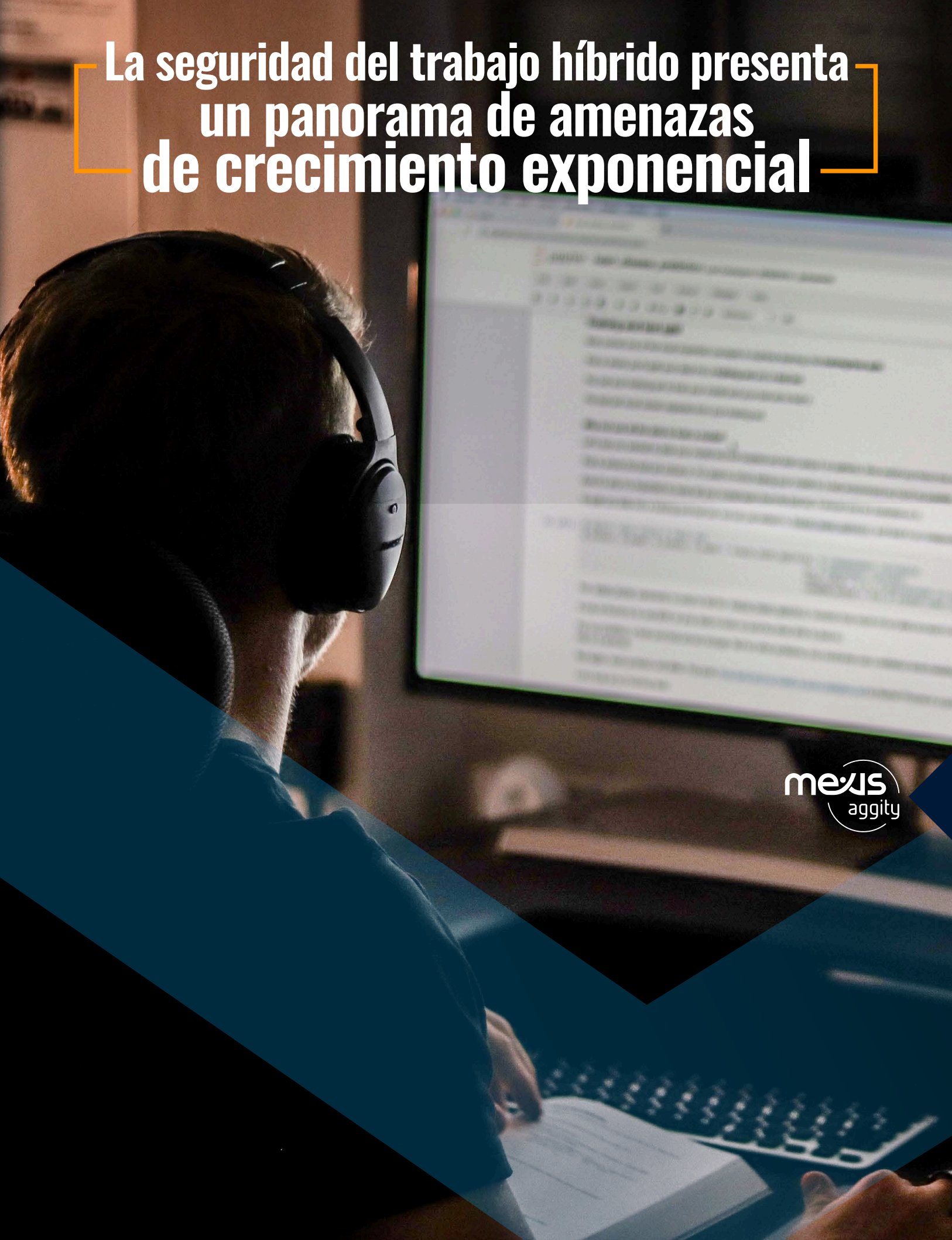
La seguridad del trabajo híbrido presenta un panorama de amenazas de crecimiento exponencial

