MARSH | Microsoft

PERSPECTIVAS | SEPTIEMBRE 2019

Encuesta de Percepción del Riesgo Cibernético en Latinoamérica 2019

MARSH & McLENNAN COMPANIES

PERSPECTIVAS | SEPTIEMBRE 2019

Encuesta de Percepción del Riesgo Cibernético en Latinoamérica 2019

CONTENIDO

Introducción

La tecnología está transformando drásticamente el entorno empresarial global, con avances continuos en áreas que van desde la Inteligencia Artificial e Internet de las cosas (IoT) a una mayor disponibilidad de datos y blockchain. La velocidad a la que las tecnologías digitales evolucionan y rompen con los modelos comerciales tradicionales sigue aumentando. Al mismo tiempo, los riesgos cibernéticos parecen evolucionar aún más rápido.

El riesgo cibernético ha pasado del robo de datos y la preocupación por la privacidad a esquemas más sofisticados que pueden interrumpir la operación en empresas, industrias, cadenas de suministro y naciones, costándole a la economía miles de millones de dólares en cada sector. La dura realidad a la que las organizaciones deben enfrentarse es que el riesgo cibernético no puede eliminarse, por lo tanto, debe gestionarse a través de la identificación, mitigación y transferencia.

La Encuesta de Percepción del Riesgo Cibernético en Latinoamérica 2019 de Marsh y Microsoft (parte de una encuesta global) refleja el estado de las percepciones sobre el riesgo cibernético y la gestión del mismo en organizaciones de nuestra región, especialmente en el contexto de un entorno tecnológico empresarial en rápida evolución. Nuestros hallazgos se centran en cinco importantes conceptos que subrayan el estado del riesgo cibernético en el actual contexto empresarial:

1. En Latinoamérica y el Caribe (LAC), la preocupación de las empresas por el riesgo cibernético aumentó desde 2017, y a la par también se incrementó la confianza en sus capacidades para gestionarlo.

2. En general, y al igual que a nivel mundial, en nuestra región las organizaciones se centran más en tecnología y prevención que en priorizar el tiempo, recursos y actividades necesarias para construir una resiliencia cibernética.

3. A pesar de que poco más de un tercio de las empresas encuestadas dijeron que el riesgo cibernético casi nunca es una barrera para adoptar nuevas tecnologías, el 29% señaló que su nivel de percepción de riesgo asociado con estas tecnologías es muy alto.

4. La digitalización de las cadenas de suministro trae beneficios, pero muchas organizaciones no le dan la importancia a la interdependencia de responsabilidades dentro de la cadena de suministro, especialmente las grandes empresas.

5. Existe ambivalencia sobre el valor tanto de la legislación gubernamental como de las normas de la industria alrededor de la ciberseguridad. La mayoría de las compañías consideran que ambas tienen una efectividad limitada. Aun así, las empresas demandan una mayor implicación del Gobierno, y su apoyo para combatir las amenazas cibernéticas que provienen de gobiernos (locales e internacionales).

La Encuesta de Percepción del Riesgo Cibernético en Latinoamérica 2019 revela signos alentadores de mejora en la forma en que las organizaciones perciben y gestionan el riesgo cibernético. El riesgo cibernético es ahora, clara y firmemente, una prioridad en las agendas de riesgo corporativo, y vemos un cambio positivo hacia la adopción de una gestión más rigurosa e integral en diferentes áreas. Sin embargo, numerosas organizaciones siguen buscando la mejor forma de articular, abordar y actuar sobre el riesgo cibernético dentro de su marco general de riesgo empresarial, incluso cuando la marea del cambio tecnológico trae nuevas y no anticipadas preocupaciones.

Esperamos que este informe ayude a su empresa a navegar rápidamente el panorama en constante evolución del riesgo cibernético. Alentamos a todas las compañías a desarrollar estrategias de resiliencia cibernética, abordando este riesgo como una amenaza crítica que, con monitoreo y la aplicación de las mejores prácticas, puede ser gestionado con confianza. Finalmente, agradecemos a nuestros clientes y en general a aquellos que compartieron sus puntos de vista sobre este importante tema.

Aspectos destacados de la encuesta

La Encuesta de Percepción del Riesgo Cibernético en Latinoamérica 2019 de Marsh y Microsoft analiza cómo las organizaciones gestionan la creciente amenaza del riesgo cibernético, especialmente en un entorno empresarial altamente dinámico que está siendo transformado por la innovación tecnológica y la interdependencia. Los resultados de la encuesta muestran una mejora desde la edición de 2017, en varias áreas relacionadas con la sensibilización y las tácticas de las organizaciones para abordar el riesgo cibernético.

Prioridad vs Confianza

El riesgo cibernético se afianzó como una prioridad empresarial en Latinoamérica, con un 73% de organizaciones ubicando esta amenaza en el Top 5 de sus preocupaciones. Además, la confianza de las empresas en su capacidad de resiliencia frente al riesgo cibernético aumentó desde 2017. Sin embargo, un tercio de las organizaciones afirman no confiar en absoluto en su capacidad de resiliencia cibernética.

