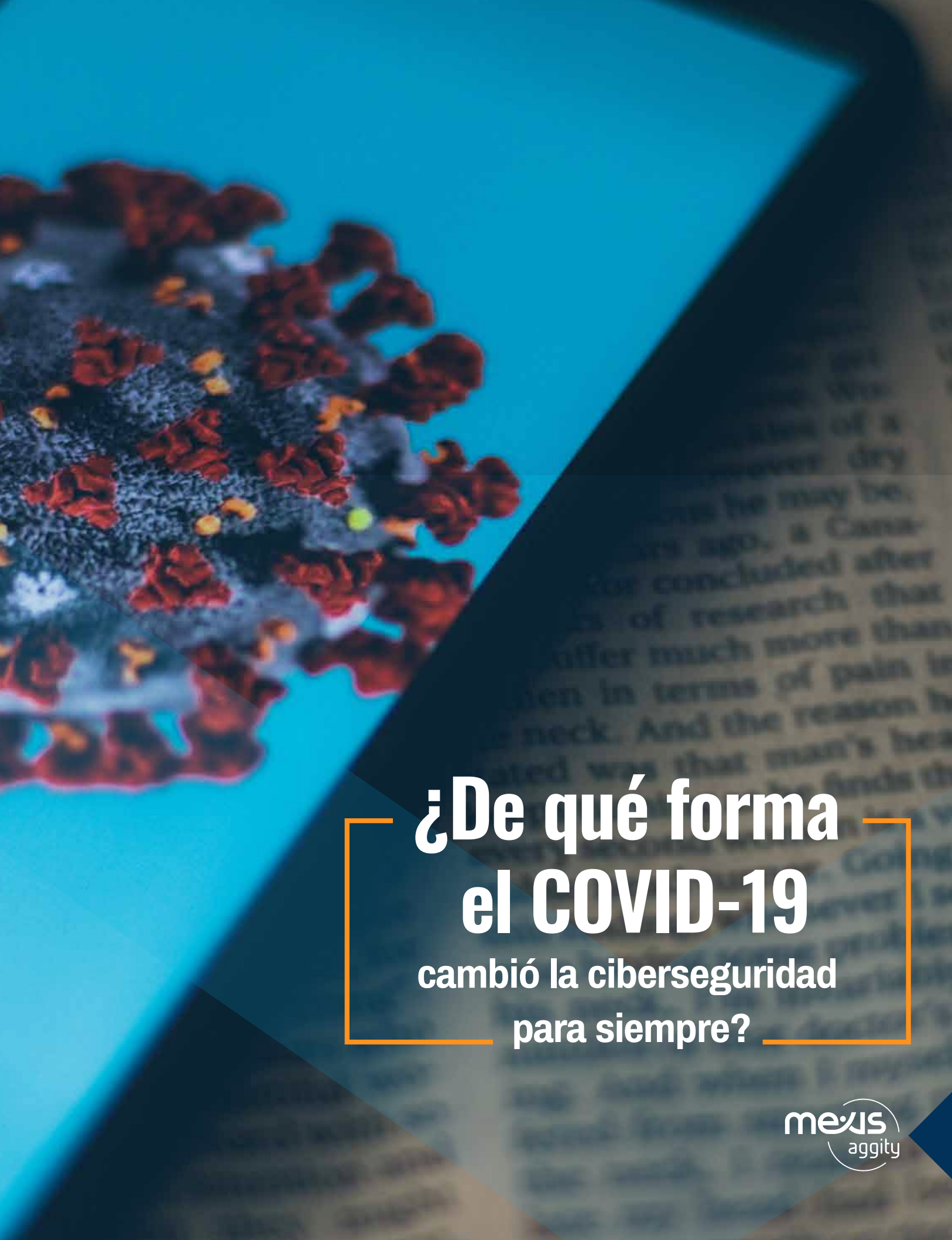
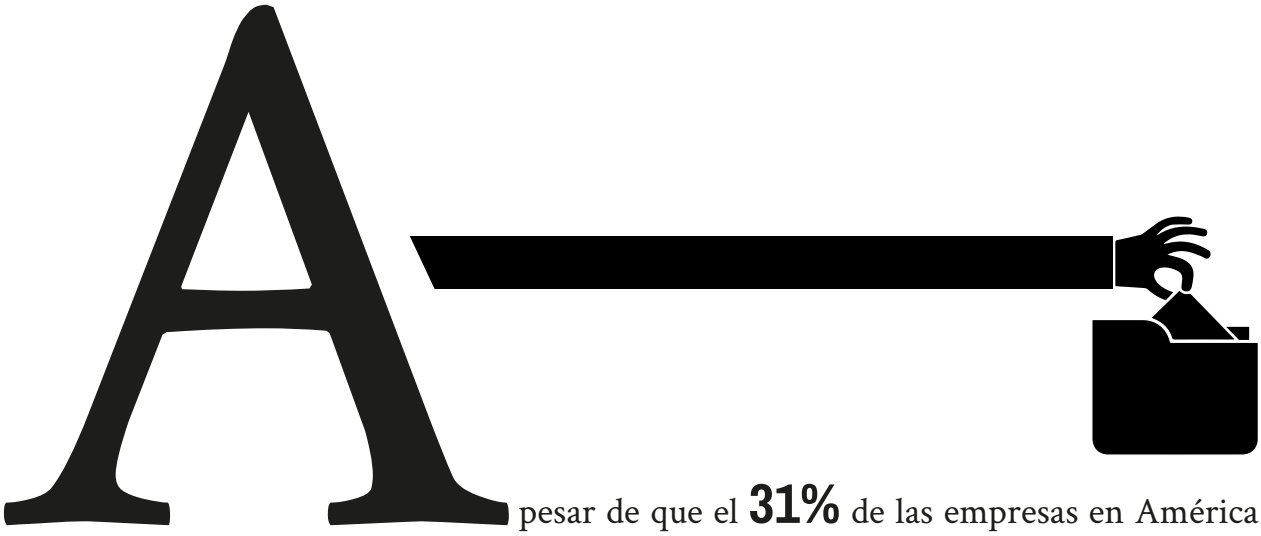


