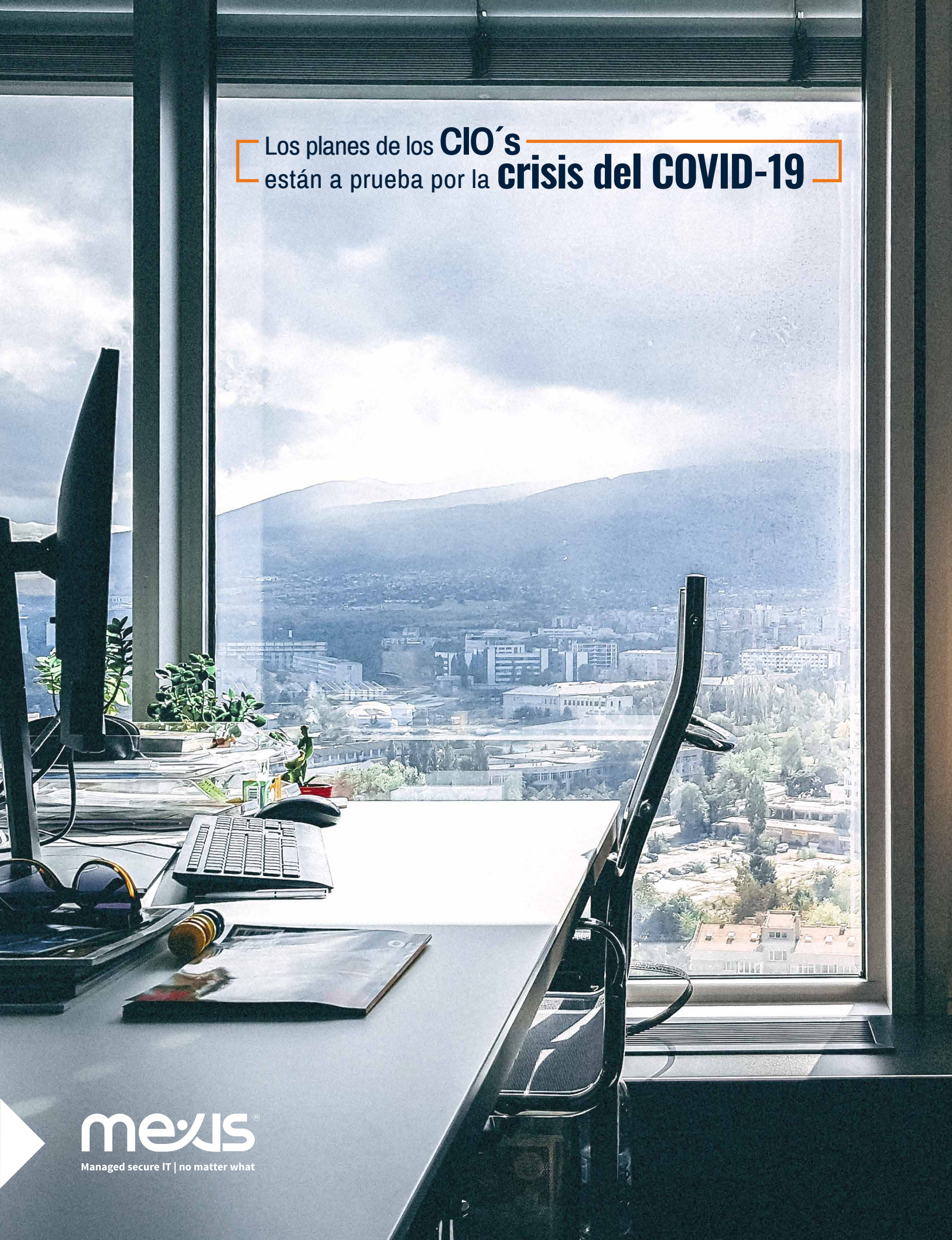
Los planes de los CIO´s están a prueba por la crisis del COVID-19



