Comunicado de prensa

Fecha	**Miércoles, 11 de noviembre de 2020**
Contacto	Lilliana García Rosas Email: lilliana.garcia.rosas@pwc.com
Páginas	4

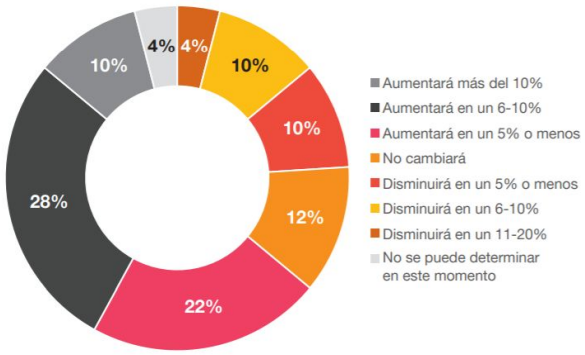
Más del 50% de las empresas mexicanas asegura que su industria podría sufrir incidentes de ciberseguridad en los próximos 12 meses

- Estos ataques podrían ser de *ransomware* (55%) o afectar a sus servicios de nube (51%)

Ciudad de México, 11 de noviembre de 2020 –La nueva normalidad derivada de la pandemia del COVID-19, ha generado retos importantes para las empresas en materia de ciberseguridad y privacidad de datos. La implementación del trabajo remoto, si bien ha servido para garantizar la salud y el bienestar de de los empleados, ha aumentado la probabilidad de sufrir ataques cibernéticos. Según el reporte *Digital Trust Insights 2021: Ciberseguridad al centro de cada decisión de negocios* de PwC, más de la mitad de las empresas mexicanas asegura que su industria podría sufrir algún incidente de ciberseguridad en los próximos 12 meses, más concretamente, de *ransomware* (55%) o afectar a sus servicios de nube (51%).

Por otro lado, el reporte también destaca que más de la mitad de los encuestados declara que los ciberdelincuentes (57%) y *hacktivistas* o *hackers* (56%) son los principales perpetradores a la hora de cometer un ataque fructífero. Asimismo, actores internos, como los empleados (48%), y otros, como los competidores (47%), también podrían perjudicar a la organización.

“Es importante que las compañías continúen preparándose para enfrentar los riesgos cibernéticos, especialmente en un momento como este, donde la dependencia de la tecnología es todavía mayor debido a la nueva normalidad”, afirma Fernando Román, socio de Ciberseguridad y Privacidad de Datos en PwC México.



¿Cómo está cambiando tu presupuesto en ciberseguridad para 2021?

Presupuesto y áreas de oportunidad

El 60% de los líderes de negocio aumentará sus inversiones en ciberseguridad para 2021: el 28% de estos, lo hará entre el 6 y el 10% y el 10% de los encuestados lo hará más allá del 10%. El 22% restante lo hará en un 5% o menos.

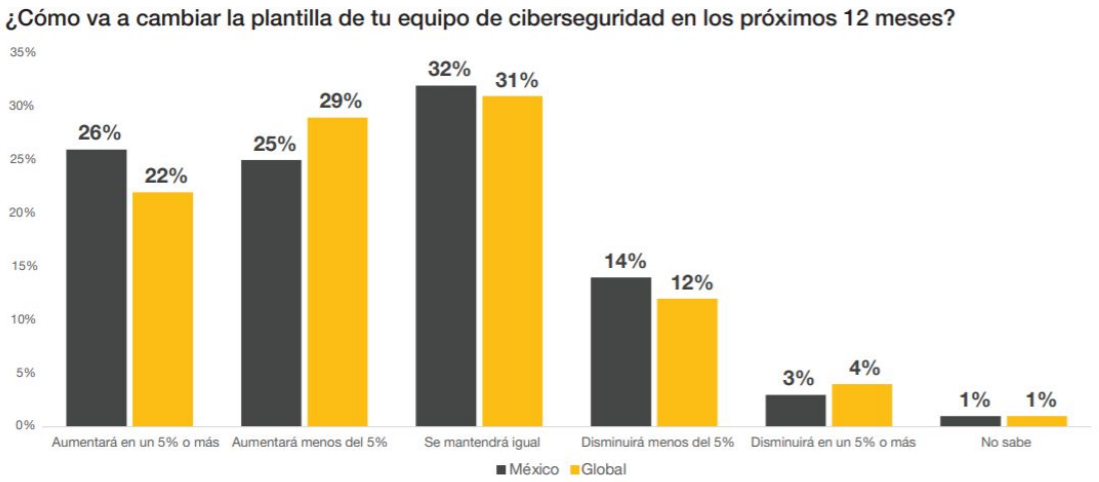
Para los próximos dos años, los encuestados creen que estos presupuestos deberían enfocarse, principalmente, en las siguientes áreas: en la mejora del conjunto de habilidades de seguridad, tecnologías avanzadas para eficientar las capacidades de detección y defensa cibernética y en cuantificar mejor los riesgos cibernéticos.

