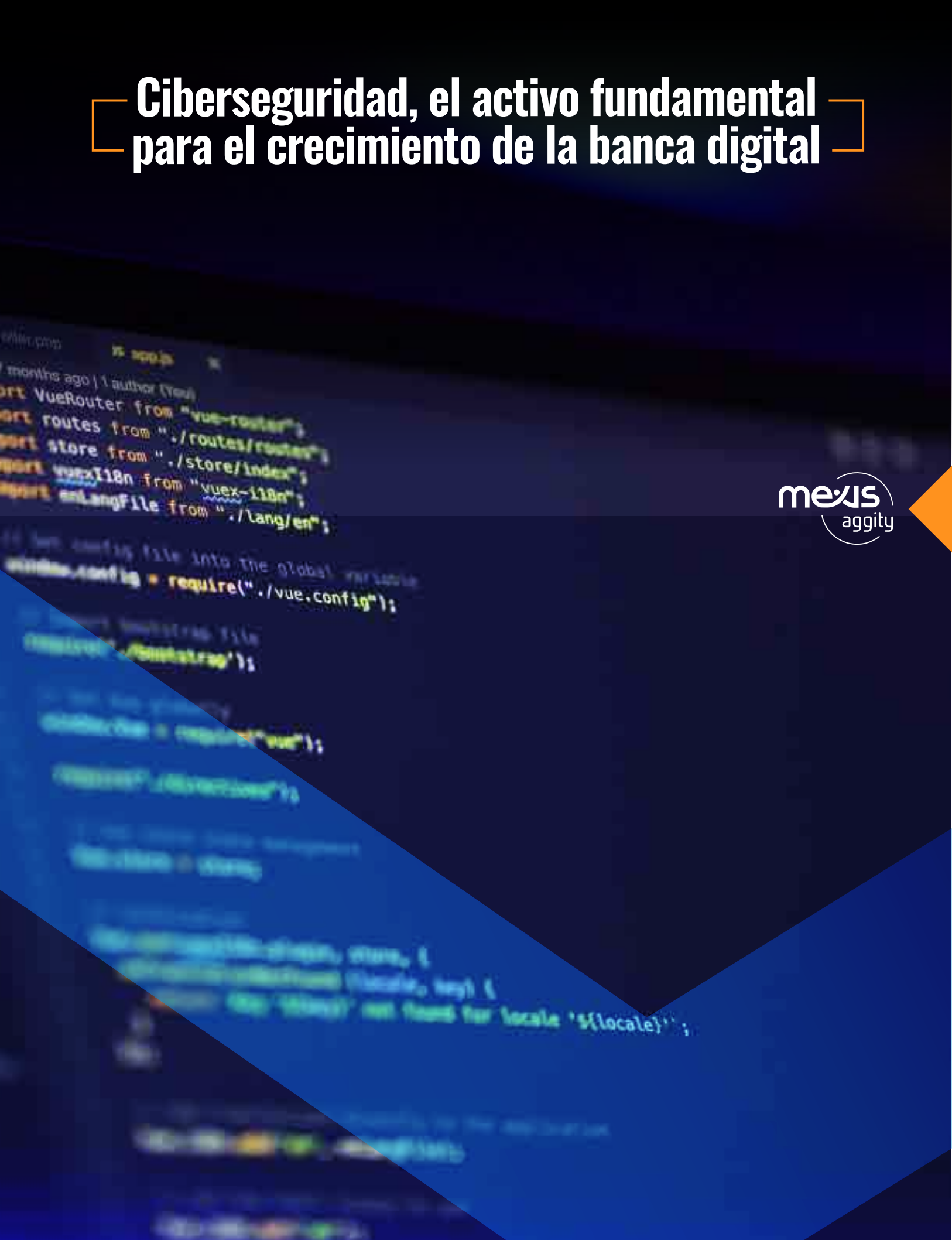
Ciberseguridad, el activo fundamental para el crecimiento de la banca digital



Vivimos en un mundo que cada vez está más conectado digitalmente.

La pandemia de Covid-19 aceleró la transformación digital, generando un cambio significativo en los modelos de negocio.

Vivimos en un mundo que cada vez está más conectado digitalmente. La pandemia de Covid-19 aceleró la transformación digital, generando un cambio significativo en los modelos de negocio y en el comportamiento de clientes, colaboradores, socios y proveedores. Esta transformación permitió continuar con las operaciones a la distancia, pero al mismo tiempo ha presentado grandes retos por atender.

En México los clientes del sector bancario sostienen un amplio uso de las sucursales, por lo que las limitaciones impuestas dificultaron sus operaciones y obligaron al sector a mejorar sus canales digitales, brindando la misma calidad, seguridad y evitando posibles saturaciones o caídas de los sistemas.

El desarrollo de estas nuevas herramientas ha sido benéfico, al permitir que ahora los procesos sean más ágiles y sencillos, así como una optimización de recursos y una ampliación en la oferta de servicios innovadores. Sin embargo, lograr una verdadera transformación requiere pasar del "digital first" al "digital only", sin descuidar los canales tradicionales, pero atendiendo la nueva realidad.

En el "digital only" la ciberseguridad es un tema prioritario y transversal para todas las operaciones, lo cual se ha reflejado en la inversión destinada a este rubro en los últimos años. Existe un creciente número de ciberdelincuentes que buscan vulnerar la integridad de la banca y de sus clientes mediante aplicaciones informáticas, sistemas biométricos e inteligencia artificial.

El impacto de un mal manejo de ciberseguridad en el “digital first” vulnera las operaciones de la banca e incluso esto puede ir desde el simple robo de información, secuestro de datos de clientes o hasta el cobro de una recompensa para su liberación.

En “digital only” el ataque afecta directamente la continuidad de las operaciones, haciendo necesario contar con un blindaje total.

El hacer frente a los riesgos cibernéticos requiere, saber diseñar y desplegar estrategias preventivas y de atención inmediata. Un ejemplo son los casos en donde los atacantes saturan la red con solicitudes para bloquear las comunicaciones, los cuales son cada vez más frecuentes. Atenderlo de manera efectiva requiere más que tener un ancho de banda suficiente, es vital conocer cuándo se debe ampliar, ensanchar y tener replicabilidad, entre otros elementos para realmente brindar esa seguridad.

Los riesgos de ataques se incrementan año con año, pero también lo hace la especialización del sector de ciberseguridad. Se debe cambiar el foco desde una actitud reactiva a una proactiva, en donde además se integre a clientes, proveedores, socios y colaboradores para construir un frente unido.

La ciberseguridad se ha convertido en una industria en crecimiento, es un tema importante en el cual tenemos que poner principal foco al ser de una de las tendencias con mayor potencial de crecimiento en un contexto cada vez más digital. El no hacerlo es seguir pensando en el “digital first” en lugar del “digital only”.

Autora: Mónica Hernández, CISO en Banco Sabadell
Fuente de información: www.forbes.com.mx