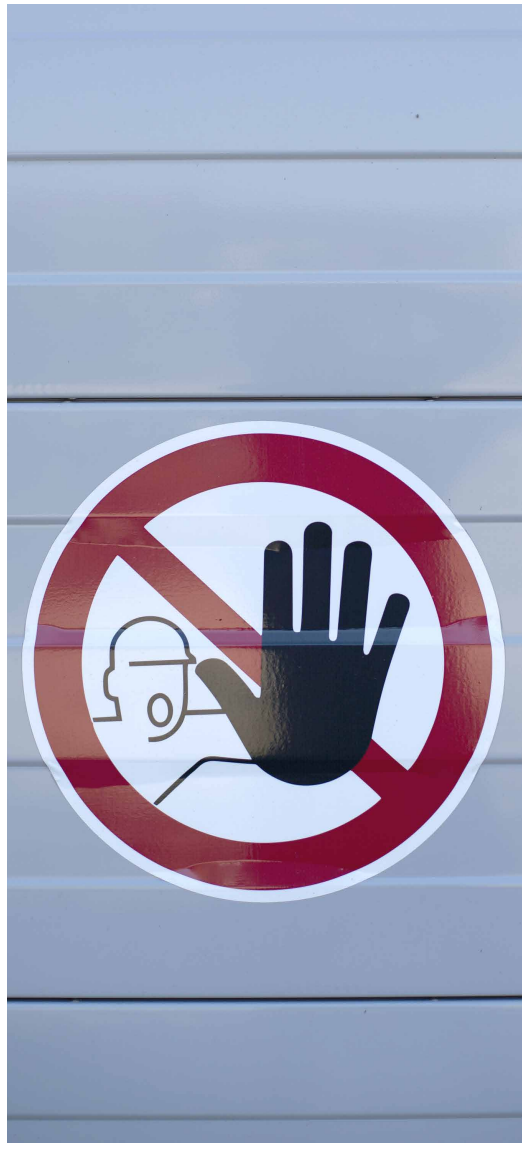
Managed secure IT | no matter what

Los planes de los CIO´s están a prueba por la crisis del COVID-19

A medida que se propaga la pandemia de Coronavirus, el CIO tiene la oportunidad perfecta para repasar la planificación de la continuidad del negocio mientras elaboran estrategias para su respuesta.

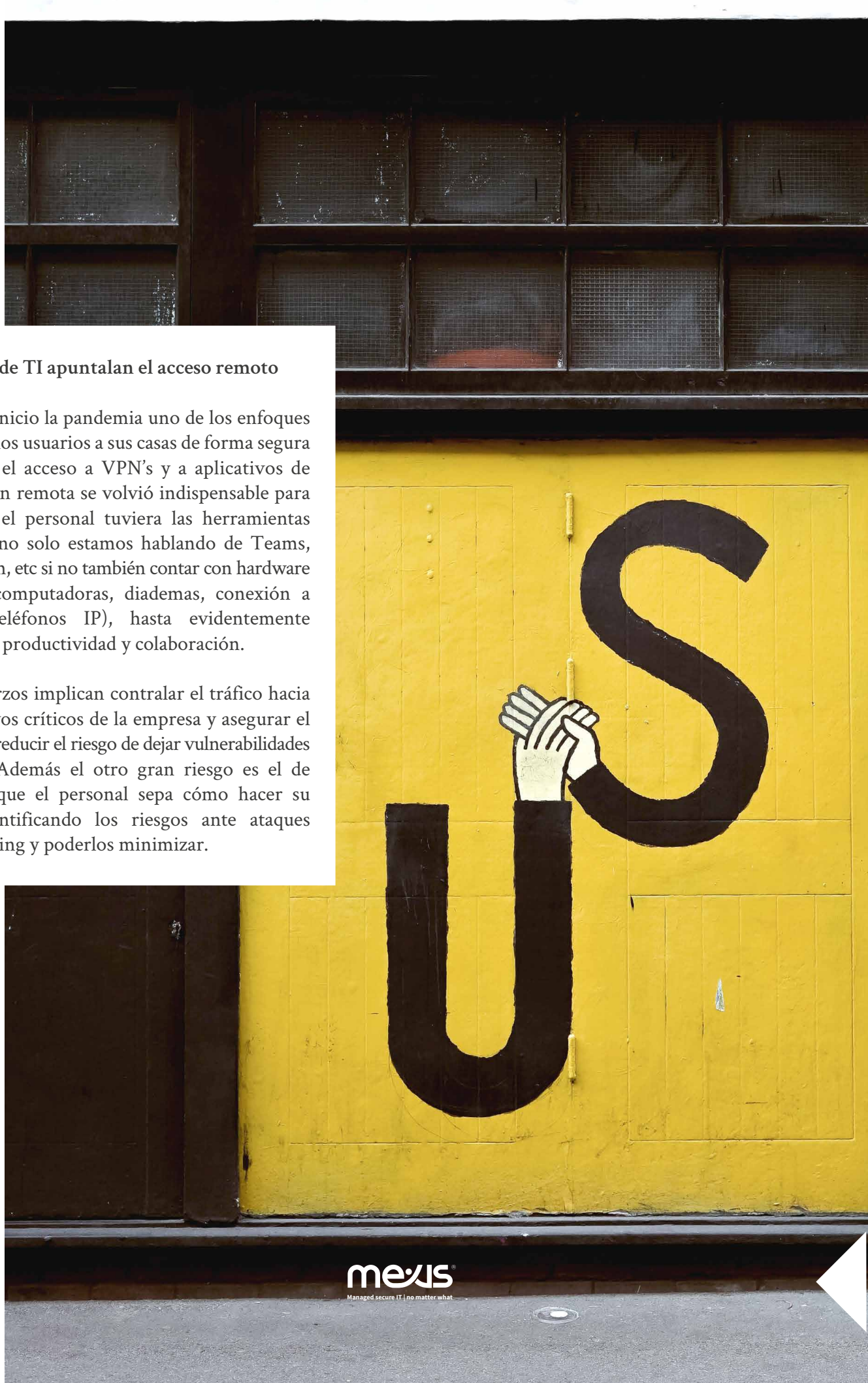
A medida que el coronavirus COVID-19 hace temblar a las industrias, es más importante que nunca que los líderes de TI se aseguren de que los empleados tengan las herramientas que necesitan para trabajar de forma remota y segura.

