México: la seguridad como ventaja comercial en una economía en crecimiento

México es la segunda economía en América Latina[1] y la decimoquinta más grande del mundo.[2] Algunos expertos sugieren que el ritmo de crecimiento económico actual de México podría hacer que el país se convierta en una de las próximas grandes potencias mundiales.[3] Para atraer más inversión al país, especialmente de corporaciones multinacionales, México ha venido erigiendo una imagen de "tierra de la oportunidad".

Al mejorar la ciberseguridad, las empresas de México pueden ayudar a que los inversores internacionales se sientan más cómodos conduciendo negocios en el país. En particular, las pequeñas y medianas empresas (PYMES) que aumentan su sofisticación en términos de seguridad son más capaces de de competir y crecer. Pero las empresas de todos los tamaños en México deben hacer lo siguiente:

- Cambiar la percepción de que el delito cibernético afecta solo a organizaciones fuera de México.
- Desarrollar una estrategia de seguridad para la defensa ante amenazas en todas las etapas de ataque.
- Considerar a los posibles efectos de prácticas deficientes de ciberseguridad como oportunidades empresariales perdidas.

Conclusiones principales

En este informe, los expertos de Cisco en la materia analizan las capacidades de seguridad de las organizaciones en México con datos del estudio de parámetros de capacidades de seguridad 2015 de Cisco.[4] Por ejemplo, descubrimos que:

- Las PYMES de México tienen menos sofisticación de seguridad y menos defensas que las grandes empresas. Muchas PYMES creen que no son objetivos probables. Sin embargo, los atacantes apuntan a menudo las PYMES para obtener acceso a las redes de empresas más grandes.
- La mayoría de las grandes empresas y PYMES de México utiliza defensas que bloquean amenazas como firewalls. Sin embargo, pocas parecen invertir en tecnologías que aborden las infracciones a medida que ocurren o que ayuden a analizar la situación después de un ataque.
- La mayoría de los ejecutivos en México (69 por ciento) considera a la seguridad como de prioridad alta. Sin embargo, la falta de presupuesto es un importante obstáculo para la inversión en ciberseguridad para muchas empresas. La devaluación del peso[5] probablemente restrinja aún más los presupuestos a corto plazo, así que los ejecutivos deberán priorizar las inversiones en ciberseguridad.

---

[1] "Mexico: Country at a Glance" ("México: un vistazo al país"), Banco Mundial: http://www.worldbank.org/en/country/mexico.

[2] "Top 10 Things to Know About the Mexican Economy" ("10 aspectos principales que hay que saber sobre la economía mexicana"), por Peter Vanham, 5 de mayo de2015, Foro Económico Mundial: https://www.weforum.org/agenda/2015/05/top-10-things-to-know-about-the-mexican-economy/.

[3] "Mexico Could Be the Next Great Power" ("México podría ser la siguiente potencia mundial"), por George Friedman, Newsmax.com, 20 de marzo de 2016: http://www.newsmax.com/Finance/GeorgeFriedman/mexico-power-economy-invest/2016/03/29/id/721358/.

[4] Para obtener más información sobre este estudio y sobre los demás informes técnicos de esta serie, consulte las páginas finales de este documento.

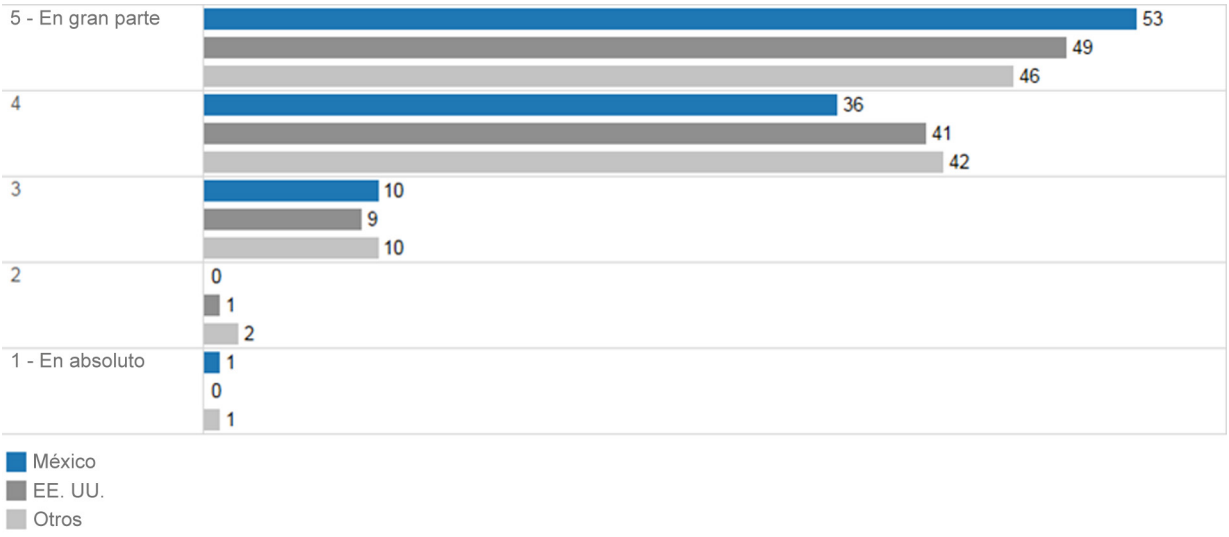
[5] "What's Behind the Volatility of Mexico's Peso?" ("¿Qué hay detrás de la volatilidad del peso mexicano?"), Knowledge@Wharton, 9 de marzo de 2016: http://knowledge.wharton.upenn.edu/article/whats-behind-the-volatility-of-mexicos-peso/.