¿De qué forma el COVID-19 cambió la ciberseguridad para siempre?

mexus aggity

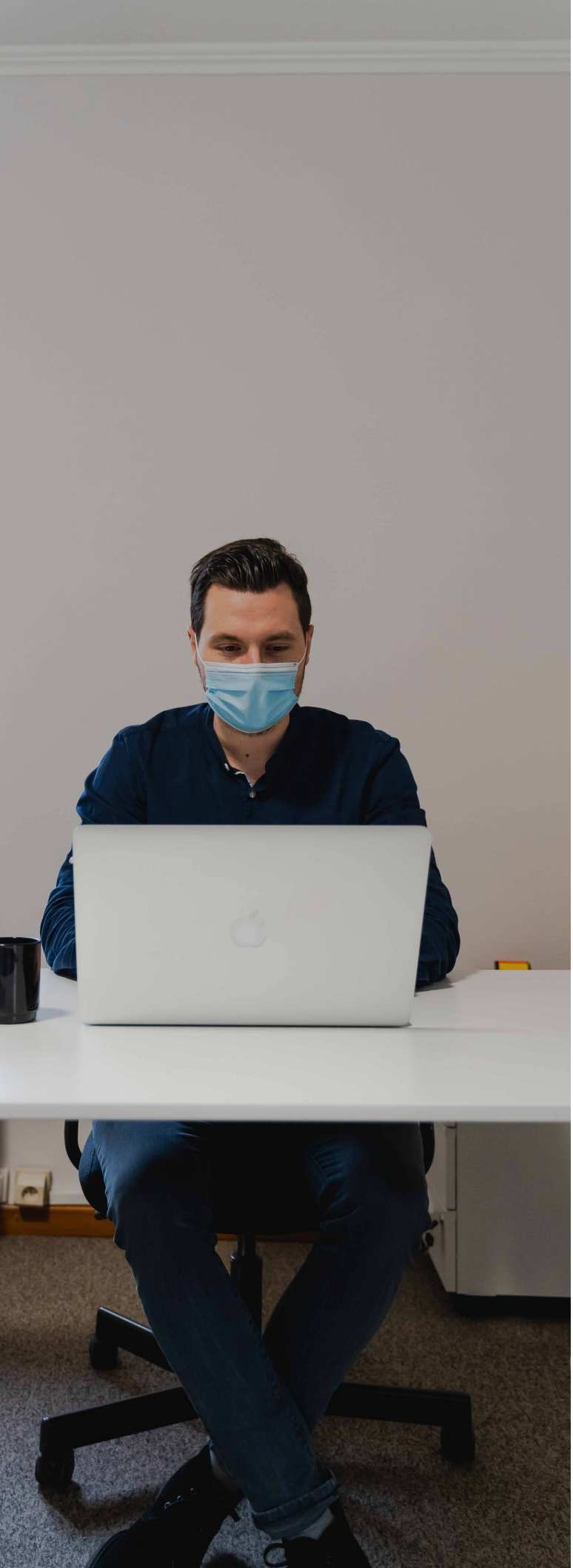


pesar de que el **31%** de las empresas en América Latina percibe un aumento en el número de ciberataques desde el inicio de la pandemia, únicamente el **24%** aumentaron sus presupuestos de ciberseguridad, y sólo el **17%** de las empresas de la región teniendo seguro contra los riesgos cibernéticos.

En Estados Unidos, Europa, Asia, Oriente Medio y África del Norte, una encuesta realizada con un grupo diverso de altos ejecutivos de ciberseguridad encontró que el **42%** de los CISO en esas regiones están de acuerdo en que la pandemia ha cambiado sus prioridades de ciberseguridad. En parte, la culpa es el aumento de los ataques a lo largo de 2020 y los atacantes que utilizan COVID como gancho para sus estafas.

El FBI informó un aumento del **400%** en las quejas de ciberseguridad durante la pandemia, y más de medio millón de usuarios de videoconferencias **sufrieron el robo y la venta de sus datos personales en la web oscura entre febrero y mayo de 2020.**

