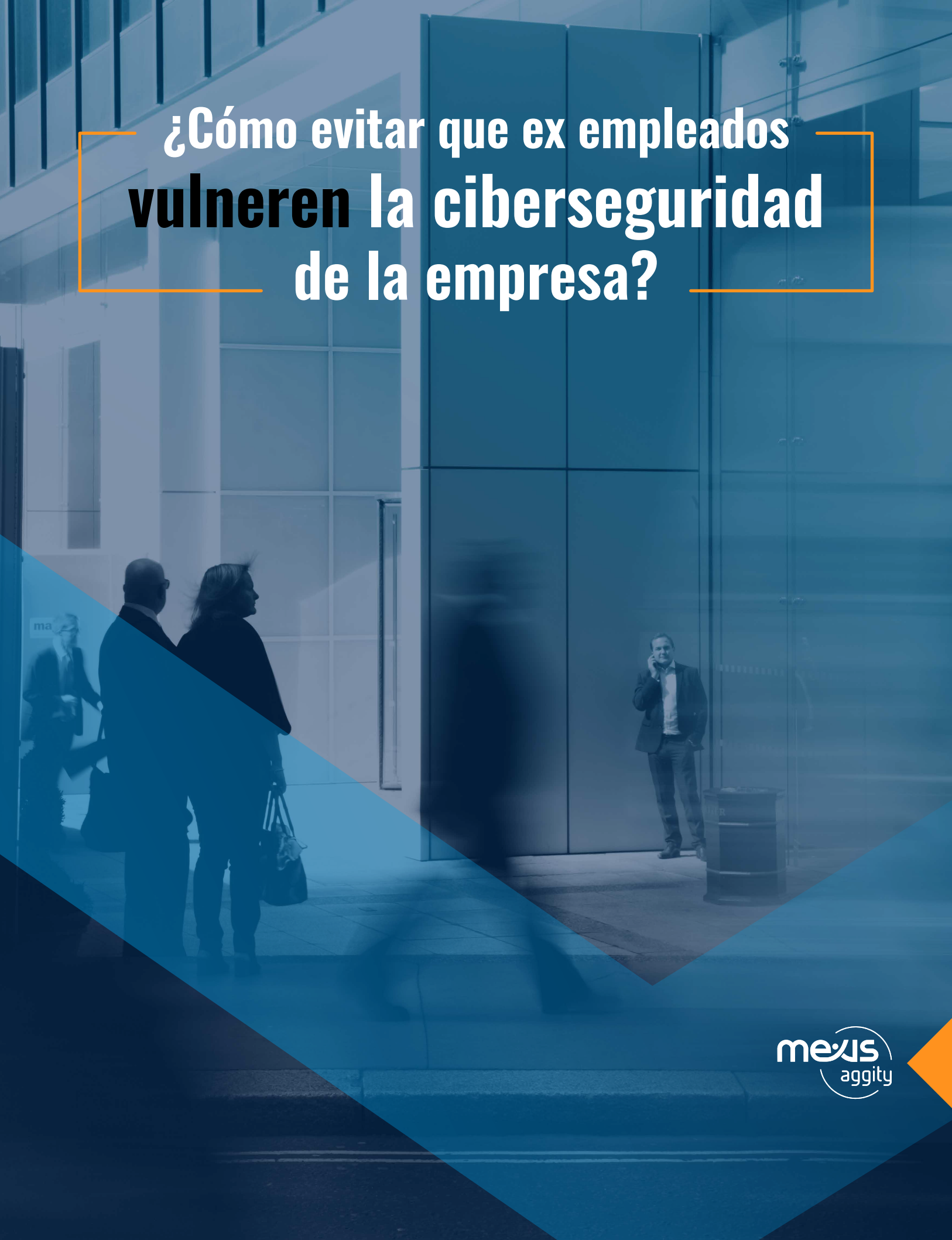