Las mejoras en la seguridad son el resultado de infracciones que derivaron en las críticas de la opinión pública

Muchas empresas de México suponen que el país no es un objetivo para los ciberataques. Sin embargo, nuestros datos demuestran que el porcentaje de empresas de México (41 por ciento) que ha sufrido una infracción a la seguridad que generó críticas en la opinión pública es mayor que en el caso de la empresas de EE. UU. (33 por ciento).

De estas organizaciones de México, casi 9 de cada 10 reportan que una infracción pública a la seguridad las hizo fortalecer las defensas de seguridad. Más de la mitad afirma que las infracciones dieron lugar a mejoras en gran medida (Figura 1). Este hallazgo subraya una tendencia entre las empresas de México a tomar un enfoque reactivo con respecto a la seguridad.

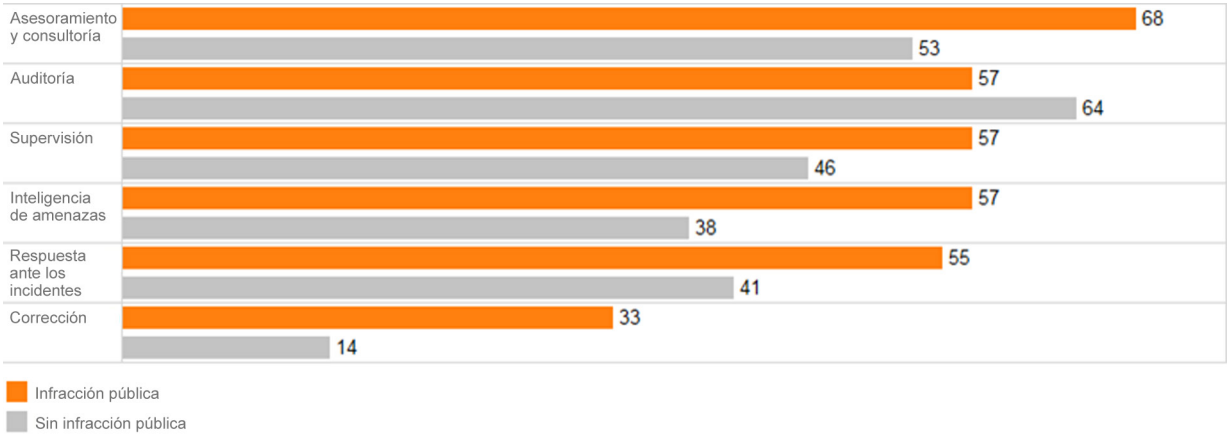
Figura 1. Porcentajes de las organizaciones que indican el grado en el que una infracción generó mejoras de seguridad



La mayoría de las organizaciones de México recurre a expertos externos para recibir orientación y apoyo después de una infracción pública. Es posible que la infracción pública hiciera que estas empresas se dieran cuenta de que estaban confiando en recursos inadecuados para administrar la seguridad. Por ejemplo, muchas PYMES de México dependen de una persona para administrar la TI y la seguridad de la empresa.

Descubrimos que el 68 por ciento de las organizaciones que sufrieron infracciones públicas a la seguridad recurrirá a recursos externos en busca de servicios de asesoría y de consulta. Un tercio informó que recurren a expertos externos para servicios de corrección. Solo el 14 por ciento de las organizaciones que no han sufrido una infracción pública a la seguridad lo hace (Figura 2).