- El 73% de los encuestados en Latinoamérica clasificó el riesgo cibernético como una de las cinco principales preocupaciones para su organización, frente al 47% en 2017.
- El nivel de confianza de las empresas latinoamericanas en su capacidad para enfrentar el riesgo cibernético aumentó en comparación con 2017, en cada una de las tres áreas críticas de resiliencia cibernética:
  - De 16% a 22% para entender, evaluar y cuantificar las amenazas cibernéticas.
  - De 12% a 20% para prevenir y mitigar ataques cibernéticos.
  - De 7% a 18% para gestionar y recuperarse de ataques cibernéticos.

Nuevas tecnologías

La innovación tecnológica es vital para la mayoría de las empresas. Sin embargo, esto añade aún más complejidad al entorno tecnológico de una organización, incluido su riesgo cibernético.

- 79% de las empresas encuestadas dijeron que han adoptado o están considerando usar una nueva tecnología.
- 49% mencionó que el riesgo cibernético casi nunca es una barrera para la adopción de nuevas tecnologías.
- El 28% considera que los beneficios de las nuevas tecnologías superan los potenciales riesgos para el negocio.
- 75% evalúa los riesgos cibernéticos antes de la adopción de nuevas tecnologías, mientras que el 25% asegura que evalúa los riesgos después de sufrir un ataque cibernético.

Cadena de suministro

La creciente interdependencia y digitalización de las cadenas de suministro conlleva un mayor riesgo cibernético para todas las partes. Sin embargo, muchas empresas no se perciben a sí mismas como amenazas para la cadena de suministro de la que son parte, y, por el contrario, piensan que están muy expuestas al riesgo cibernético de parte de sus proveedores.

  - El 34% dijo que el riesgo cibernético que representan sus socios y proveedores de la cadena de suministro para su organización es alto o muy alto.
  - Solo el 18% dijo que el riesgo cibernético que ellos mismos representan para su cadena de suministro es alto o muy alto.
- Los encuestados tienden a establecer estándares más rigurosos en sus organizaciones que los que le requieren a sus proveedores

Rol del Gobierno

Las organizaciones generalmente consideran que la regulación gubernamental y los estándares de la industria tienen una eficacia limitada para ayudar a gestionar el riesgo cibernético, con la notable excepción de los ataques generados por los propios gobiernos.

- 53% consideran que las políticas y regulaciones nacionales o internacionales sobre ciberseguridad son esenciales para que las empresas adopten mejores prácticas y se minimice el posible impacto negativo en el sector privado.
- 43% de las empresas consideran que los estándares de la industria, como ISO o NIST, contribuyen a la mejora de la ciberseguridad dentro de la empresa.

- 61% dijeron estar muy preocupadas por el potencial daño de los ciberataques generados por gobiernos. El 55% asegura que los gobiernos deberían hacer más para proteger a la empresa privada de este tipo de ataques.

Cultura de seguridad y resiliencia cibernética

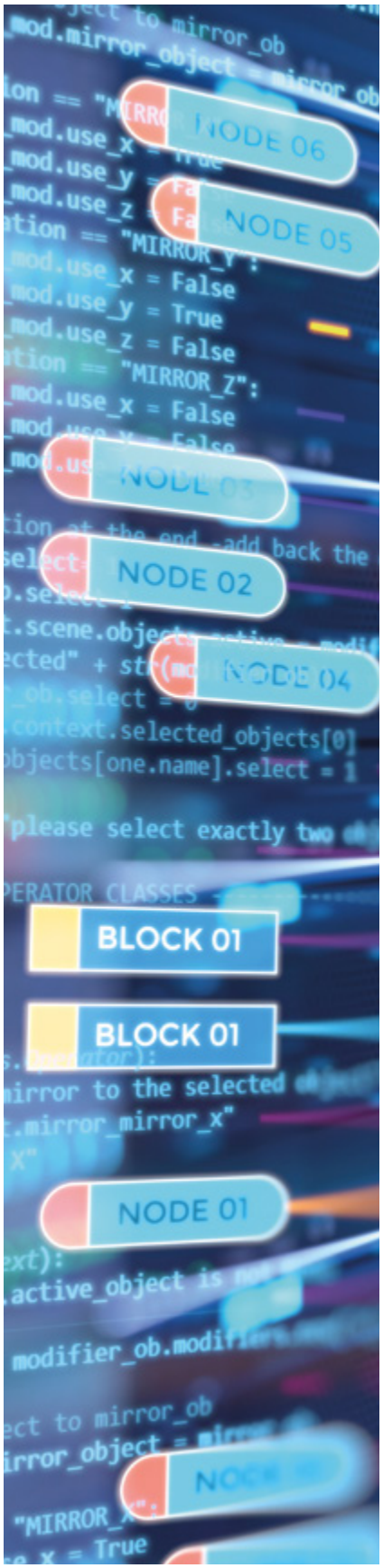
Muchas organizaciones están enfocando sus inversiones de ciberseguridad en herramientas tecnológicas de protección, descuidando otras áreas de gestión de riesgos que crean resiliencia cibernética, como la evaluación y transferencia de riesgos, así como la planificación de la respuesta en caso de un ataque.

