# Si el trabajo remoto llegó para quedarse, las empresas tienen más trabajo por hacer

La modernización de TI ha sido durante mucho tiempo un tema de discusión para los gobiernos, y la respuesta rápida y eficiente a los nuevos requisitos de trabajo remoto es una prueba de que esos esfuerzos han valido la pena. Muchas empresas han estado sentando las bases para capacidades de trabajo remoto generalizadas durante años: adoptando soluciones en la nube, implementando plataformas comerciales escalables, implementando herramientas de colaboración y agilizando el intercambio de datos.

Si bien el enfoque dedicado a la modernización ha preparado a las empresas para este cambio rápido, es esencial considerar los nuevos desafíos logísticos y las preocupaciones de seguridad que se han introducido.

Las redes privadas virtuales de las que dependen habitualmente los empleados remotos para acceder a la red del gobierno funcionan las 24 horas, los 7 días de la semana, lo que dificulta mantenerlas actualizadas con las últimas actualizaciones y parches de seguridad. Para agravar el problema, muchas VPN no fueron diseñadas para esta escala de trabajo remoto y están causando ralentizaciones o acceso limitado.

Las nuevas y amplificadas preocupaciones de seguridad que han surgido tampoco pueden pasarse por alto. Con los empleados fuera de la oficina, y lejos de la seguridad de la red gubernamental, los ciberdelincuentes están desarrollando sus tácticas. Las empresas deben elevar sus estrategias de protección de datos.

- **Los riesgos son muy altos con los ataques de ransomware.** Los ataques de ransomware han aumentado en todas las instituciones gubernamentales, educativas y proveedores de atención médica, pero el clima actual está poniendo el sistema de atención médica en un riesgo aún mayor a medida que la misión se vuelve más crítica que nunca. A menudo, las organizaciones confían en centros de datos y sistemas de almacenamiento de décadas que se implementaron antes del surgimiento del ransomware, lo que dificulta o imposibilita que las empresas recuperen y usen los datos recuperados.
- **Una gran cantidad de nuevos puntos de acceso.** Históricamente, las empresas tenían estrictas políticas de traer su propio dispositivo. La pandemia ha forzado un cambio, lo que llevó a las empresas a flexibilizar las restricciones para permitir que más empleados continúen el trabajo de misión crítica de forma remota. Si bien es esencial, este cambio expone un nuevo conjunto de problemas de seguridad en un momento en que los profesionales de TI y seguridad del gobierno ya están trabajando para obtener la máxima capacidad.
- **Nuevos riesgos de comunicación.** Las plataformas de vídeo han reemplazado la sala de conferencias, y tanto los piratas informáticos como los profesionales de seguridad están prestando atención. Al mismo tiempo que algunas plataformas informan más del 50% de crecimiento en el lapso de unas pocas semanas, el FBI emite advertencias sobre la

seguridad de estos métodos de comunicación recientemente populares.

**¿Qué sigue para las empresas?**

El aumento del trabajo remoto no retrocederá cuando la pandemia disminuya, y muchos de estos cambios serán permanentes. Las empresas se han adaptado rápida y exitosamente a la nueva demanda de trabajo remoto, pero deben asegurarse de tener la infraestructura adecuada, una que cree una base sólida y segura para el trabajo remoto expandido permanentemente. Necesitan una experiencia de datos moderna que les permita usar más de sus datos, al tiempo que reduce la complejidad y el gasto de administrar la infraestructura detrás de ellos.

Una infraestructura de escritorio virtual ofrece administración simplificada, seguridad mejorada, mejor rendimiento y costos reducidos. Un VDI también permite que las empresas se vuelvan mucho más ágiles, obteniendo la capacidad de dirigirse a los usuarios que trabajan tanto en casa como en la oficina con requisitos informáticos muy diversos. Las nuevas capacidades de entrega permiten a los equipos de TI centralizar completamente la administración de la VDI, creando un nuevo paradigma de seguridad donde no se almacena nada en el punto final.

En un entorno de problemas de seguridad elevados, las características de protección de datos, como la copia de seguridad y la restauración, son más críticas que nunca. Estas características facilitan la recuperación en caso de pérdida de datos o falla del sistema. Los datos no se pueden bloquear en una cinta, en un almacén o en un disco de rotación lenta cuando es probable que las empresas necesiten funciones de copia de seguridad y restauración rápida. Ahora es el momento de aprovechar ampliamente la protección de datos.

Establecer y mantener un entorno preparado para el trabajo remoto es fundamental para que las empresas avancen. El éxito comienza con la base correcta: una experiencia de datos moderna que se define por las interfaces de programación de aplicaciones y presenta herramientas de administración comunes y sencillas y análisis proactivos que son accionables a escala. También debe ser transparente, abarcando cualquier protocolo, cualquier nivel de servicio y múltiples nubes en un solo entorno. Por último, debe ser sostenible y de actualización automática.