9 MANERAS DE EVITAR LOS **PROBLEMAS COMUNES DE RED** ANTES DE QUE ESTOS SUCEDAN

En la actual cultura de trabajo móvil y de continuidad de horario, los profesionales de TI tienen el reto de la administración de infraestructuras de TI cada vez más complejas, tratando de anticiparse a la detección oportuna de situaciones antes de que éstas se conviertan en problemas. Solamente un minuto de inactividad de una red de TI puede costarle US$ 5,600 en promedio a una organización y puede afectar significativamente su productividad.

546859/ES/20150415

Aquí hay **9 consejos** para evitar los problemas comunes en la red y continuamente asegurar la salud de sus sistemas:

01 **Identifique los problemas de hardware antes de estos que ocurran** – Manténgase delante de los problemas potenciales del hardware, revisando regularmente su infraestructura de TI para determinar la temperatura estándar de sus servidores, conocer cuando los discos duros están llegando a su máxima capacidad, ver si la memoria se está agotando, o cuando sea el momento adecuado para aumentar el ancho de banda de sus conexiones a Internet. El mantenerse al corriente de las condiciones de la red, le permitirá planificar mejoras de hardware antes de que éstas se vuelvan críticas.

02 **Automatice sus procesos de reinicio** – Cuando un servicio de Windows falla o cuando su servidor se cuelga, el método común para la recuperación del mismo es reiniciar manualmente el servidor. Para evitar la interrupción prolongada de los servicios, automatice este proceso y así su sistema reiniciará el servidor o el servicio después de haber estado fuera de operación por un período de tiempo determinado.

03 **Mantenga un ojo en los saboteadores** – El software de antivirus es importante, pero no debe ser la única arma para proteger su organización contra las amenazas de seguridad. Monitorice el tráfico inusual de su red, los picos de utilización de CPU o los abruptos intentos de conexiones - todos ellos son indicadores relacionados con la presencia de un malware. Sea capaz de reconocer, en etapas tempranas, los comportamientos maliciosos en su red, lo que le permitirá limitar el impacto de cualquier ataque general.

04 **Verifique las condiciones ambientales** – Las altas temperaturas, humedad, fugas de agua, etc. son algunas condiciones potencialmente dañinas que ponen en riesgo la continuidad de operación de su centro de datos. Sea proactivo en la monitorización de los equipos de enfriamiento y de otras condiciones ambientales las cuales aseguran que sus dispositivos se encuentran seguros y de esta forma evitar mayores problemas.

05 **Asegúrese que su sitio web tenga un adecuado rendimiento** – El desempeño del sitio web es decisivo para cualquier compañía. Retrasos en las descargas de las páginas web o en las respuestas de las acciones que son solicitadas, pueden producir pérdidas en ventas o de posibles prospectos de negocios. Monitorice y pruebe regularmente su sitio web para asegurarse que posee una alta disponibilidad y un aceptable desempeño en el servicio.

06 **Las máquinas virtuales deben de estar fuera del lugar, pero no fuera de nuestro control** – La virtualización proporciona gran flexibilidad pero también puede ser poco confiable. Es importante darle un adecuado seguimiento y monitorizar sus máquinas virtuales para conocer en todo momento: cómo están siendo utilizadas, el uso del CPU, de la memoria, así mismo la velocidad de la red a fin de evitar problemas en su desempeño.

07 **Encuentre la raíz de los problemas de las bases de datos** – El bajo desempeño de las bases de datos puede ser el resultado de una serie de aspectos, incluyendo problemas de hardware, interferencia de aplicaciones de terceros o corrupción dentro de la base de datos. Con el fin de solucionar los problemas de manera eficiente y optimizar el rendimiento, usted necesita primero identificar las causas. El mantenimiento regular de su base de datos ayudará a evitar los problemas.

08 **Evite la mala calidad de sonido y de video** – Los frecuentes problemas de calidad del sonido de voz sobre IP (VoIP) y cortes en la transferencia de video pueden ser frustrantes para los usuarios. Estas interrupciones son típicamente resultado de un retraso o pérdida en la transmisión de paquetes de User Datagram Protocol (UDP). Con el fin de evitar estos problemas de calidad, asegúrese de que su red es capaz de manejar el incremento de tráfico UDP que su servicio requiere.

09 **Organice sus necesidades de respaldos de seguridad** El mantenimiento y la garantía de las copias de seguridad - sistema operativo, imagen completa, virtualización, SQL, Exchange, etc. - funcionando exitosamente pueden ser un desafío y usualmente son tareas no de alta prioridad, que son fundamentales para salvaguardar y mantener un registro de sus datos, en caso de presentarse un fallo en la red o en el sistema. Para ahorrar tiempo, utilice un servicio de monitorización que analice continuamente el estado de todas las copias de respaldo y envíe notificaciones cuando se presenten problemas dentro de su ejecución.

¡Monitorización unificada para el rescate!

Una solución de monitorización unificada le ofrece una única plataforma desde la cual podrá ver, registrar y administrar estos tipos de situaciones de red antes de que ellos se conviertan en problemas. Para consejos adicionales sobre la administración proactiva de desafíos comunes de red y conocer cómo PRTG Network Monitor puede ayudarle, descargue aquí una visión general de **„11 Problemas Diarios que PRTG Network Monitor le Ayuda a Resolver.“**

PAESSLER PRTG NETWORK MONITOR

www.paessler.es/problemas-diarios-en-la-red

www.paessler.es