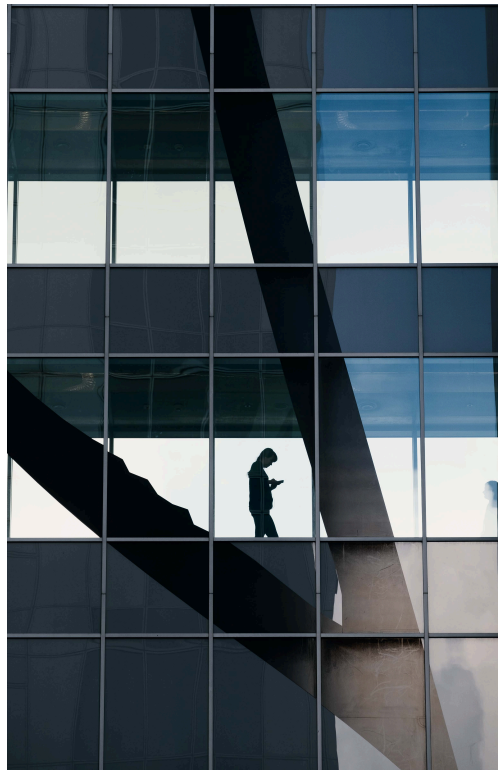


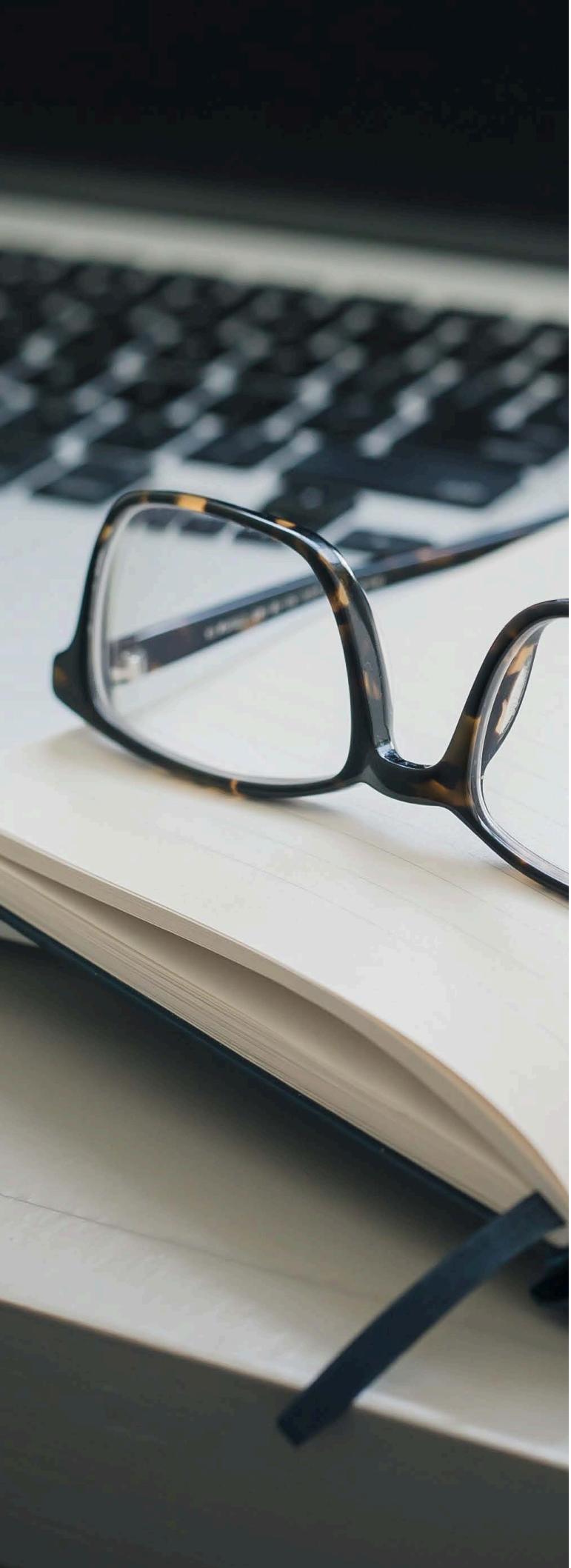
Estudio global y exhaustivo que pone de manifiesto la tensión existente entre los equipos de TI y los profesionales que trabajan desde casa, algo que los responsables de seguridad deben resolver para garantizar el futuro del trabajo.

Los resultados del estudio muestran que los equipos de TI se han visto obligados a comprometer la seguridad en favor de la continuidad del negocio en un momento en el que el aumento de las amenazas está más que presente. Además, sus intentos de aumentar o actualizar las medidas de seguridad en favor de los profesionales que realizan su actividad en remoto han sido a menudo rechazados.

Esta realidad resulta especialmente llamativa en el caso de los futuros trabajadores cuya edad se sitúa actualmente entre 18 y 24 años, nativos digitales que se sienten cada vez más frustrados por el hecho de que la seguridad se interponga en su trabajo, lo que a veces lleva a muchos a eludir los controles.

