Digitalización y ciberseguridad,

oportunidad para elevar la competitividad de las organizaciones: Siemens

Digitalización y ciberseguridad van de la mano, y juntas representan una oportunidad para elevar la competitividad de las organizaciones a través de asegurar la continuidad del negocio, resguardar su propiedad intelectual y optimizar procesos para mejorar la productividad.

El reto está en que las empresas den relevancia al tema y en el rezago tecnológico que se enfrenta en México y América Latina, dijo Natalia Oropeza, Chief Cibersecurity Officer de Siemens a nivel global.

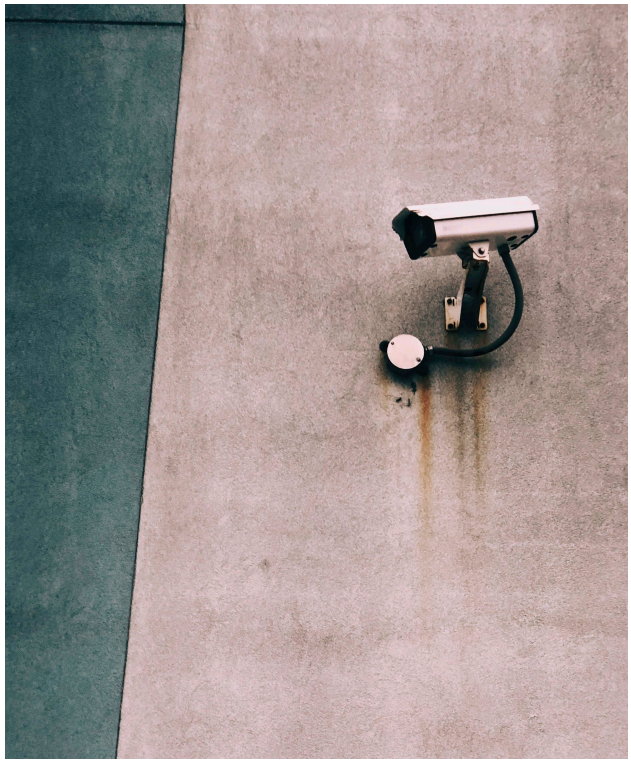
"No podemos digitalizar sin establecer ciberseguridad. Son las dos caras de la misma moneda, digitalización y ciberseguridad", dijo.