- 88% de organizaciones dijeron que el área de TI/seguridad de la información es la principal responsable de la gestión del riesgo cibernético. Importante destacar el crecimiento de la figura del gerente de riesgos como pieza clave de la gestión del riesgo cibernético, que pasó del 17% en 2017 al 46% en 2019.
- 54% de la inversión en ciberseguridad de las empresas latinoamericanas para los próximos años se centra en tecnología y mitigación.
- 62% dijo que un ataque o incidente cibernético en su empresa sería el principal facilitador para incrementar la inversión en riesgos cibernéticos.
- 56% aseguran que la adopción de nuevas tecnologías ayudará a generar una mayor inversión en ciberseguridad.
- 33% de las organizaciones dijeron usar métodos cuantitativos para evaluar su exposición al riesgo, un aumento considerable con respecto al 8% de 2017.
- 81% ha fortalecido la seguridad de los sistemas y computadoras corporativas en los últimos dos años, pero solo el 28% ha llevado a cabo capacitaciones de gestión del riesgo cibernético, o simulaciones de escenarios de pérdidas.

Seguro cibernético

Las coberturas de seguros cibernéticos se están ampliando para hacer frente a las nuevas amenazas, y también la percepción empresarial sobre dichas coberturas.

- 29% de las empresas encuestadas cuentan con un seguro cibernético, frente al 47% de la media global.
- El porcentaje de empresas con seguro cibernético varía en función del tamaño de la organización: 40% con ingresos +US$1,000 M; 37% con ingresos entre US$1,000 y 100 M; y 22% con ingresos inferiores a US$100 M.
- 52% consideran que el seguro cibernético cubre todas o gran parte de las necesidades de su empresa. Sin embargo, el 39% declaran no saber si el seguro es una herramienta eficaz de protección.
- 75% de las empresas con seguro cibernético confían en que sus pólizas cubrirán el costo de un evento cibernético.



Riesgo cibernético: Prioridad vs Confianza

En Latinoamérica cada vez más compañías asumen el riesgo cibernético como una prioridad, y la confianza en su resiliencia cibernética aumentó. Sin embargo, una de cada tres empresas todavía no confía en absoluto en su capacidad de resiliencia.

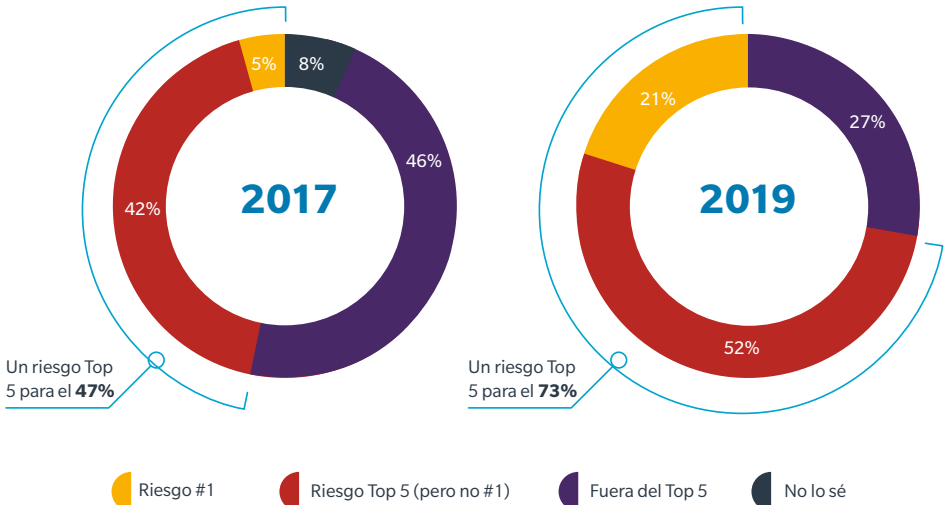
Aumenta la percepción del riesgo cibernético

Impulsados por la frecuencia y la gravedad de los incidentes de alto impacto, como el caso de *WannaCry* o *NotPetya* de 2017, los riesgos cibernéticos aumentaron significativamente su posicioamiento entre las principales prioridades de las organizaciones encuestadas en 2019 (ver gráfica 1). En Latinoamérica, 73% de las empresas clasificó el riesgo cibernético como una de las cinco principales preocupaciones para su organización, frente al 42% en 2017. El número de empresas que cita el riesgo cibernético como su preocupación número 1 se cuadruplicó en dos años, pasando del 5% al 21%.

GRÁFICA 1

El riesgo cibernético se consolida como priodidad en las agendas corporativas.