Aunque se están logrando avances con el lanzamiento de vacunas, **la batalla de la ciberseguridad está lejos de terminar.** Desafortunadamente, a medida que las empresas regresen a la oficina de alguna manera, estos problemas remotos únicos permanecerán. Se expusieron así los problemas que las empresas deben abordar:



• Transición hacia la nube

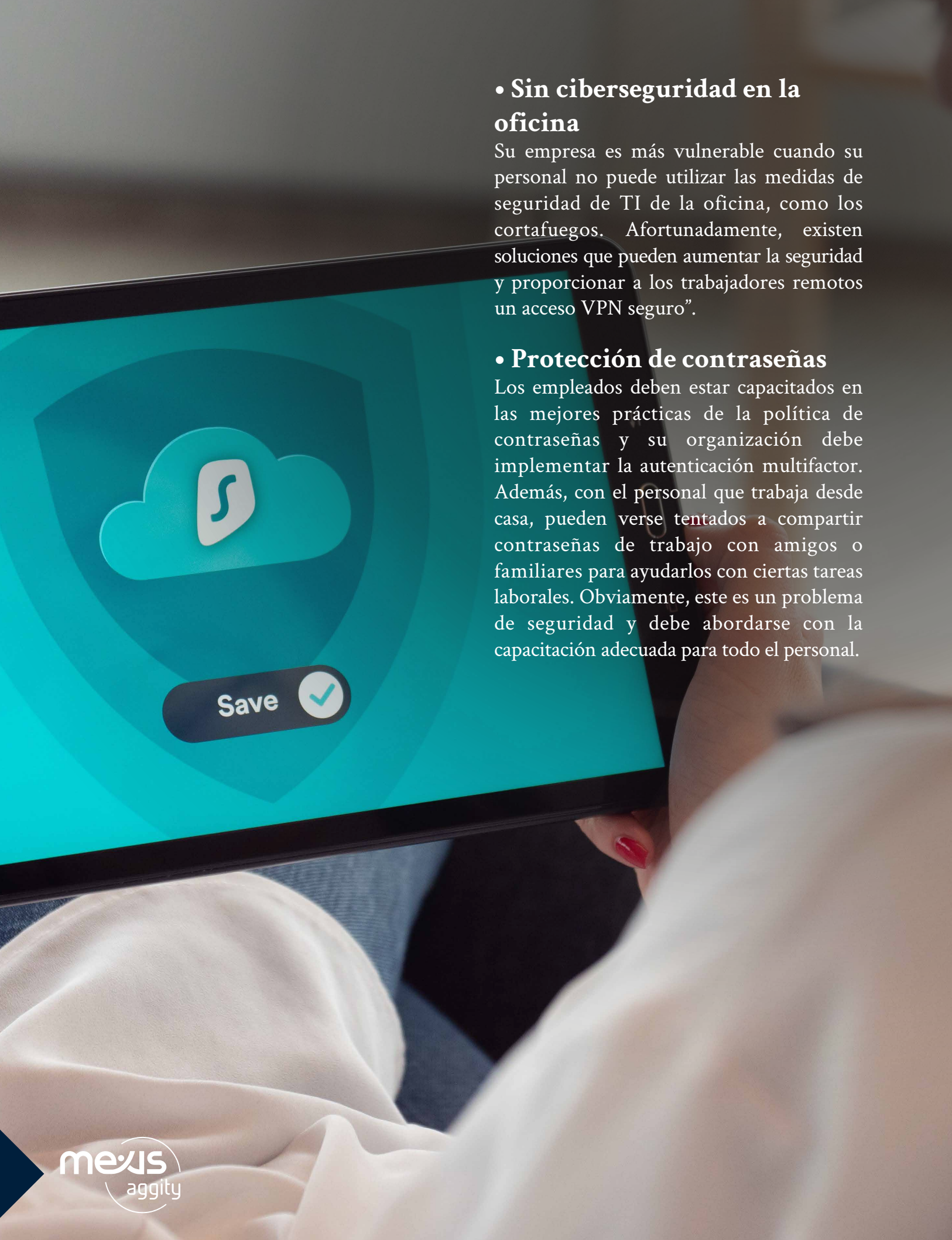
Desde la pandemia, se prefieren las soluciones de acceso remoto y las organizaciones están trasladando gradualmente los procesos comerciales críticos a la nube. Sin embargo, depender cada vez más de la nube y crear agilidad en ella podría crear más vulnerabilidades si no se protege adecuadamente. Microsoft descubrió que el 39% de las empresas están dando prioridad a las inversiones en seguridad en la nube sobre la seguridad de los datos y la información o incluso la seguridad de la red.