Figura 2. Porcentajes de las organizaciones que externalizan servicios de seguridad, total o parcialmente, a otros proveedores

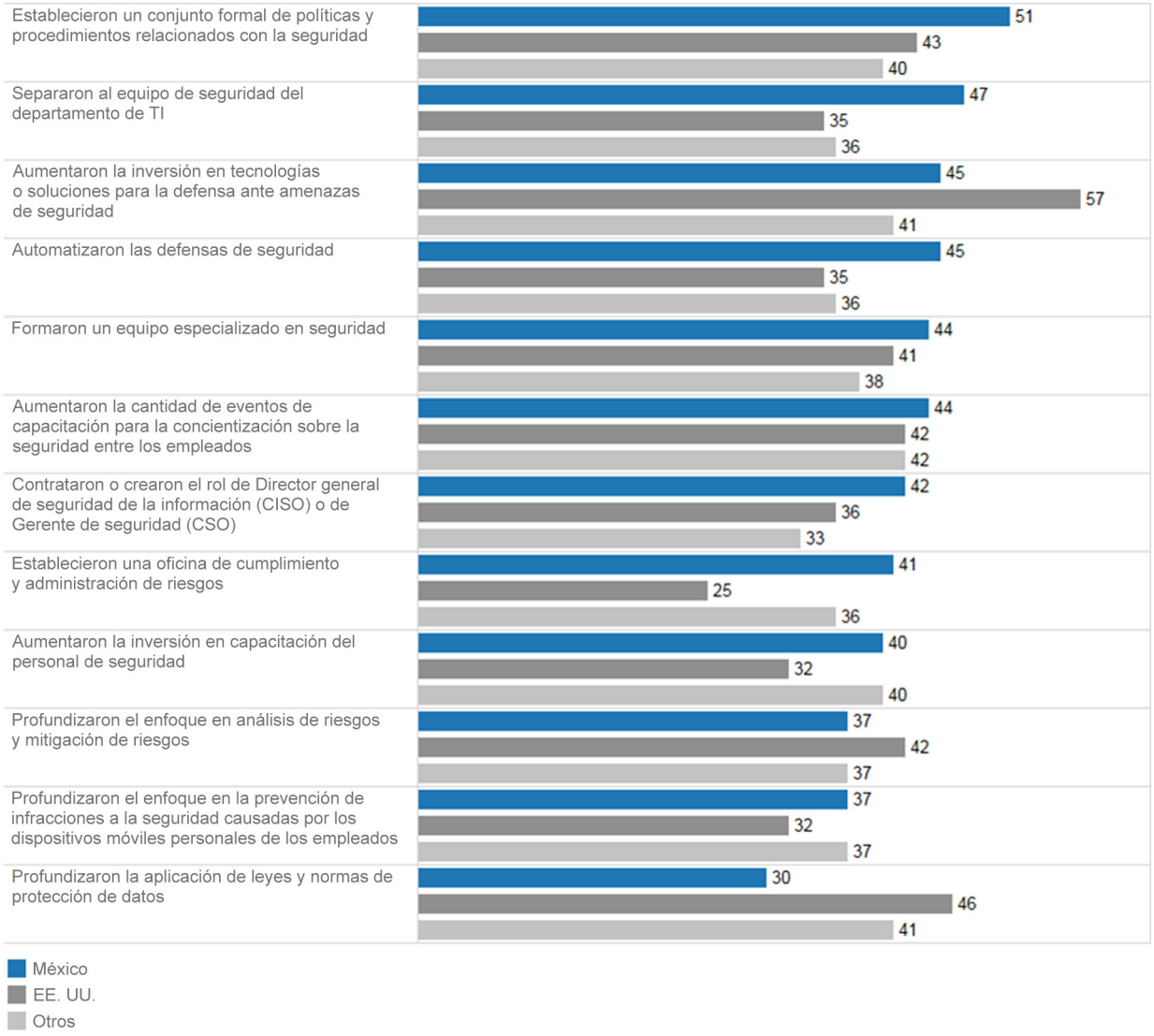


Las restricciones de presupuesto dificultan la inversión en tecnología de seguridad

En la Tabla 3 se muestran los tipos de mejoras que implementaron las organizaciones de México luego de sufrir una infracción pública. Algunos de los cambios principales citados por los encuestados son los siguientes:

