Ciberseguridad y privacidad de datos: hacia una gestión proactiva de riesgos

Digital Trust

Edición México

Introducción

La revolución digital está transformando cómo las organizaciones deben abordar las tecnologías emergentes y concebir nuevas formas de estructurar sus procesos. Hasta hace una década podíamos percibir indicios de una disrupción, pero hoy los cambios parecen no detenerse. Estos presentan desafíos y oportunidades mayúsculos que deben encarar las empresas rápidamente, ya que de sus estrategias digitales podría depender su competitividad y, en última instancia, su supervivencia.

Esto ilustra la importancia de tener un mayor control sobre la información sensible que se maneja, debido a que la seguridad podría verse debilitada, comprometiendo la privacidad de sus datos y sus operaciones cotidianas, lo que causaría daños económicos y en procesos estructurales. Los riesgos han mutado hacia elementos más integrados entre sí, como la ciberseguridad, la privacidad y la ética de datos, los que hoy están íntimamente ligados a las incidencias en los negocios.

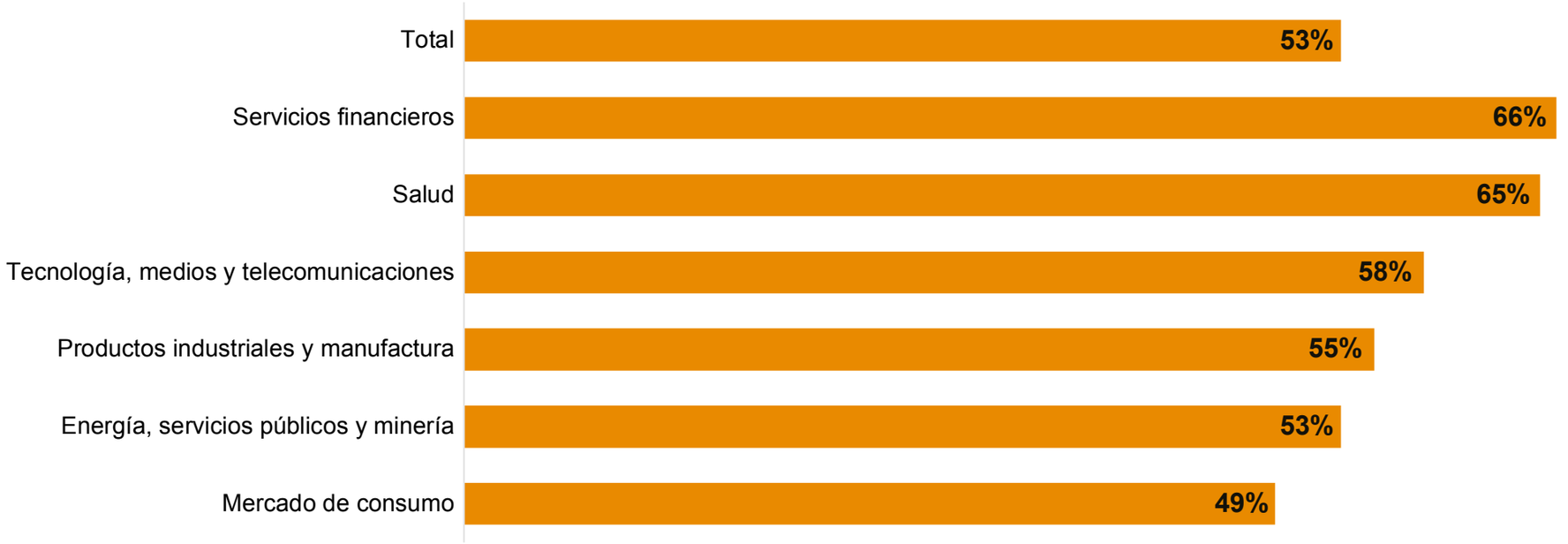
Si bien hay otros elementos como la confianza digital y la atracción adecuada de talento, la resiliencia cibernética se ha convertido en uno de los pilares de defensa en las organizaciones, por lo que contar con sistemas de recuperación, mantener la información íntegra ante intrusiones y continuar la marcha de la empresa ante un ataque, es primordial.