• Phishing por correo electrónico

El phishing por correo electrónico durante la pandemia se disparó. Existe una mayor prioridad para capacitar a los trabajadores y prepararlos para reconocer y saber cómo lidiar con las amenazas desde la pandemia y desarrollar las mejores prácticas para el acceso seguro al correo electrónico.

•Variando los dispositivos remotos

Los dispositivos móviles necesitan su propia protección de seguridad única. Pero al 52% de las organizaciones les resulta difícil proteger los dispositivos móviles de los problemas de ciberseguridad. Un primer paso fundamental para resolver esto es implementar una política eficaz de administración de dispositivos móviles.



• Sin ciberseguridad en la oficina

Su empresa es más vulnerable cuando su personal no puede utilizar las medidas de seguridad de TI de la oficina, como los cortafuegos. Afortunadamente, existen soluciones que pueden aumentar la seguridad y proporcionar a los trabajadores remotos un acceso VPN seguro".

• Protección de contraseñas

Los empleados deben estar capacitados en las mejores prácticas de la política de contraseñas y su organización debe implementar la autenticación multifactor. Además, con el personal que trabaja desde casa, pueden verse tentados a compartir contraseñas de trabajo con amigos o familiares para ayudarlos con ciertas tareas laborales. Obviamente, este es un problema de seguridad y debe abordarse con la capacitación adecuada para todo el personal.

Desafíos de ciberseguridad en la oficina

De cara al futuro, las organizaciones inevitablemente implementarán un híbrido de horarios de trabajo desde casa y en la oficina para su personal. Desafortunadamente, el regreso a la vida de la oficina presentará sus propios problemas de ciberseguridad únicos. Como ejemplo reciente, muchos piratas informáticos están distribuyendo archivos maliciosos e intentos de phishing que se parecen a los documentos de capacitación de COVID-19.

¿Por qué arriesgarse con los ciberataques?

La transición al trabajo remoto ha sido un obstáculo difícil de navegar para muchas empresas. Es lo suficientemente desafiante mantener las operaciones y la productividad mientras se trabaja desde casa, no importa garantizar una ciberseguridad remota completa. Sin embargo, a medida que aumentan los problemas de seguridad (como las estafas de phishing), también debe hacerlo la seguridad y la resistencia de su organización.

Con las amenazas de ciberseguridad que enfrentan tanto los trabajadores remotos como los que regresan a la oficina, es esencial mejorar su seguridad de TI.

Fuente de información: cio.com.mx
Autor: José Luis Becerra Pozas