El informe combina los datos de una encuesta global de YouGov en la que participaron 8.443 trabajadores de oficina que, de un día para otro, tuvieron que trabajar desde sus hogares durante la pandemia; y de una encuesta global a 1.100 responsables de la toma de decisiones de TI, realizada por Toluna. Las principales conclusiones son:





El **76 %** de los equipos de TI admite que la seguridad quedó en un segundo plano frente a la continuidad del negocio durante la pandemia, mientras que el **91%** se sintió presionado a comprometer la seguridad en favor de la continuidad del negocio.

Casi la mitad **(48 %)** de los trabajadores más jóvenes **(18-24 años)** encuestados consideraron que las herramientas de seguridad eran un obstáculo, lo que llevó a casi un tercio **(31 %)** a intentar saltarse las políticas de seguridad de la empresa para realizar su trabajo.

El **48%** de los trabajadores encuestados está de acuerdo en que las medidas de seguridad aparentemente esenciales suponen una gran pérdida de tiempo, porcentaje que se eleva al **64 %** entre las personas de **18 a 24 años.**

Más de la mitad **(54 %)** de los jóvenes de entre **18 y 24 años** estaban más preocupados por cumplir los plazos que por exponer a su organización a una violación de los datos; el **39%** no estaba seguro de lo que decían sus políticas de seguridad, o ni siquiera sabía si su empresa las tenía, lo que sugiere un creciente nivel de apatía entre los trabajadores más jóvenes.

Como resultado, el **83 %** de los equipos de TI creen que el aumento del teletrabajo ha creado una «bomba de relojería» que podría provocar fallos en la red corporativa.

Si la seguridad resulta demasiado tediosa, la gente encontrará una forma de evitarla. Por ello, la seguridad debe encajar en la medida de lo posible en los patrones y flujos de trabajo existentes, con una tecnología que sea discreta, segura por diseño e intuitiva para el usuario. En última instancia, tenemos que hacer que sea tan fácil trabajar de forma segura como trabajar de forma insegura, y podemos hacerlo incorporando la seguridad a los sistemas desde el principio.

El informe destaca que muchos equipos de seguridad se han esforzado por frenar el comportamiento de los usuarios con el objetivo de mantener los datos a salvo. El 91% ha actualizado las políticas de seguridad para tener en cuenta el aumento del trabajo desde casa, mientras que el 78% ha restringido el acceso a sitios web y aplicaciones. Sin embargo, estos controles a menudo crean fricciones para los usuarios, que se resienten y presionan al departamento de TI, lo que hace que los equipos de seguridad se sientan abatidos y rechazados:

- El **37 %** de los trabajadores encuestados afirmó que las políticas y tecnologías de seguridad suelen ser demasiado restrictivas.
- El **80 %** de los equipos de TI experimentan la reacción de aquellos usuarios a los que no les gusta que se les impongan controles en casa; el **67 %** de los equipos de TI dicen que reciben quejas sobre esto semanalmente.
- El **83 %** de los equipos de TI afirmaron que intentar establecer y aplicar políticas corporativas en torno a la ciberseguridad es imposible ahora que las líneas entre la vida personal y la profesional son tan difusas.
- El **80 %** de los equipos de TI afirmó que la seguridad informática se estaba convirtiendo en una «tarea ingrata» ya que nadie los escucha.
- El **69 %** de los equipos de TI señaló que se les hace sentir como los «malos» por imponer restricciones.

Los CISO se enfrentan a un volumen, una velocidad y una gravedad de los ataques cada vez mayores, sus equipos están teniendo que trabajar las veinticuatro horas del día para mantener la seguridad del negocio, mientras facilitan la transformación digital masiva con una visibilidad reducida. Los equipos de ciberseguridad ya no deben cargar con el peso de asegurar el negocio únicamente sobre sus hombros, la ciberseguridad es una disciplina integral en la que todos deben participar.

Para crear una cultura de seguridad más colaborativa, debemos involucrar y educar a los trabajadores en los crecientes riesgos de ciberseguridad, mientras que los equipos de TI necesitan entender mejor cómo la seguridad afecta a los flujos de trabajo y a la productividad.

A partir de aquí, la seguridad necesita ser reevaluada en base a las necesidades tanto del negocio como del trabajador híbrido.

Fuente de información:
www.ciberseguridad.link