Un buen programa de ciberseguridad requiere de una estrategia para los proyectos desde su comienzo, lo que significa captar al personal adecuado y capacitado para diseñar, construir y sostener una transformación digital. Al mismo tiempo, relacionarse con negocios que han pasado por cambios similares y han tenido éxito, además de colaborar con firmas líderes en tecnología para apuntalar estos esfuerzos, ayudará a este proceso.

La inteligencia artificial (IA), por ejemplo, presenta grandes ventajas para las compañías, pero es un medio por el que los delincuentes cibernéticos pueden encontrar un sinnúmero de ventanas para cometer intrusiones de alto impacto, lo que comprometería cualquier diseño débil o mal implementado.

Es importante considerar que si bien se están dando los pasos adecuados hacia una transformación digital, no se deben ignorar o minimizar los riesgos cambiantes inherentes al ámbito de ciberseguridad y a la integridad de la información, por lo que es imperativa la actualización e innovación constantes en cada sector productivo. De acuerdo con el reporte de PwC, *Digital Trust Insights 2018*,[1] la industria de servicios financieros ha incluido, por diseño, una gestión proactiva de los riesgos cibernéticos y de privacidad desde su concepción, seguido por los sectores de salud y tecnología, medios y telecomunicaciones.

Inclusión de una gestión proactiva de riesgos cibernéticos y privacidad desde su concepción, por industria



Fuente: Digital Trust Insights 2018, PwC.

El impacto financiero es revelador en el *Global Economic Crime and Fraud Survey 2018*, de PwC (GECS 2018), pues muestra que los ciberataques se han convertido en el fraude más disruptivo globalmente, donde el 14% de compañías encuestadas afirmó que ha perdido más de un millón de dólares (mdd), mientras que el 1% ha sufrido un menoscabo de más de 100 mdd. En este sentido, la disrupción de los procesos de negocio (30%) y la apropiación indebida de activos (24%) son los principales fraudes cometidos a través de ciberataques, con el malware (36%) y el phishing (33%) como los medios más comunes.[2]

En este reporte de *Digital Trust*, edición México, se revelan algunas de las más importantes percepciones de los negocios en materia de ciberseguridad y privacidad de datos en el último año, así como los nuevos riesgos asociados y las tendencias emergentes hacia un marco empresarial más resiliente.

[1] Digital Trust Insights 2018, PwC, https://www.pwc.com/us/en/services/consulting/assets/journey-to-digital-trust.pdf

[2] Global Economic Crime and Fraud Survey 2018, PwC, https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf

Riesgos inmediatos e incidencias

La tecnología será un aspecto fundamental en la reconfiguración de la definición del riesgo en el mundo. En el reporte del Foro Económico Mundial, *Global Risks Perception Survey 2019*, se confirma la latente preocupación acerca del fraude de datos o robo y los ciberataques, ocupando el cuarto y quinto lugares en términos de probabilidad. Se espera que las noticias falsas y el robo de identidad sean una amenaza creciente para este año, al igual que las intrusiones de privacidad hacia empresas y gobiernos.[3]

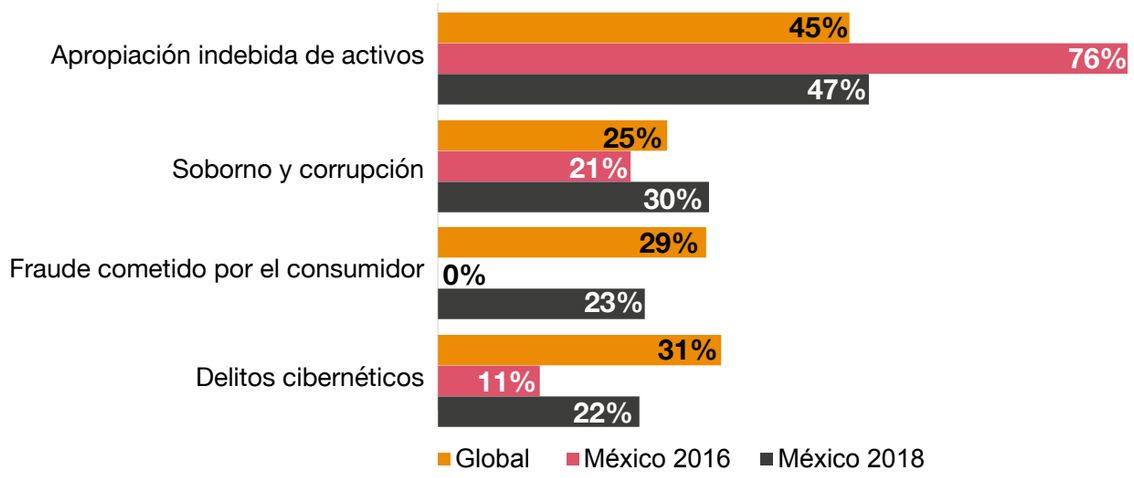
En 2018 se han dado brechas de información masivas, revelando vulnerabilidades en hardware; estos riesgos podrían potenciarse con el uso de la IA para perpetrar estos delitos. Asimismo, el impacto de los ataques podría afectar a tal grado la infraestructura de algún país que, en algunos casos, alcanzaría niveles de seguridad nacional.