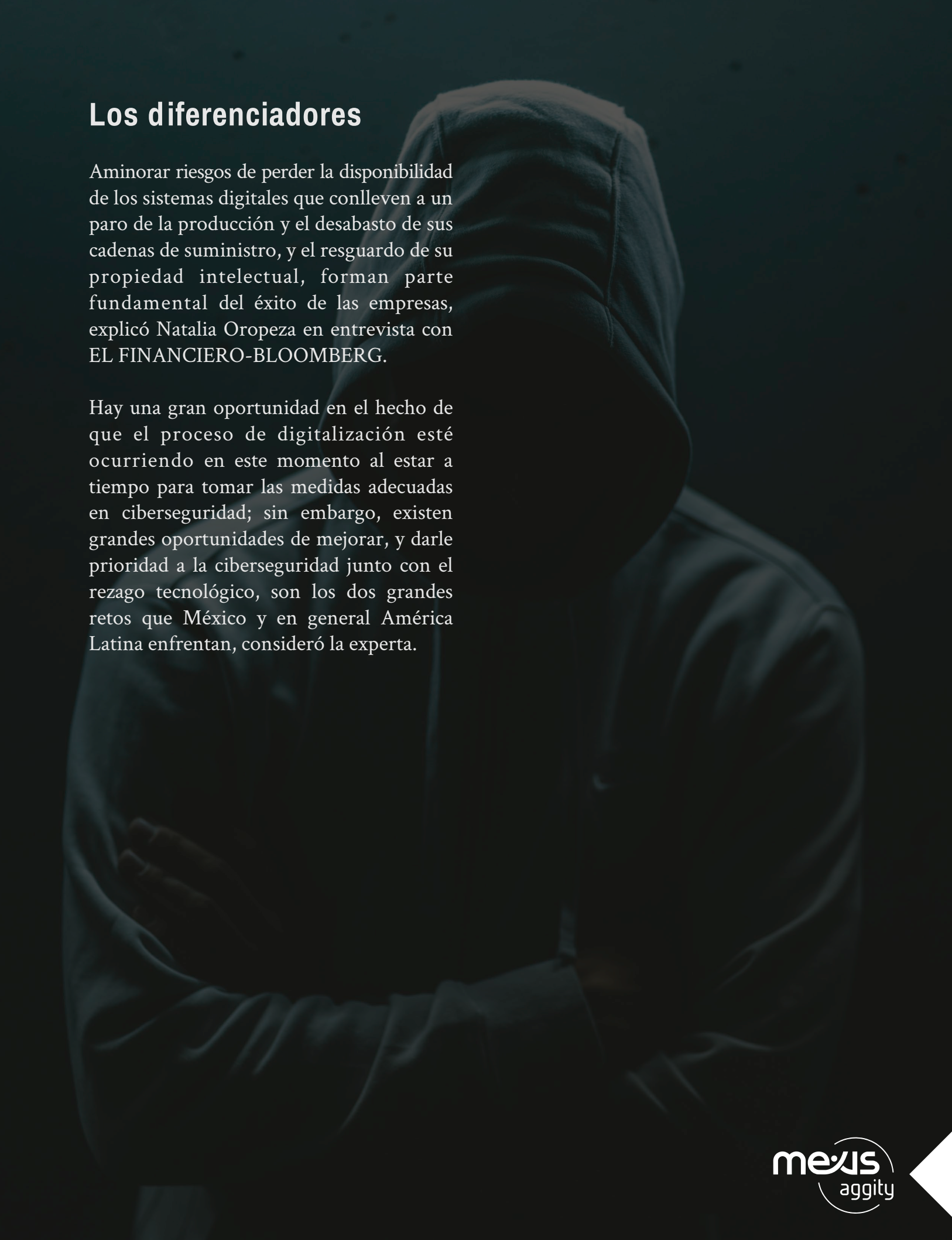
Conforme se avanza en la digitalización industrial o en cualquier otro entorno, aumenta la superficie propensa a los ataques cibernéticos y con ello las vulnerabilidades. Tan sólo en los últimos cinco años se ha duplicado el número de dispositivos conectados a internet, de 25 mil millones en 2015 a 50 mil millones al cierre del 2020.

Con la pandemia de Covid-19 se aceleró el ritmo de digitalización a nivel mundial y con ello, las amenazas y los ataques. Las estadísticas indican que el cibercrimen creció un 600 por ciento desde que inició la pandemia, lo que elevó el valor del mercado para productos y servicios de ciberseguridad, valuado en 156 mil millones de dólares con un crecimiento anual de 27 por ciento.

En Siemens hay aproximadamente mil alertas cada mes, originadas por ataques de hackers, y la empresa detectó un 85 por ciento más de malware en los primeros meses de esta pandemia, todas ellas neutralizadas con éxito.

Este contexto refleja la interrelación de la digitalización y ciberseguridad con la competitividad de las organizaciones con la protección de su valor agregado o sus diferenciadores en el mercado.





Los diferenciadores

Aminorar riesgos de perder la disponibilidad de los sistemas digitales que conlleven a un paro de la producción y el desabasto de sus cadenas de suministro, y el resguardo de su propiedad intelectual, forman parte fundamental del éxito de las empresas, explicó Natalia Oropeza en entrevista con EL FINANCIERO-BLOOMBERG.

Hay una gran oportunidad en el hecho de que el proceso de digitalización esté ocurriendo en este momento al estar a tiempo para tomar las medidas adecuadas en ciberseguridad; sin embargo, existen grandes oportunidades de mejorar, y darle prioridad a la ciberseguridad junto con el rezago tecnológico, son los dos grandes retos que México y en general América Latina enfrentan, consideró la experta.