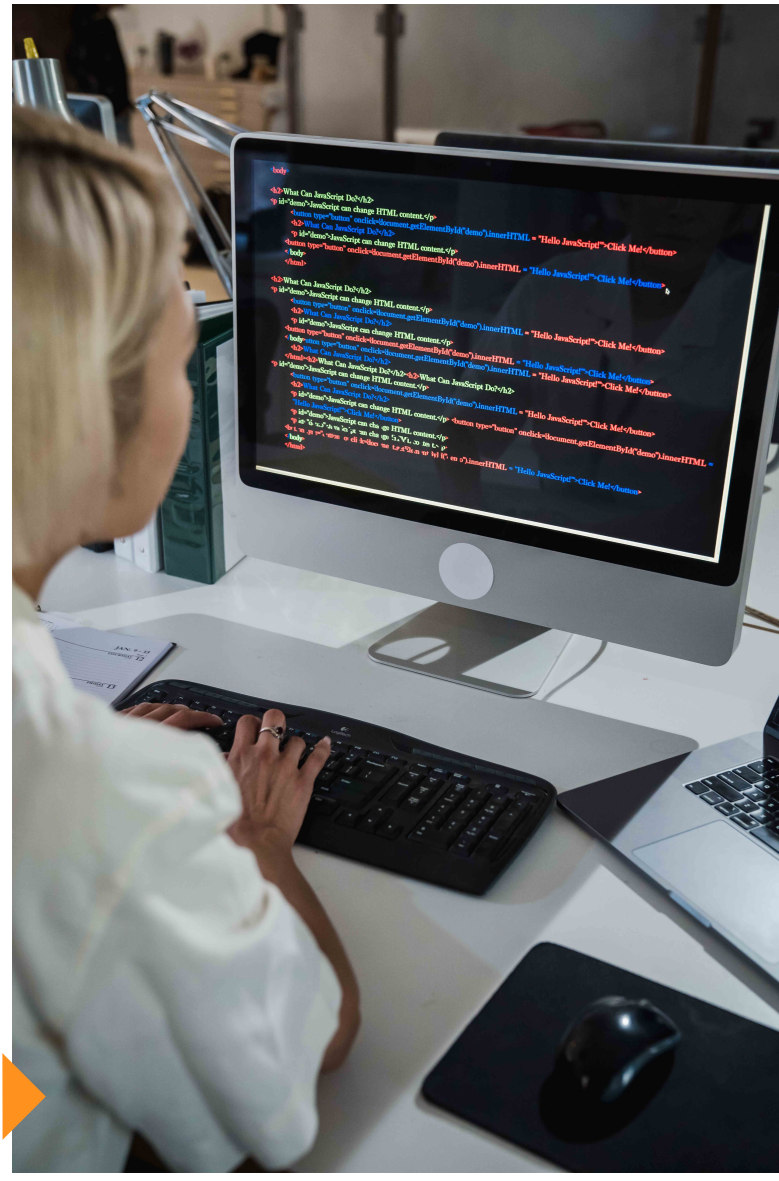