P. De las siguientes amenazas comerciales, clasifique las 5 principales que más preocupan a su empresa.



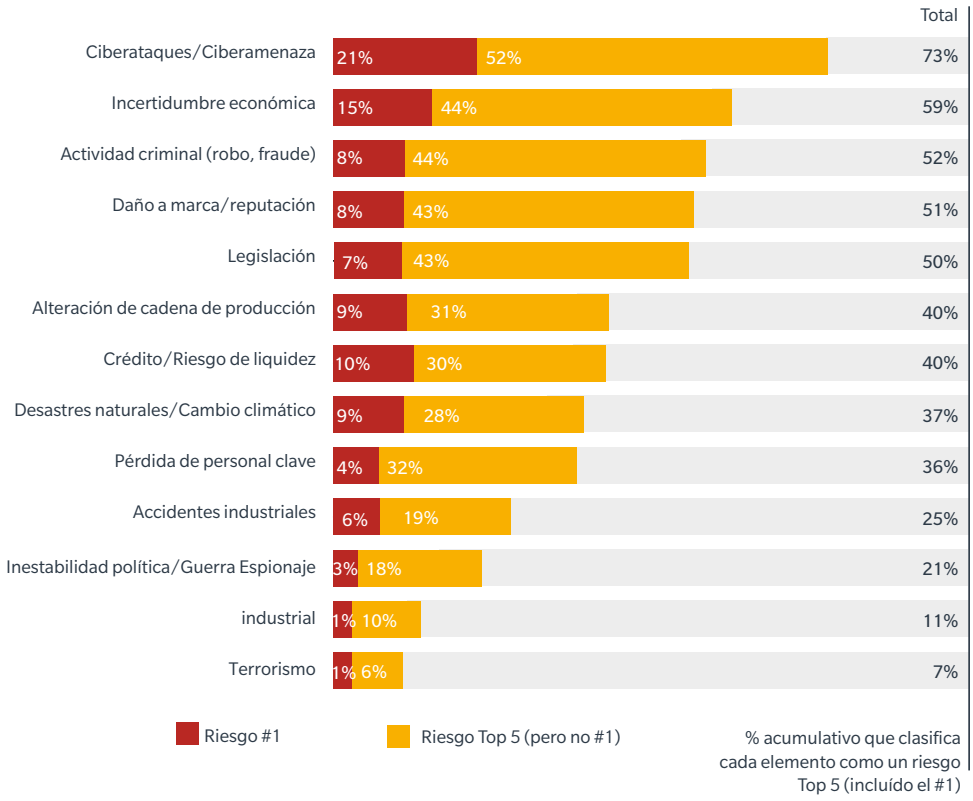
En 2019, más encuestados clasificaron el riesgo cibernético como una de sus principales preocupaciones en comparación con otros riesgos importantes del negocio (ver gráfica 2). La incertidumbre económica ocupó el segundo lugar del Top 5, con un 59%, 14 puntos porcentuales por debajo de los ataques y amenazas cibernéticas.

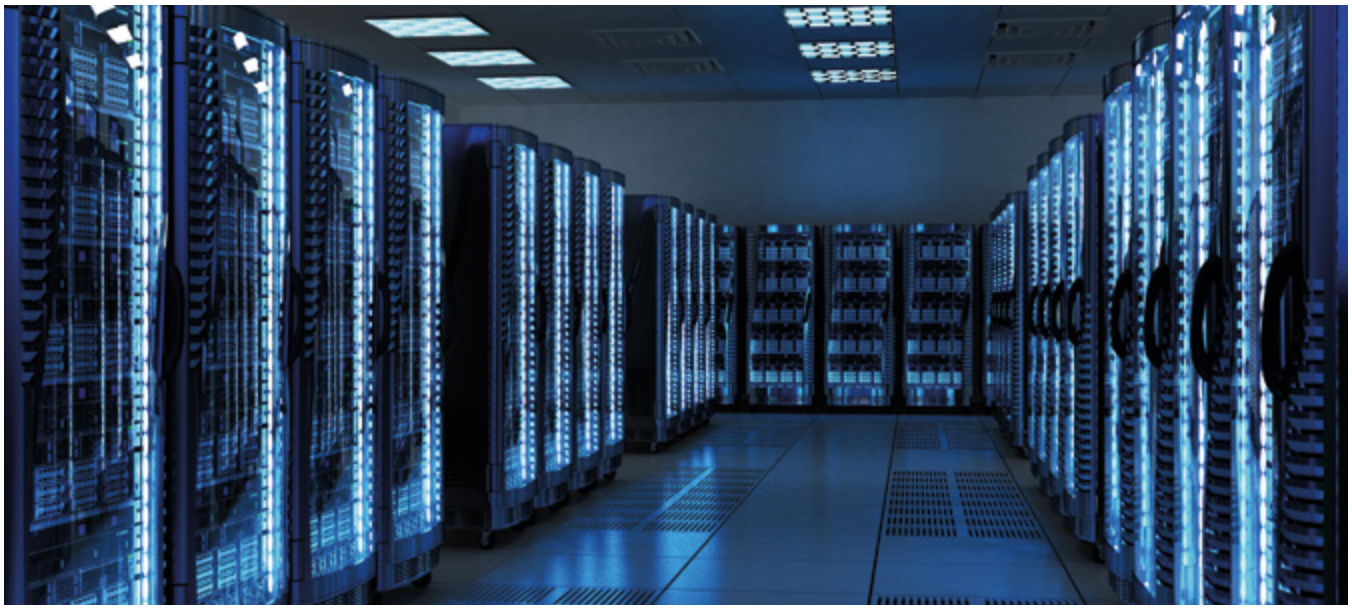
Estos resultados sugieren un fuerte aumento en la prominencia del riesgo cibernético, y se correlacionan fuertemente con otros estudios recientes. Por ejemplo, el Informe **Global de Riesgos 2019 del Foro Económico Mundial (WEF)** clasificó el robo de datos y los ataques cibernéticos entre los cinco riesgos más frecuentes a nivel global.

GRÁFICA 2

El riesgo cibernético supera a otros riesgos por un amplio margen.

De las siguientes amenazas, clasifique las 5 principales preocupaciones para su organización.





La confianza en la resiliencia cibernética aumenta

La encuesta de este año encontró un aumento en la confianza de las empresas en su capacidad para gestionar cada área crítica de resiliencia cibernética:

1. Comprender, evaluar y medir el posible riesgo cibernético. Identificar el tipo, probabilidad y potencial impacto económico de las amenazas a las que se exponen por el uso de tecnología y datos en sus operaciones.