> "Cuando los brotes afectan los canales y las operaciones tradicionales, el valor de los canales, productos y operaciones digitales se vuelve inmediatamente obvio", según la analista de Gartner Sandy Shen. "Esta es una llamada de atención a las organizaciones que se centran en las necesidades operativas diarias en el gasto de invertir en negocios digitales y resiliencia a largo plazo ".



Para la mayoría de las organizaciones, eso significa un impulso en la planificación de la continuidad del negocio (BC). Desde la ejecución de "simulacros de incendio" asociados con amenazas cibernéticas hasta la puesta en marcha de centros de datos adicionales y la comunicación sobre los desafíos del trabajo remoto, los líderes de TI se enfrentan al COVID-19.

Aquí, los líderes de TI comparten sus planes para reforzar BC, proporcionando plantillas para que sus pares mantengan a las empresas funcionando sin problemas en preparación para los desastres, sin importar la forma que tomen.



Los líderes de TI apuntalan el acceso remoto

Desde que inicio la pandemia uno de los enfoques fue llevar a los usuarios a sus casas de forma segura por lo que el acceso a VPN's y a aplicativos de colaboración remota se volvió indispensable para lograr que el personal tuviera las herramientas adecuadas, no solo estamos hablando de Teams, Skype, Zoom, etc si no también contar con hardware (incluidas computadoras, diademas, conexión a internet, teléfonos IP), hasta evidentemente software de productividad y colaboración.