En nuestro país, y de acuerdo con la edición México de la *Encuesta de Delitos Económicos 2018*,[4] de PwC (EDE 2018), se identifica un aumento en las incidencias en crímenes cibernéticos del 11% en 2016, al 22% en 2018.

Más aún, la EDE 2018 muestra que 15% de las empresas en México considera que experimentará un ataque cibernético en los próximos 24 meses. Al mismo tiempo, 56% indicó haber sido víctima de ciberataques por malware y phishing, con la interrupción de los procesos de negocios como el evento más frecuente (25%) tras una incursión cibernética.

Por su parte, la edición 22 de la *Encuesta Global de CEO*,[5] edición México, publicada en 2019, desvela que el 87% de los directores generales señala que al adoptar una nueva tecnología, su negocio maneja proactivamente los riesgos de ciberseguridad y privacidad, mientras que el 78% dice que su empresa es ciberresiliente.

Tipos de delitos económicos



Fuente: EDE 2018, de PwC.

[3] The Global Risks Report 2019, FEM, http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

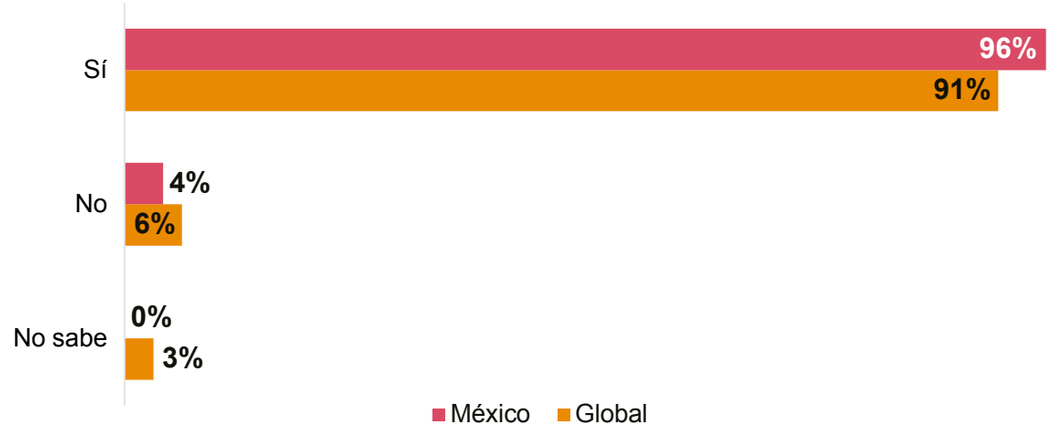
[4] Encuesta de Delitos Económicos 2018, edición México, PwC, https://www.pwc.com/mx/es/publicaciones/c2g/2018-04-13-encuesta-delitos-economicos-2018-mexicov4.pdf

[5] 22 Global CEO Survey, edición México, PwC, https://www.pwc.com/mx/es/archivo/2019/20190214-22ceosurvey-edicion-mexico.pdf?utm_source=Website&utm_medium=DescargaPDF