2. Ser capaz de reducir la probabilidad de que ocurran ataques cibernéticos o prevenir posibles daños. Esto comprende una combinación de protecciones técnicas y no técnicas.

3. Gestión, respuesta y recuperación de ataques cibernéticos. Planes de contingencia claros y bien ensayados, y recursos fácilmente disponibles para minimizar las consecuencias negativas y el tiempo para recuperarse de un incidente.

En conjunto, estas áreas proporcionan una medida general de la resiliencia cibernética de una organización, es decir, de su capacidad para navegar con éxito un ataque cibernético; aplicar programas y actividades de planificación, evaluación, prevención, mitigación y respuesta para su correcta gestión; y volver a operar con normalidad, con un tiempo de inactividad o pérdidas mínimas. Esta clasificación se alinea con el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) para detectar, prevenir, responder y recuperarse.

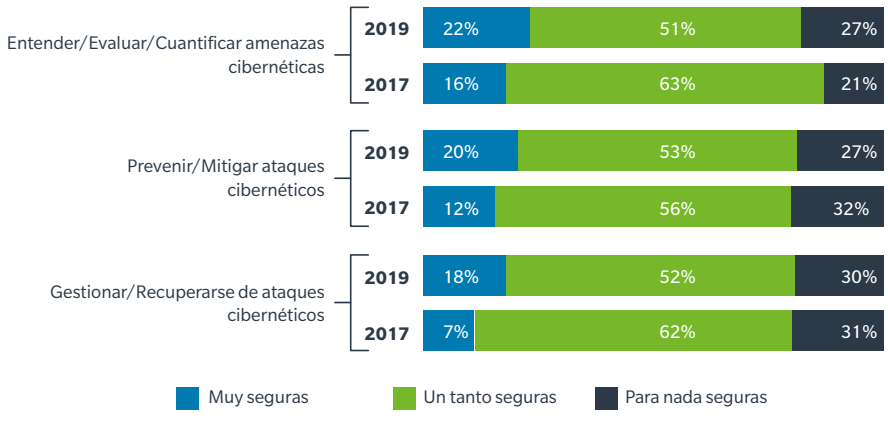
En 2019, la proporción de empresas que informaron sentirse confiadas o muy confiadas en su resiliencia cibernética fue del 73%. El incremento más significativo con respecto a 2017 fue el relacionado con la confianza en la gestión, respuesta y recuperación de un incidente cibernético, pasando del 7 al 18%.

Sin embargo, una de cada tres empresas dijo no confiar en absoluto en su capacidad de resiliencia en cada una de las tres áreas críticas. Esto refleja la necesidad de seguir trabajando en la detección, prevención, respuesta y recuperación de las amenazas/eventos cibernéticos.

Esta falta total de confianza puede deberse, en parte, a que las organizaciones todavía no consiguen tangibilizar el resultado de sus inversiones cada vez mayores en tecnología de seguridad cibernética: productos y servicios destinados a prevenir o mitigar los ciberataques. Se pronostica que el mercado de seguridad cibernética global superará los US$124 mil millones en 2019, pero a pesar del aumento del gasto en seguridad cibernética, el costo anual del delito cibernético en 2019 se estima en US$1,000 millones de millones.

GRÁFICA 3

La confianza en las medidas de resiliencia cibernética mejoró en 2019 vs 2017.



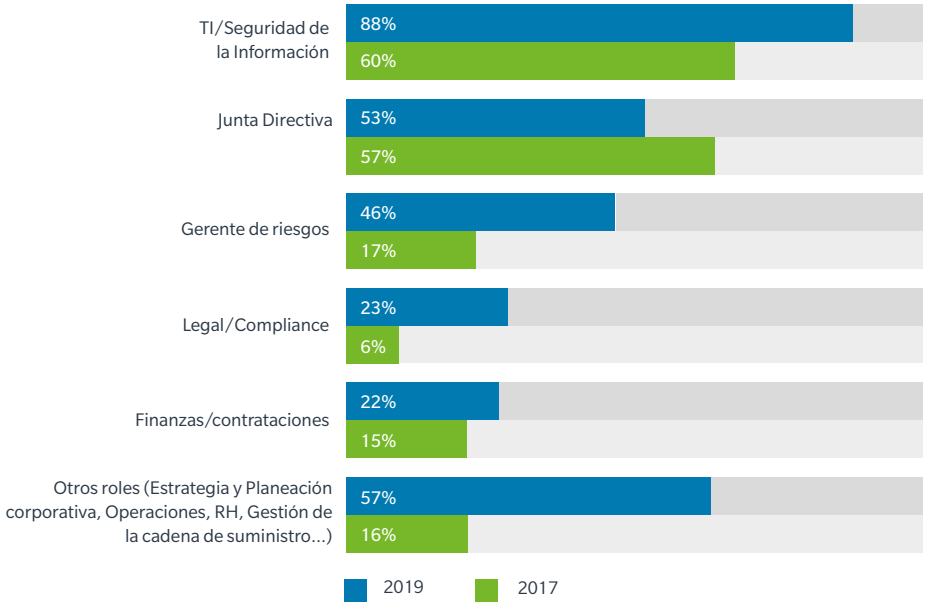
La responsabilidad cibernética aún se delega en gran medida al área de TI y Seguridad de la Información

La responsabilidad de la gestión del riesgo cibernético recae principalmente en el área de TI y Seguridad de la Información, y ha aumentado significativamente (28%) en los dos últimos años: 9 de cada 10 empresas identificaron esa área como el principal responsable del riesgo cibernético en 2019 (ver gráfica 4). Otro de los roles que también tuvo un incremento en cuanto a su nivel de responsabilidad dentro de la organización fue el gerente de riesgos, que pasó de un 17% en 2017 a un 46% en 2019. Este incremento indica una clara y positiva tendencia hacia un rol más destacado de los gerentes de riesgos. Sin embargo, sorprende que lejos de aumentar la responsabilidad de las Juntas Directivas, ésta haya disminuido un 4% desde 2017.