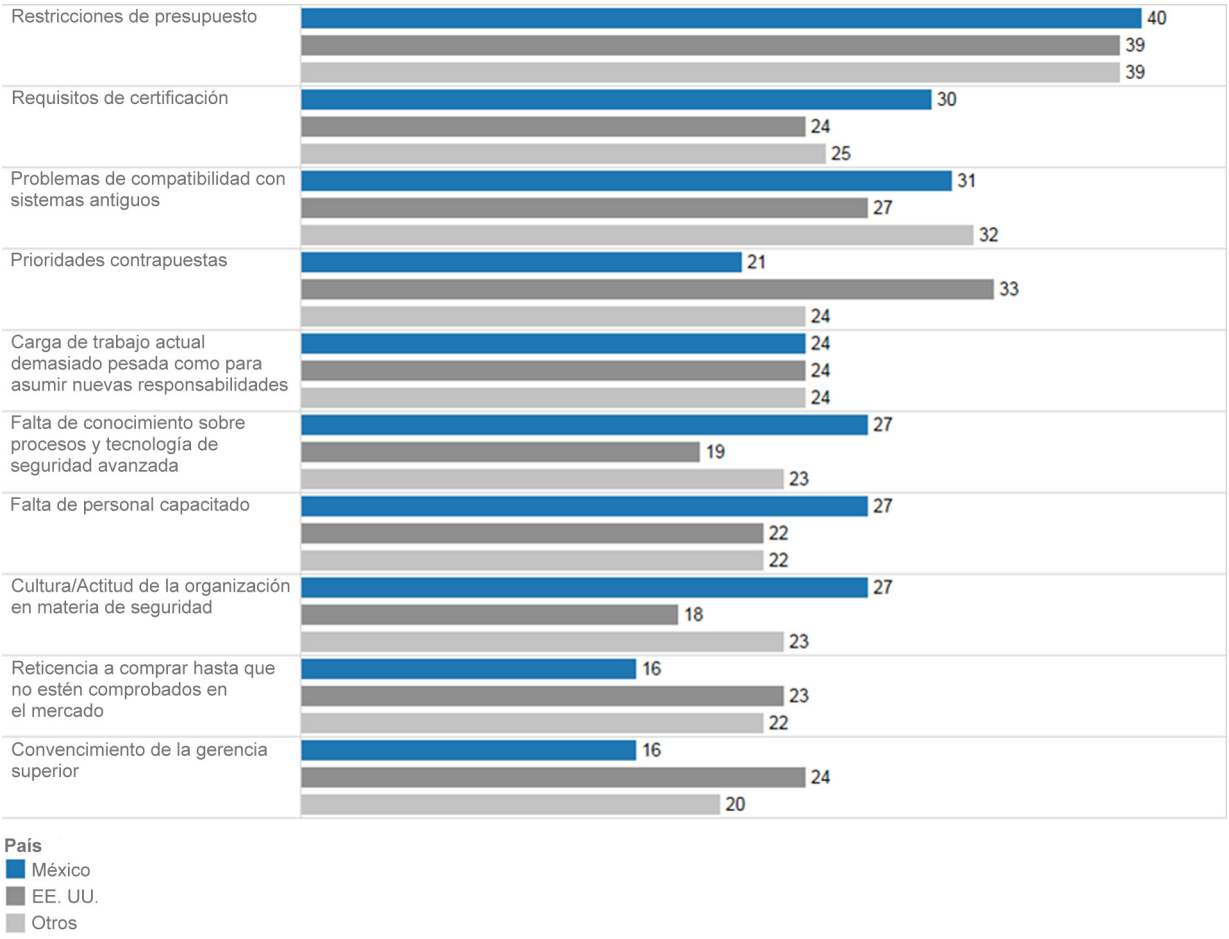
- Establecimiento de un conjunto formal de políticas y procedimientos de seguridad.
- Creación de un equipo de seguridad que está separado del departamento de TI.
- Automatización de defensas de seguridad.

Figura 3. Porcentajes de las organizaciones que informaron los tipos de mejoras realizadas para proteger contra otras infracciones



A pesar de la gran cantidad de mejoras, las organizaciones de México han aumentado su inversión en tecnologías o soluciones de defensa de seguridad luego de que una infracción pública en menor nivel que las empresas de EE. UU. La falta de presupuesto parece ser el obstáculo más grande a la inversión en ciberseguridad, no solo en México sino también en otros países (Figura 4). Sin embargo, las organizaciones deben considerar los mayores costos que podrían afrontar (financieros, entre otros) si sufren una infracción a la seguridad y son blanco de la crítica de la opinión pública.

