio, ejecutaban aplicaciones de inventario, producción y envío.

Cualquiera de estas catástrofes podrían haber producido importantes trastornos para el negocio para la empresa con sede en New Jersey, pero una estrategia de disaster recovery (DR) con backup y replicación site-to-site ayudó a la compañía a recuperar sus servicios de TI rápidamente y mantener la disponibilidad de sus datos más críticos. "Esta iniciativa de recuperación ante desastres funcionó tan bien que estamos planificando la ampliación de la replicación a nivel mundial. Nuestros sitios en Norteamérica, Europa y Asia-Pacífico replicarán las VMs dentro de sus respectivas regiones", comenta Dave Clark, ingeniero senior de infraestructuras de Catalent.

Directrices para mantener la disponibilidad de datos de la salud

Cuestiones con los datos de pacientes El coste de cualquier brecha en los datos sanitarios no solo se mide en pérdidas de tiempo y dinero, sino en algunos casos en vidas humanas. El sector de la sanidad se encuentra bajo el escrutinio constante de los consumidores, instituciones reguladoras y proveedores de seguros.

Los nuevos tratamientos y el coste creciente de la atención a los pacientes, no las inversiones directas en TI, son los factores principales del incremento del gasto de la atención médica. Sin embargo, la demanda técnica del sector sanitario se está redefiniendo rápidamente y la gestión de datos continúa siendo la principal prioridad de las infraestructuras dedicadas al cuidado de la salud.

Sencillamente no se aceptan paradas y tiempos de inactividad en las organizaciones actuales de la atención sanitaria. Cuando los datos no se encuentran disponibles, las organizaciones tienen que ser capaces de recuperarlos al instante para mantener el cumplimiento, asegurar la productividad, satisfacer la demanda de los consumidores y lo más importante, salvar vidas.

"SI BIEN LA DISPONIBILIDAD SE HA ESTABLECIDO COMO UN FACTOR CLAVE PARA EL ÉXITO DE LA EMPRESA HOY EN DÍA, ESTA NO ES FÁCIL DE LOGRAR, Y LA MAYORÍA DE EMPRESAS ESTÁN LLEVANDO A CABO INVERSIONES IMPORTANTES EN TI SIN ALCANZAR LOS OBJETIVOS DE DISPONIBILIDAD ESPERADOS"

—Carla Arend, analista de IDC

"Si falla alguno de nuestros sistemas críticos, nuestro negocio se detiene. Además, debemos ser capaces de demostrar que podemos restaurar los backups rápidamente para cumplir con la HIPAA y otros requisitos regulatorios", comenta Nick Vega, especialista de sistemas de red en Roswell Park Cancer Institute, una de las primeras instalaciones hospitalarias dedicadas al estudio e investigación del cáncer en Fase 1 del país.

Pero, según comenta Arend de IDC, "si bien la disponibilidad se ha establecido hoy en día como un factor clave para el éxito del negocio, esta no es fácil de lograr y la mayoría de empresas están llevando a cabo importantes inversiones en TI sin alcanzar los objetivos de disponibilidad esperados".

Los exigentes estándares de retención, la demanda creciente de los clientes y el incremento en la complejidad de las infraestructuras de TI, hacen que la salvaguarda adecuada de la creciente cantidad de información sensible que deben proteger y almacenar, se convierta en todo un desafío para las organizaciones de la atención sanitaria.

Los responsables de TI en estos entornos deben evaluar las opciones existentes en materia de soluciones de disponibilidad de datos usando estos factores críticos como guía:

LA PRIVACIDAD DE LOS DATOS DEBE MANTENERSE: El cumplimiento con las regulaciones del sector sanitario y las auditorías dictan los estándares para la privacidad de la información electrónica confidencial de la salud. El cifrado integrado end-to-end es crucial para proteger los datos de los pacientes y empleados, al igual que la seguridad de acceso a los datos y los controles de delegación.

ES FUNDAMENTAL CONTAR CON UN BACKUP RÁPIDO Y UNA DISPONIBILIDAD SIEMPRE ACTIVA: Con una tolerancia cero para las interrupciones de los sistemas, las organizaciones deben proporcionar una disponibilidad garantizada para todos los sistemas, lo que requiere medidas suficientes para asegurar la recuperación de alta velocidad de los datos en cuestión de minutos.

UN PLAN DE DISASTER RECOVERY ES CLAVE: Las organizaciones de la atención sanitaria se enfrentan a algunos de los estándares más exigentes en materia de DR, que implican la realización de pruebas de DR anuales, lo que resulta caro y requiere mucho trabajo. La simplificación y automatización de las soluciones de backup y recuperación que incorporen DR integrado puede ahorrar tiempo y dinero.

LOGRAR FLEXIBILIDAD A TRAVÉS DE LA CONECTIVIDAD CON LA NUBE A medida que las empresas complementan y reemplazan las infraestructuras tradicionales con servicios de nube pública y privada, estas pueden ahorrar tiempo, mitigar riesgos y reducir de forma significativa los costes operativos y de inversión.

ALMACENAR Y MANTENER LOS DATOS DE FORMA RENTABLE: Las organizaciones que se enfrentan a diversos requisitos para la retención de datos a largo plazo, necesitan usar dispositivos de cinta o deduplicación para llevar a cabo el archivado y gestión rentable de los cada vez mayores volúmenes de datos.

DEBEN CONSIDERARSE SERVICIOS SATÉLITE O REMOTOS: La centralización de las instalaciones de oficinas remotas y sucursales es fundamental para mejorar el backup y la recuperación. Esta estrategia puede consumir un importante ancho de banda y recursos, pero el consumo de ancho de banda WAN puede reducirse manteniendo las actividades de backup y restauración localmente en los sitios remotos.

Garantizar la disponibilidad

Veeam® reconoce los nuevos desafíos a los que se enfrentan las empresas de todo el mundo para hacer realidad el concepto Always-On Enterprise™ (negocio siempre activo), un negocio que debe operar en modo 24/7. La empresa está trabajando con las organizaciones de la atención sanitaria para ayudarles a cumplir objetivos de tiempo y punto de recuperación (RTPO™) de menos de 15 minutos para TODAS las aplicaciones y los datos a través de un nuevo tipo de solución que ofrece recuperación de alta velocidad, capacidad de recuperación verificada, evita la pérdida de datos, aprovechamiento de datos y visibilidad completa.

Veeam Availability Suite™ incluye Veeam Backup & Replication™, que utiliza tecnologías de almacenamiento (storage), nube (cloud) y virtualización que habilitan el centro de datos moderno para ayudar a las organizaciones a ahorrar tiempo, mitigar riesgos, y reducir de forma drástica los costes operativos y de inversión, a la vez que se apoyan los objetivos empresariales actuales y futuros de los clientes de Veeam.

Para obtener más información visite www.veeam.com.

VEEAM

IDG