GRÁFICA 4

El equipo de TI sigue siendo el principal responsable de la gestión del riesgo cibernético en la mayoría de las empresas.

P: Clasifique las tres áreas que sean los principales responsables de la gestión del riesgo cibernético.



% que identifica cada función como uno de los principales responsables

Las nuevas tecnologías aumentan la exposición cibernética

Las empresas están adoptando la innovación tecnológica, y la mayoría no considera que el riesgo cibernético sea una barrera. Sin embargo, la evaluación del riesgo cibernético asociado a las nuevas tecnologías no es tan rigurosa y consistente como debería ser.

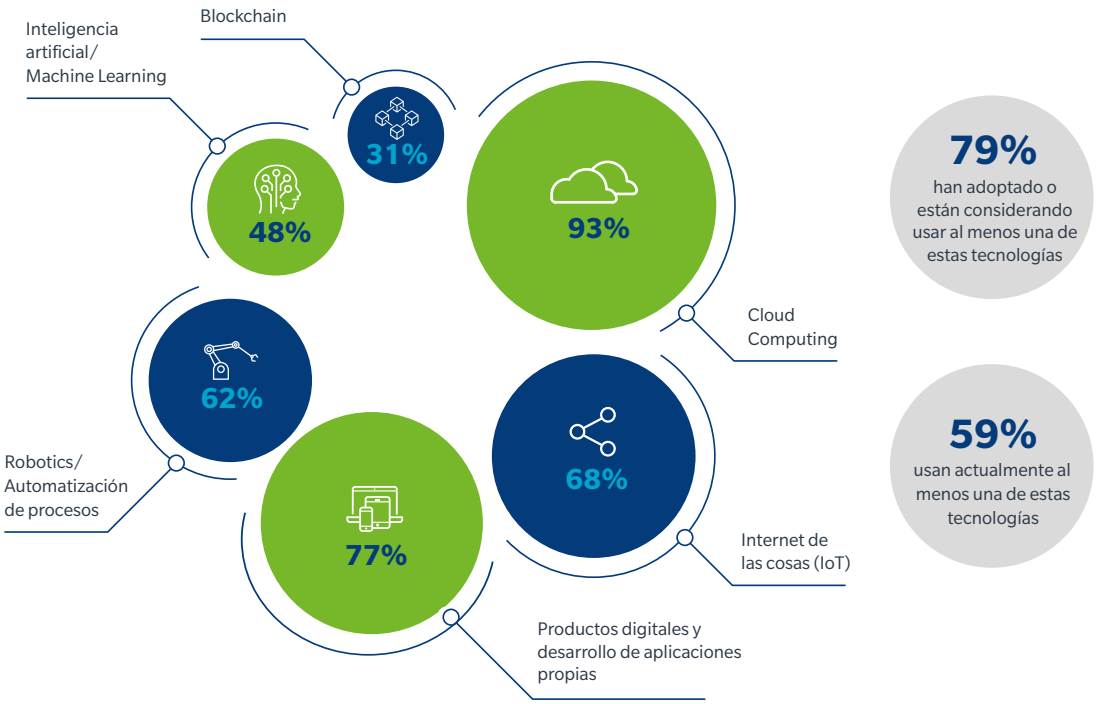
Se estima que para 2025 la cantidad de dispositivos conectados a internet a nivel mundial sea de 75 mil millones. A medida que el mundo se acerca a un "Internet de todo", aumenta la cantidad y variedad de activos digitales que las empresas almacenan, procesan y comparten. Incluso industrias tradicionales como la manufacturera esperan que casi el 50% de los productos que desarrollan sean "inteligentes" o" conectados" de alguna manera para 2020, abriendo nuevas fuentes de ingresos en servicios basados en datos.

Casi el 80% de los encuestados en 2019 aseguran que han implementado al menos una tecnología emergente (como Cloud, productos digitales y dispositivos conectados/IoT), o están considerando hacerlo (ver gráfica 5).

GRÁFICA 5

Una buena parte de empresas usan o están considerando usar nuevas tecnologías.

P: Para cada una de las siguientes tecnologías, indique cual de las siguientes se aplica mejor a su organización.



% de empresas que han adoptado o están probando/considerando cada tecnología.