México, hacia un entorno más seguro y confiable

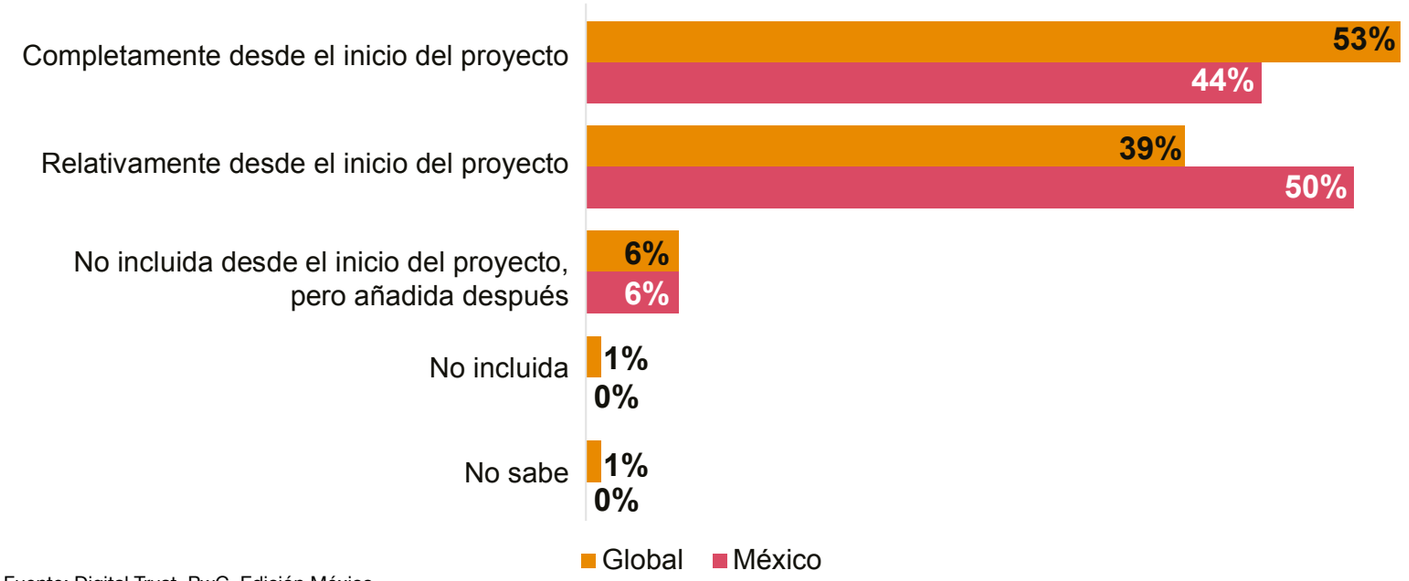
Entre los hallazgos de *Digital Trust*, edición México, se destaca que casi la mitad de los participantes (47%) indicó que una de sus mayores preocupaciones para su negocio es el cibercrimen. Con esta inquietud, las organizaciones mexicanas han impulsado proyectos de transformación digital, ya que los grupos de interés encargados (Consejo y C-Suite) han incluido personal de seguridad y privacidad en el 96% de los casos (91% globalmente), y el 44% (53% a nivel global) ha incluido una gestión proactiva de los riesgos cibernéticos y privacidad, por diseño, en el plan de proyecto y el presupuesto desde su concepción.

¿Los grupos de interés del proyecto incluyen personal de seguridad y/o privacidad?



Fuente: Digital Trust PwC. Edición México.

¿Hasta qué grado la gestión proactiva de riesgos cibernéticos y de privacidad es incluida, por diseño, en el plan de proyecto y el presupuesto?



Fuente: Digital Trust, PwC. Edición México.

Con respecto a las amenazas internas, el 40% de los encuestados mexicanos afirmó que su grado de preocupación ha permanecido igual en los últimos 12 meses, el 23% percibió un ligero aumento y solo el 7% cree que se ha incrementado considerablemente. En materia de cibercrimen, el 24% dice que se ha mantenido igual, el 36% afirma que se ha acrecentado ligeramente, y un 12% indica que se ha intensificado significativamente.

En lo que concierne a la pérdida (robo) de confidencialidad, el 28% (35% a nivel global) de las entidades mexicanas piensa que su nivel de preocupación se ha mantenido igual en los últimos 12 meses; tanto en México como globalmente, el 27% de los encuestados cree que se ha acrecentado ligeramente, y el 16% (17% a nivel global) en nuestro país dice que ha aumentado de manera importante.