Figura 4. Porcentajes de las organizaciones que informan obstáculos para adoptar procesos y tecnología de seguridad avanzados



Las restricciones de presupuesto probablemente sigan siendo una barrera para las inversiones en seguridad en México por algún tiempo. La devaluación del peso ha impulsado a muchas empresas del país a preocuparse aún más por los costos. Parecen financiar solo los proyectos de tecnología que garantizan la promoción del crecimiento comercial. Muchas aún no pueden incluir a la seguridad en esta categoría.

Las empresas de México tampoco están reconociendo la función de la seguridad como un factor que facilita del crecimiento. No reconocer esa verdad puede socavar su éxito a largo plazo. Esto es especialmente cierto para las PYMES, que representan una gran porción del ecosistema económico del país. Las pocas organizaciones de México que invierten adecuadamente en seguridad se están posicionando a la vanguardia de la competencia. Están mejor posicionadas para ganar la confianza de clientes cada vez más exigentes, especialmente compañías multinacionales que desean expandir sus operaciones en México.

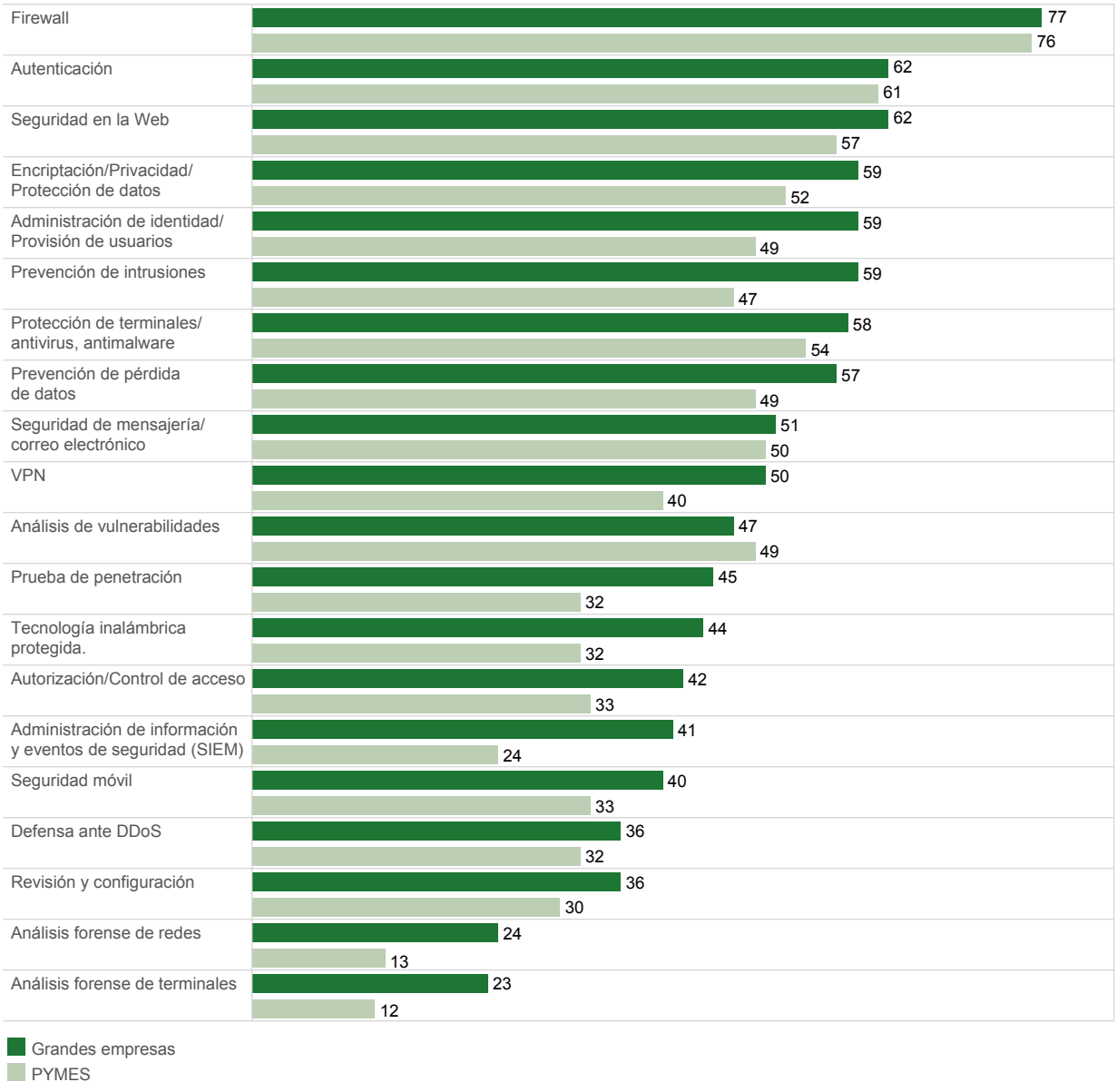
En un futuro cercano, las empresas más grandes probablemente exijan que sus proveedores, incluidas las PYMES, demuestren un alto nivel de seguridad. Las empresas que no puedan cumplir con estos requisitos corren el riesgo de quedar rezagadas en la floreciente economía de México.