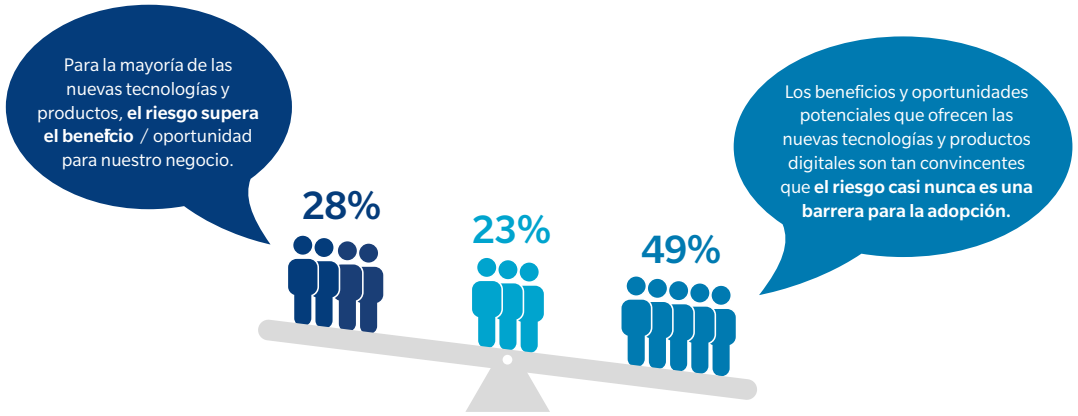
Los desafíos de seguridad pueden manifestarse cada vez que una nueva tecnología se integra en la infraestructura empresarial, lo que representa una nueva y adicional preocupación para la huella tecnológica de la organización. Los riesgos y exposiciones que presentan las nuevas tecnologías deben valorarse frente a los posibles beneficios para el negocio, y la tolerancia al riesgo varía según la industria y la empresa. A la pregunta de si los riesgos de adopción de nuevas tecnologías superan o no los potenciales beneficios, la mitad de los encuestados (49%) afirmó que el riesgo cibernético casi nunca es una barrera para la adopción de nuevas tecnologías (ver gráfica 6).

Sin embargo, un tercio de las empresas (28%) mencionaron que la mayoría de las nuevas tecnologías presentan riesgos que superan los posibles beneficios y oportunidades. Esta tendencia es mayor entre las empresas de menor tamaño (aquellas con ingresos anuales inferiores a US$100 millones), independientemente del sector.

GRÁFICA 6

En general, se considera que los posibles beneficios de las nuevas tecnologías superan los riesgos potenciales.

P: Indique cuál de las siguientes dos declaraciones refleja mejor la actitud de su organización.



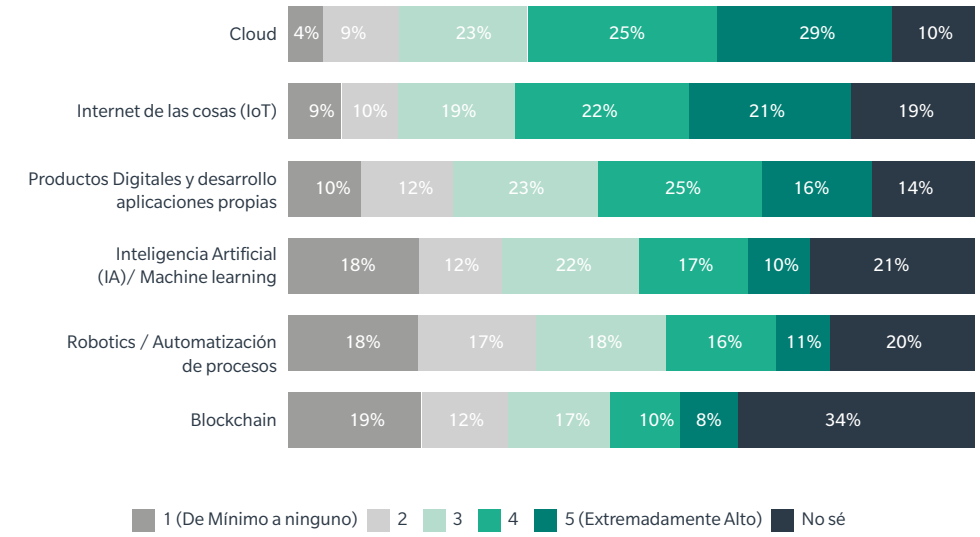
% de organizaciones que están de acuerdo con alguna de las declaraciones.

A pesar de la inclinación por tecnologías nuevas y emergentes, existe incertidumbre sobre el nivel de riesgo asociado con estas tecnologías (ver gráfica 7). A la pregunta sobre el nivel de riesgo cibernético asociado con estas nuevas tecnologías, la nube informática obtuvo la menor cantidad de respuestas relacionadas a la opción "no sé" (10%), en tanto que el blockchain obtuvo la más alta (34%). En el caso de nuevos productos digitales o aplicaciones digitales en desarrollo, las opiniones se dividieron en partes iguales: aquellos que percibieron un alto nivel de riesgo y aquellos que vieron un nivel menor. El más alto nivel de incertidumbre se relacionó con las nuevas tecnologías blockchain (34%) e inteligencia artificial (20%).

GRÁFICA 7

Muchos responsables de la toma de decisiones empresariales no están seguros del grado de riesgo que representan las nuevas tecnologías empresariales.

P: Califique el nivel de ciberriesgo percibido asociado con cada tecnología, en una escala de 5 puntos.