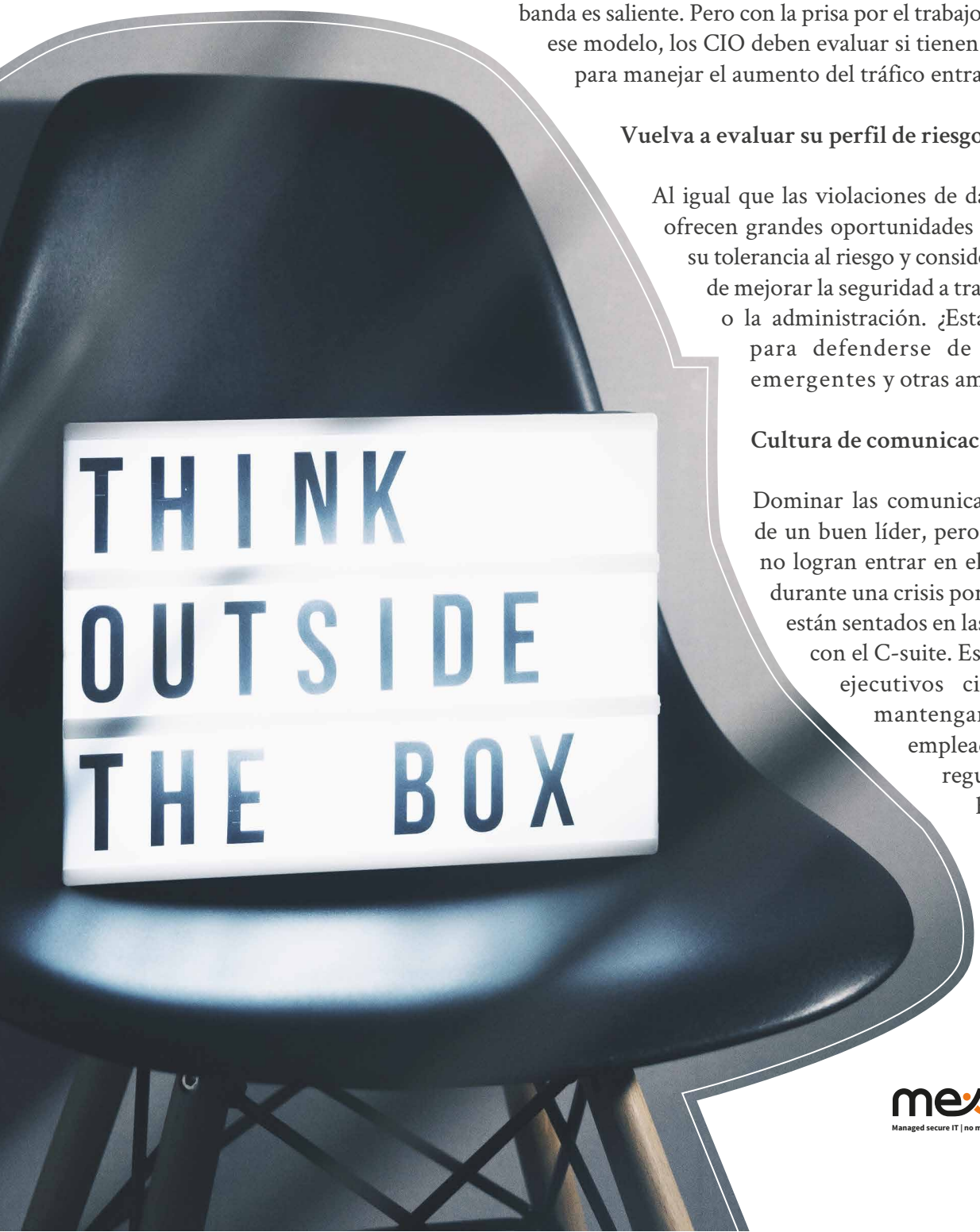
Estos esfuerzos implican contralar el tráfico hacia los aplicativos críticos de la empresa y asegurar el medio para reducir el riesgo de dejar vulnerabilidades expuestas. Además el otro gran riesgo es el de garantizar que el personal sepa cómo hacer su trabajo identificando los riesgos ante ataques como phishing y poderlos minimizar.

Aplicaciones y datos

Los CIO deben asegurarse de que los sistemas de TI correctos estén completamente operativos. ¿La mejor aplicación? Email. "Sin correo electrónico, los lugares se detienen" menciona especialista. Es de vital importancia garantizar que los empleados puedan acceder a cualquier software de primer nivel que necesiten para hacer su trabajo en casa.

Hardware y ancho de banda

Muchas personas en sectores de trabajo sin conocimiento tienen computadoras de escritorio, por lo que los CIO deben considerar si permiten que ese personal use sus dispositivos domésticos en lugar de sus PC de trabajo. Y deben asegurarse de tener suficiente ancho de banda para manejar el tráfico externo. Para la mayoría de las corporaciones, el 70 por ciento del requisito de ancho de banda es saliente. Pero con la prisa por el trabajo remoto cambiando ese modelo, los CIO deben evaluar si tienen la capacidad de red para manejar el aumento del tráfico entrante.



Vuelva a evaluar su perfil de riesgo

Al igual que las violaciones de datos, las pandemias ofrecen grandes oportunidades para que TI evalúe su tolerancia al riesgo y considere formas creativas de mejorar la seguridad a través de la tecnología o la administración. ¿Está equipado con TI para defenderse de los ciberataques emergentes y otras amenazas?

Cultura de comunicación

Dominar las comunicaciones es la marca de un buen líder, pero muchos ejecutivos no logran entrar en el personal de rango durante una crisis porque olvidan que no están sentados en las mismas reuniones con el C-suite. Es imperativo que los ejecutivos cierren el ciclo y mantengan a todos los empleados actualizados regularmente cada día hábil.

Fuente de información:
www.cio.com