"Si bien un gran porcentaje de las empresas en México piensa invertir en ciberseguridad el próximo año, la desaceleración económica está obligándolas a reducir costos y dirigir sus recursos a las áreas y proyectos fundamentales que ayuden a la sustentabilidad de sus negocios", afirma Fernando Román. “Los directivos son conscientes de que este rubro debe fortalecerse, ya que no solo podría evitar un perjuicio económico sino también reputacional”, matiza.

En cuanto a las áreas de oportunidad en la materia de cara 2021, el 84% de las compañías cree que existen nuevas y mejores soluciones para proteger las infraestructuras en la nube, mientras que el 83% asegura que el trabajo remoto durante la pandemia, reveló la necesidad de modernizar algunos capacidades dentro de la organización, como la gestión de accesos, identidades o dispositivos móviles.

Talento

Más del 50% de las compañías mexicanas planea reforzar su plantilla en el área de ciberseguridad. De este porcentaje, 26% de las empresas la aumentará un 5% o más. No obstante, el 32% del total asegura que la mantendrá igual.



A nivel global, la brecha en la fuerza laboral de este rubro es tan grande que para satisfacer la demanda de especialistas, esta tendría que crecer en un 145%, tal y como apunta el Consorcio Internacional de Certificación de Seguridad de Sistemas de Información (ISC).

En México, se estima que hay 341 mil profesionales de ciberseguridad, según el (ISC), y de acuerdo con nuestros resultados, 53% de los ejecutivos busca que sus nuevas contrataciones tengan habilidades digitales de inteligencia de seguridad (49%), así como en gestión y análisis de datos (45%).

El papel del CISO y el CEO en la estrategia de ciberseguridad

El CISO y el CEO deben ser las personas clave a la hora de diseñar una estrategia de ciberseguridad, para que ambas visiones den como resultado un plan de acción acorde con las necesidades del negocio. Asimismo, debe definirse también un lineamiento claro sobre a quién le reporta el CISO. En México, casi un tercio (32%) de los líderes de ciberseguridad encuestados tiende cuentas al *Chief Technology Officer* (CTO) y solo un 13%, al CEO.

Para consultar información con mayor detalle, haga clic aquí.

Metodología

Los hallazgos de la *Global Digital Trust Insights 2021 (Global DTI 2021)* fueron obtenidos luego de realizar entrevistas en línea, durante julio y agosto, a 3,249 ejecutivos de negocios y tecnología de 44 países y siete mercados alrededor del mundo de industrias tecnología, telecomunicaciones (22%), minoristas y consumo (20%), servicios financieros (19%), manufactura (19%), salud (8%), energía (8%) y gobierno / servicios públicos (4%). En el caso específico de México participaron 120 ejecutivos (mujeres 42% y hombres 58%

Sobre PwC

En PwC, nuestro propósito es generar confianza en la sociedad y resolver problemas importantes. Somos una red de firmas en 157 países con más de 284,000 personas

comprometidas a brindar calidad en servicios de aseguramiento, asesoría e impuestos. Obtenga más información y cuéntenos lo que le importa al visitarnos en www.pwc.com