La necesidad de contar con defensas contra amenazas de seguridad en todas las fases de un ataque

Las organizaciones de México no deben conformarse con herramientas como firewalls y soluciones antivirus que ayudan a bloquear amenazas. Cuando una amenaza evoluciona, no todas las infracciones pueden detenerse. Por lo tanto, las empresas deben mejorar su inversión en tecnologías para resolver las infracciones apenas ocurren. También deben agregar herramientas para analizar su entorno de TI luego de una infracción. Esta práctica permite la mejora continua de sus defensas.

Por ejemplo, más de tres cuartos de los encuestados, pertenecientes tanto a grandes empresas como a PYMES, informó que sus organizaciones utilizan firewalls. Pero solo un pequeño porcentaje de los encuestados parece utilizar tecnologías como investigación forense de la red e informática forense de terminales. Esas son herramientas esenciales para los equipos de seguridad "durante" y "después" de las fases de un ataque. De hecho, muy pocas PYMES parecen utilizar herramientas de detección y análisis (Figura 5).

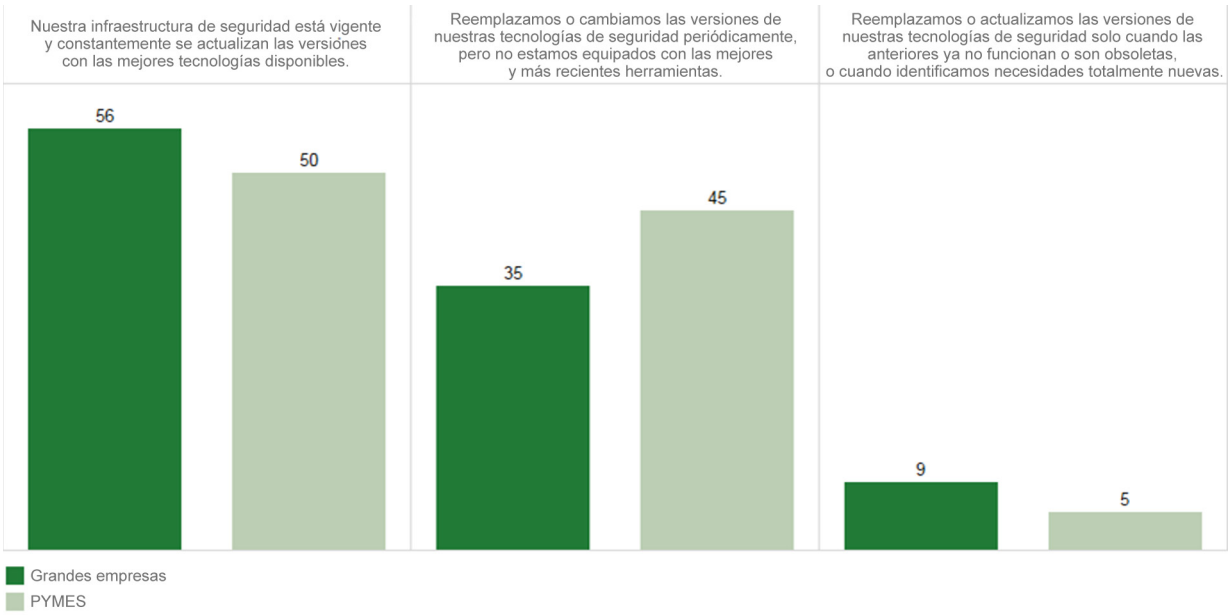
Figura 5. Porcentajes de grandes empresas y PYMES que utilizan diversas defensas contra amenazas de seguridad



Las PYMES de México utilizan menos tecnologías de seguridad que las grandes empresas. Pero las grandes empresas también deben extender el uso de estas tecnologías. Como se muestra en la Figura 5, más del 62 por ciento de las grandes empresas de México solo utiliza firewalls como tecnología de seguridad. En algunos casos, menos de un cuarto de las grandes empresas informó que utiliza una tecnología de seguridad determinada.