¿Cómo evitar que ex empleados **vulneren** la ciberseguridad de la empresa?

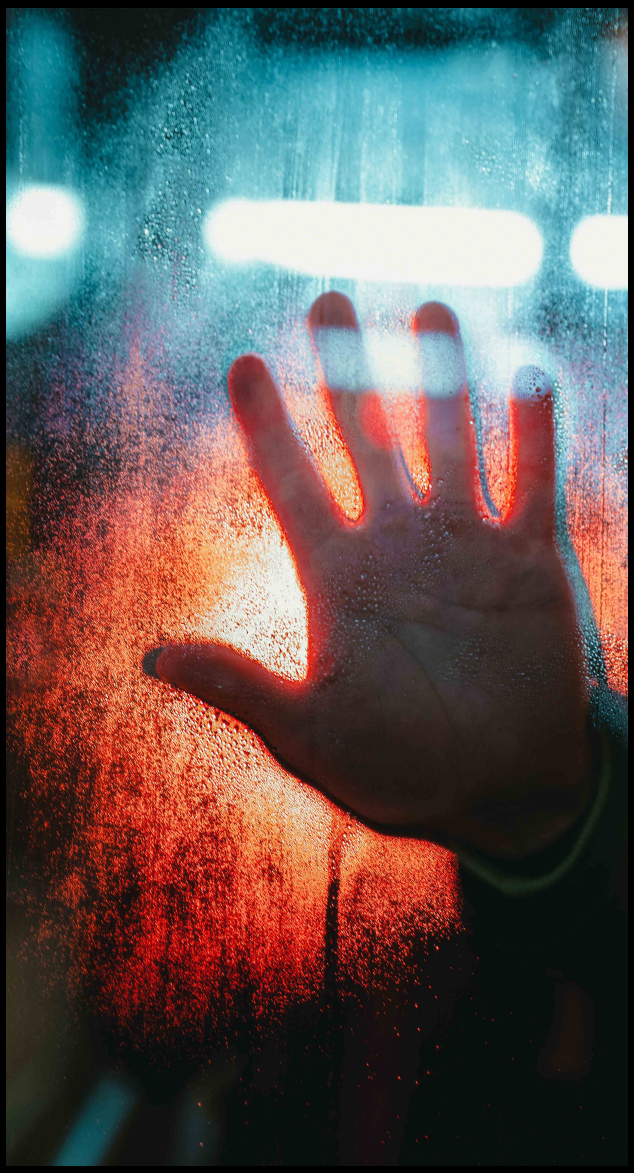
mexis aggity

DOS DE CADA CINCO LÍDERES DE PYMES MEXICANAS NO PUDO CONFIRMAR SI LOS EX EMPLEADOS TIENEN ACCESO O NO A LOS ACTIVOS DIGITALES.

Cuando un empleado se va, una de las preocupaciones de algunas empresas es que pueda atentar contra la ciberseguridad y robar información o causar un conflicto, especialmente si no salieron en buenos términos. Este temor se intensifica en las pequeñas y medianas empresas (pymes), pues al menos un **40%** teme que un ex empleado acceda a los archivos corporativos.



De acuerdo con un estudio sobre el comportamiento de las pymes durante tiempos de crisis, muchos directivos de empresas no tienen la certeza de que el acceso a la información es imposible para los colaboradores que se van. **Dos de cada cinco no pudo confirmar si se tiene acceso o no a los activos digitales.**



> "En México, 29% de las pymes considera los recortes de empleo como una posible medida para reducir costos en caso de crisis, pero **es la reducción de personal considerado un factor de riesgo para la seguridad de la información",** indica el informe.

Entre las principales preocupaciones en torno al tema, destaca que se haga un **mal uso de los datos** en los nuevos trabajos de las personas con **67%,** o **utilizar las bases de datos corporativas** como listas de clientes que permitan generar oportunidades de negocios a nivel personal con **56%.**

El acceso no autorizado de terceros puede convertirse en un gran problema para cualquier empresa, ya que afecta a su competitividad cuando los datos corporativos se comparten con un competidor, se venden o se eliminan.

Crece conciencia de ciberseguridad

Ante la búsqueda de combatir la crisis económica relacionada con los problemas del entrono, las empresas están tomando medidas para seguir recortando gastos y garantizar su supervivencia.

El principal es menor inversión en publicidad y promoción **(36%),** seguido de reducir gastos en vehículos tanto en compra como en renta **(34%),** y reducir la fuerza laboral y congelar contrataciones con **(31%).** La buena noticia es que la ciberseguridad no se está sacrificando tanto, solo en un **13%** de los casos porque ya se tiene conciencia de todos los impacto que se pueden tener.

Qué hacer

Al abordar los retos más grandes para mantener una resiliencia cibernética, el problema más grande que han vivido las pymes es la infiltración de datos con **41%,** así como comprender los nuevos riesgos (donde se involucran ex empleados) con **34%** y problemas operativos por fallas en el área de TI, con **34%.**

Pablo Basso, Gerente de Tecnología e Innovación en Ecomsur, líder en soluciones de Full-commerce en Latinoamérica, explica que hay muchas malas prácticas que buscan el acceso y robo de información, por lo que las áreas de seguridad de las empresas deben prepararse mejor.

- Datos de la encuesta de PwC, Digital Trust Insights 2022, revelan que 63% de los líderes de negocios preveía, en este año, un aumento en el número de ciberataques a sus servicios de nube y robo de datos que podrían afectar sus estrategias de marketing y ventas. Muchos sí ocurrieron.

Ante esto, ¿cómo pueden las pymes protegerse?

. Mantener el control del número de colaboradores que accedan a los datos de la organización.

. Crear una política de acceso a los activos, donde se incluyan correos, carpetas compartidas y documentos en línea

. Hacer copias de seguridad periódicas de los datos esenciales

. Fomentar la cultura de cambio frecuente de contraseñas en los empleados

. Educar sobre el tema de ciberseguridad

. Acercarse con especialistas para intensificar la protección

. Buscar seguros contra ciberataques que cubran pérdidas causadas por hackeos o ransomware

. Implementar un modelo de cero confianza donde siempre se verifique al usuario y dispositivo que trata de acceder a los datos, estableciendo seguridad por capas

. Estar siempre prevenido ante posibles casos

Fuente de información: eleconomista.com.mx