Malware, phishing, ingeniería social y el retorno de inversión

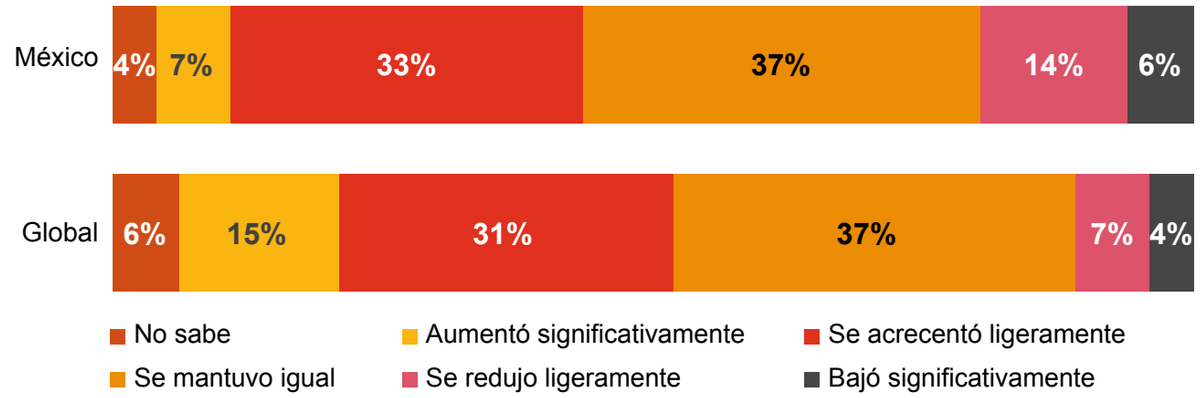
El dinamismo de los delitos cibernéticos y sus formas de impactar a la sociedad cambian constantemente, es decir, lo que ayer significaba un ataque por malware hoy podría haber mutado a intrusiones más sofisticadas. El phishing representa una de las maneras que más trastoca a las personas, ya que a través de diversos mecanismos de espionaje mediante aplicaciones o la pérdida del control físico de smartphones o computadoras, u otros tipos de ingeniería social, los cibercriminales podrían ganar acceso a dispositivos y a datos personales.

Por ejemplo, el malware si bien fue la mayor amenaza durante 2018 para dispositivos móviles, se cree que este pueda extenderse a un sinnúmero de formas más, principalmente para obtener mayores recursos a través de nuevas tácticas alineadas a cambios del mercado, por ejemplo, un menor peligro en la criptominería por la baja paulatina de las monedas virtuales.

Los ataques se han enfocado en los usuarios, más que en las tiendas o consorcios, utilizando el ransomware, el robo de identidad y otro tipo de engaños, principalmente al instalar aplicaciones o abrir enlaces.

En cuanto al phishing y a la ingeniería social, el 37% de participantes en *Digital Trust*, edición México, considera que el nivel de preocupación en los últimos 12 meses permaneció igual; otro 33% señaló que ha observado un ligero aumento, y un 7% ha percibido un incremento considerable.

Phishing/ingeniería social



Fuente: Digital Trust, PwC. Edición México.

Metodología

Digital Trust Insights, de PwC, anteriormente conocido como G*lobal State of Information Security Survey* (GSISS), contó con la participación de 3,000 líderes empresariales alrededor del mundo, como termómetro de la percepción en la preparación de las organizaciones para abordar el negocio digital, gestión de riesgo y los desafíos de cumplimiento. Para la elaboración de *Digital Trust*, edición México, fueron encuestados 177 líderes de negocio del país, pertenecientes a compañías de todos los tamaños, además de medianas y grandes empresas en sectores clave como servicios financieros, salud, productos industriales, productos de consumo, tecnología, medios y telecomunicaciones, y de energía, minería y servicios públicos.

pwc.com/mx/DigitalTrust

Contactos

Fernando Román
Socio Líder
Cybersecurity & Privacy Solutions
+52 (55) 5263 5898
fernando.roman@pwc.com

Yonathan Parada
Socio
Cybersecurity & Privacy Solutions
+52 (81) 8881 4106
yonathan.parada@pwc.com

El contenido de este documento es meramente informativo y de ninguna manera debe considerarse como una asesoría profesional, ni ser fuente para la toma de decisiones. En todo caso, deberán consultarse las disposiciones fiscales y legales, así como a un profesionista calificado.

©2019 PwC. Todos los derechos reservados. PwC se refiere a la red y/o una o más firmas miembro de PwC, cada una de las cuales constituye una entidad legal independiente. Para obtener mayor información consulta www.pwc.com/structure

Elaborado por Creative México: 553305-2019-pg-foll-digital-trust-mx