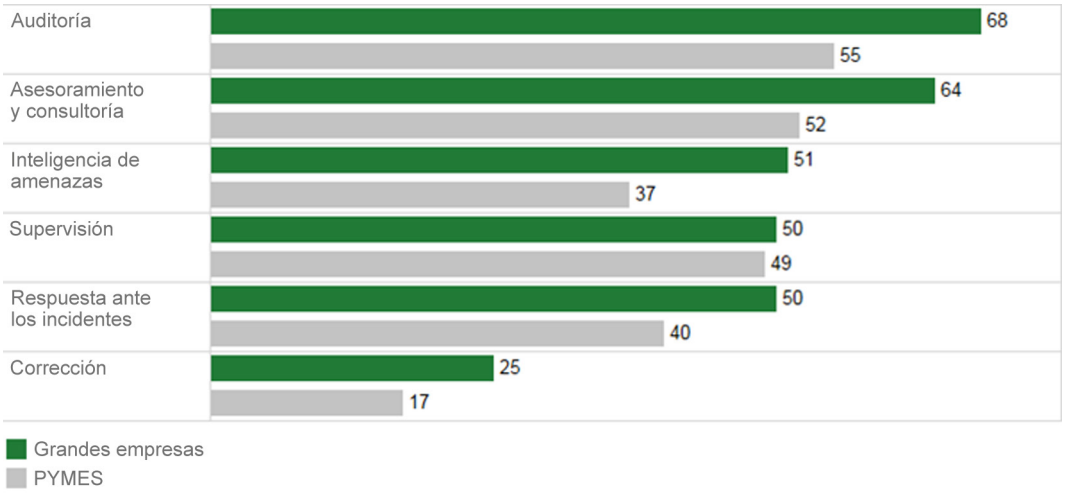
A pesar de no utilizar muchas tecnologías de seguridad, el 50 por ciento de las PYMES describió su infraestructura de seguridad como “muy vigente” y “en constante actualización con las mejores tecnologías disponibles” (Figura 6). El cincuenta seis por ciento de las grandes empresas reportó la misma evaluación positiva de su infraestructura de seguridad.

Figura 6. Porcentajes de las grandes empresas y PYMES que concuerda plenamente con las afirmaciones con respecto a su infraestructura de seguridad



Muchas empresas de México contratan servicios administrados para aumentar su nivel de sofisticación de seguridad. Las grandes empresas probablemente lo hagan más que las PYMES. Los servicios de auditoría (68 por ciento) y de asesoramiento y consultoría (64 por ciento) son los servicios que las grandes empresas usan con mayor frecuencia. (Consulte la Figura 7). La mitad de las grandes empresas que participaron en nuestro estudio también informó que dependen de terceros para proporcionar monitoreo, respuesta ante los incidentes o inteligencia de amenazas.

Figura 7. Porcentajes de las grandes empresas y PYMES que externalizan servicios de seguridad, total o parcialmente, a otros proveedores:



Secuela de una “tormenta perfecta” de debilidades de la seguridad

Claramente, muchas organizaciones de México tienen brechas en su seguridad. Una posible razón es que no piensan en elaborar una estrategia integral desde el principio. La falta de una estrategia, combinada con un enfoque reactivo a la seguridad y poca o ninguna inversión en defensas más sofisticadas, deja a las empresas vulnerables ante ataques e incapaces de responder adecuadamente ante un incidente.

Esta “tormenta perfecta” de debilidades de seguridad puede ser muy costosa. Un ejemplo: una empresa de México cuyo sitio web había sido atacado por hackers se puso en contacto con Cisco. Los atacantes iniciaron una campaña de denegación de servicio distribuido (DDoS) que dejó fuera de servicio el sitio web durante uno de los momentos de mayor movimiento del año de la empresa. El tiempo de inactividad durante ese período tuvo un efecto significativo en los ingresos.