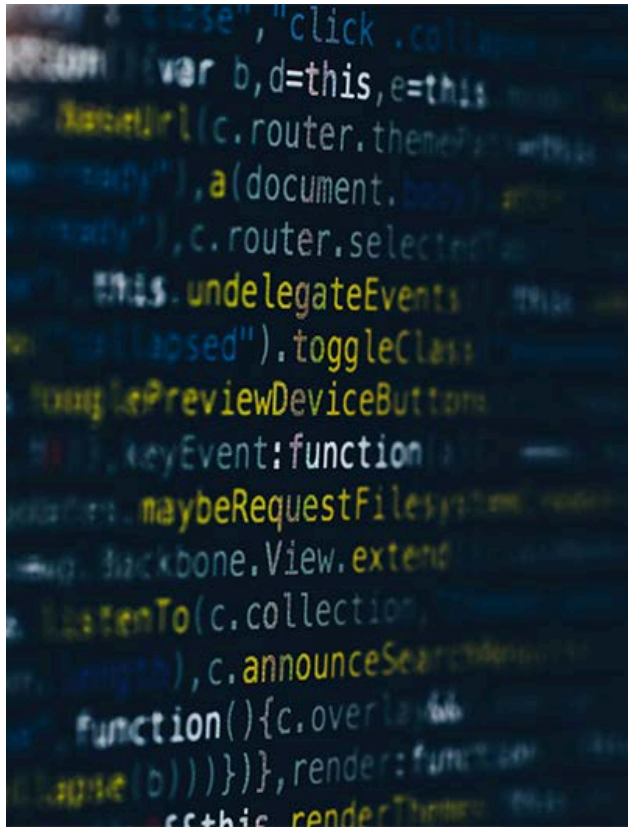
“Las empresas, los gobiernos, aun no le ponen la prioridad al tema que se merece y eso es un gran riesgo. Aceptar el riesgo es legítimo, pero ignorarlo conlleva a matar al negocio y para aceptar el riesgo hay que reconocerlo. Una vez que las empresas, los bancos y los gobiernos lo reconocen, entonces lo atienden de manera adecuada”, señaló.

La calidad y condiciones de la infraestructura es otro gran reto para la protección de los ciberataques. Si la infraestructura no es renovada y actualizada, cuando se conecta a las redes amplían la superficie de ataque y aumentan el riesgo, y en este sentido son las pequeñas y medianas empresas las más vulnerables al no darle prioridad al tema y creer que se trata de inversiones cuantiosas, cuando no lo son si se toman las medidas a tiempo.

“Es muy importante, uno, asignar la prioridad al tema de ciberseguridad, y dos, instalar las medidas de seguridad en las fases primeras de los diseños de los sistemas y de los procesos de digitalización”, aseguró Oropeza.

Inversión, el camino a seguir.

La inversión en la instalación de las medidas adecuadas resulta menos alta cuando se hacen por diseño, lo que se conoce como security by design. Si se invierte en ciberseguridad desde el principio del diseño de los procesos, del software y los sistemas que intervienen en la digitalización,



> “Se pagan centavos” comparado con lo que se tendría que gastar en caso de hacer composturas con el tiempo o pagar por un ataque de ransomeware en donde el atacante encripta los archivos de las empresas y a cambio pide dinero, explicó Natalia Oropeza.

En este sentido, Siemens ha trabajado en el campo de seguridad de las Tecnologías de la Información (IT) durante 30 años. Debido al impulso de la digitalización y la convergencia de ambientes dentro y fuera del mundo digital, optó por un enfoque holístico en beneficio de clientes, socios y en general de la sociedad.

> “Es precisamente la protección y la experiencia de protegernos a nosotros mismos, lo que nos hace fuertes y atractivos para proteger a otras empresas”, resaltó.

La investigación en innovación para desarrollar soluciones y herramientas de protección, se combina con el conocimiento sobre los procesos industriales para entender cómo funcionan, cómo interactúan las partes en las líneas de producción, sus protocolos de comunicación normales, y las anomalías que dan información de un ataque, detalló.

Así, la armonización es punto relevante en la ciberseguridad, y por ello, Siemens fue miembro fundador de la Charter of Trust, una alianza en la que trabaja con otras compañías en diversos temas como la seguridad en cadenas de suministro y también con gobiernos sobre las diferentes regulaciones para elevar la protección del mundo digital y la confianza en su utilización.

El enfoque actual de Siemens y a largo plazo, se centra en centra en sistemas de diseño de auto aseguramiento, validación de seguridad del gemelo digital, next-Gen patching, seguridad para
sistemas co-operativos, post quantum crypto, Homomorphic Encryption, automated forensics, y análisis de malware, controles de seguridad en la nube en tiempo real, así como seguridad en la cadena de suministro, entre otos.

> “Nosotros hemos hecho innovación por 170 años y la ciberseguridad no es la excepción”, finaliza Oropeza.

Fuente de información:
www.elfinanciero.com.mx