Inicialmente, la empresa trató de bloquear el ataque varias veces de forma externa con defensas tradicionales de seguridad pero no tuvo éxito. Cuando los expertos en seguridad de Cisco investigaron el ataque de DDoS utilizando sus propios equipos, descubrieron que el ataque estaba empleando un amplificador interno que enviaba solicitudes y bloqueaba la red. Luego pudieron solucionar el ataque y ayudar a la empresa a recuperarse.

Conclusión: Es momento de mejorar la ciberseguridad

La mayoría de los ejecutivos de México (69 por ciento) considera a la seguridad como una alta prioridad. Sin embargo, esta postura no parece promover el nivel de inversión en ciberseguridad que necesita el país. El convencimiento de los ejecutivos es esencial para profundizar el apoyo (y el presupuesto) para las iniciativas de seguridad. Los directores de TI de la organización también deben trabajar en estrecha colaboración con los ejecutivos para ayudarles a comprender las deficiencias de seguridad y a priorizar las inversiones en seguridad.

Independientemente de su magnitud, todas las empresas de México deben:

- Reconocer que es posible que ya hayan sufrido alguna infracción. Admitir que simplemente es posible que no tengan las herramientas necesarias para detectar amenazas sofisticadas en su red.

- Adoptar un enfoque más dinámico e integral con respecto a la seguridad. Considerar el posible impacto comercial si la organización mantuviera su estado actual en términos de seguridad y sufriera una infracción de importancia. ¿La empresa perdería clientes? ¿Perdería ingresos? ¿Podría seguir funcionando?

- Determinar si la organización tiene suficientes recursos calificados internos para administrar actividades esenciales de seguridad. Si no, considerar la posibilidad de externalizar total o parcialmente ciertas responsabilidades a expertos externos.

- Priorizar la inversión en tecnologías de seguridad e implementar una estrategia de seguridad para que la organización pueda defenderse mejor contra amenazas en todas las etapas de un ataque: antes, durante y después.

Más información

Para obtener información sobre la cartera de productos y soluciones integrales para protección contra amenazas avanzadas de Cisco, visite www.cisco.com/go/security.

Acerca del estudio de parámetros de capacidades de seguridad 2015 de Cisco

En el estudio de parámetros de capacidades de seguridad 2015 de Cisco se examinan a los productos y soluciones contra amenazas en tres dimensiones: recursos, capacidades y sofisticación. El estudio incluye organizaciones pertenecientes a varios sectores en 12 países. En total, encuestamos a más de 2400 profesionales de seguridad, incluidos directores generales de seguridad de la información (CISO) y gerentes de operaciones de seguridad (SecOps). Encuestamos a profesionales en los siguientes países: Australia, Brasil, China, Francia, Alemania, India, Italia, Japón, México, Rusia, Reino Unido y Estados Unidos. Los países que participaron en la encuesta fueron seleccionados por su importancia económica y diversidad geográfica.

Para leer las conclusiones del estudio más general de parámetros de capacidades de seguridad de Cisco, consulte el Informe de seguridad anual 2016 de Cisco: www.cisco.com/go/asr2016.

Acerca de esta serie

Un equipo de expertos en diversos sectores y países de Cisco analizó el Estudio de parámetros de capacidades de seguridad 2015 de Cisco. Ofrecen una perspectiva específica en el panorama de la seguridad en 10 países y cuatro sectores (servicios financieros, salud, telecomunicaciones y transporte). En los informes técnicos de esta serie se destaca el panorama y los desafíos de seguridad que afrontan las organizaciones en términos de ciberseguridad. Este proceso ayudó a contextualizar las conclusiones del estudio y a focalizar la atención en los temas relevantes para cada país y sector que analizamos.

Acerca de Cisco

Cisco está desarrollando soluciones de seguridad verdaderamente eficaces integradas, automatizadas y fáciles de usar. Sobre la base de una presencia inigualable en el ámbito de redes, además de contar con los niveles más extensos y profundos de tecnologías y talentos del sector, Cisco ofrece el mejor grado posible de visibilidad y capacidad de respuesta para detectar más amenazas y corregirlas más rápidamente. Si recurren al área de Seguridad de Cisco, las empresas se ubican en una excelente posición para aprovechar de manera segura todas las ventajas de un nuevo mundo de oportunidades de negocios digitales.

Para obtener más información sobre el enfoque centrado en amenazas de Cisco, visite www.cisco.com/go/security.

Sede central en América
Cisco Systems, Inc.
San José. CA

Sede Central en Asia Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede Central en Europa
Cisco Systems International BV Amsterdam.
Países Bajos

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y de fax están disponibles en el sitio web de Cisco: **www.cisco.com/go/offices**.