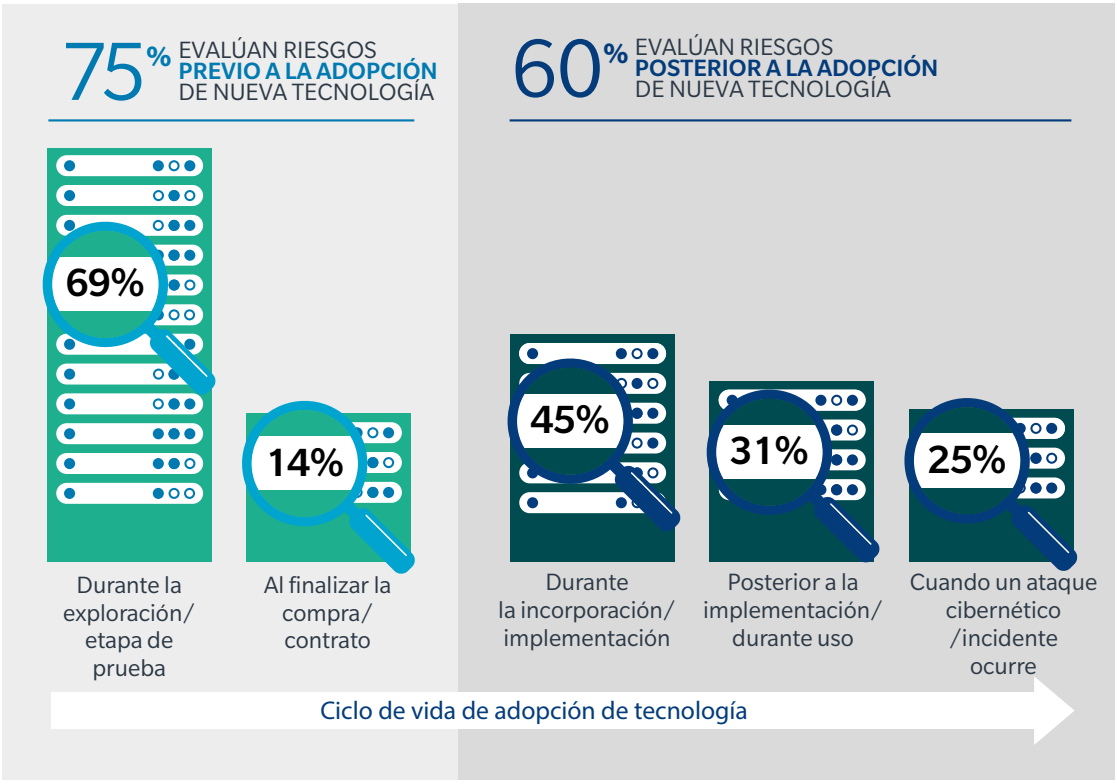
La mayoría de las empresas (75%) realizan evaluaciones del riesgo cibernético, bien en las etapas de exploración inicial y pruebas de las nuevas tecnologías que van a implementar en su organización, o al finalizar la compra de dicha tecnología. Un 60% llevan a cabo esta evaluación después de haber implementado la nueva tecnología, o cuando ocurre un evento/ataque cibernético (25%) (ver gráfico 8).

Casi la mitad de las empresas en Latinoamérica (42%) examinan los riesgos potenciales de una nueva tecnología antes y después de su implementación. Sin embargo, solo un 2% evalúa el riesgo cibernético a lo largo de todo el ciclo de vida de la tecnología, lo que incluye revisiones periódicas más allá de su etapa de adopción. Resulta precoupante que un 12% asegure que no realiza ningún tipo de evaluación del ciber riesgo, antes, durante o después de implementar una nueva tecnología.

GRÁFICA 8

El riesgo cibernético se evalúa más durante las etapas de exploración o pruebas de la nueva tecnología.

P: Cuando adopta e implementa nuevas tecnologías, como las que acaba de identificar, ¿en cuál de las siguientes etapas evalúa el riesgo cibernético?



42% evalúan los riesgos antes y después de la adopción

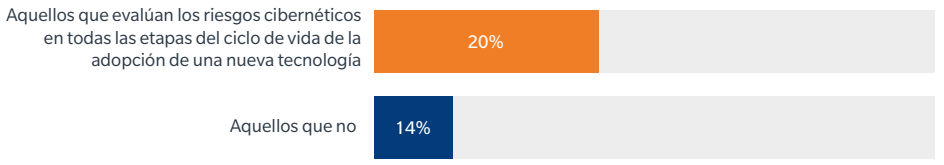
2% evalúan los riegos en todo el ciclo de vida de la tecnología

12% no evalúan en absoluto en ninguna etapa

El selecto grupo de empresas que evalúan el riesgo cibernético de forma continua a lo largo de todo el proceso de implementación de nuevas tecnologías confían más en sus capacidades para gestionar o responder a ataques cibernéticos (ver gráfica 9).

GRÁFICA 9

Las organizaciones que evalúan continuamente el riesgo cibernético de las nuevas tecnologías tienen más confianza en su ciberseguridad general.



% de los que reportaron mucha confianza en su capacidad de gestionar o responder a un ataque cibernético.

Las empresas que prueban los riesgos de la tecnología en múltiples etapas de implementación pueden sentirse mejor informadas porque la evaluación continua de riesgos proporciona visibilidad en tiempo real de riesgos y vulnerabilidades emergentes. Preparadas con un conocimiento oportuno de posibles debilidades o exposiciones de seguridad, están bien posicionadas para implementar mejoras en tiempo real y desarrollar planes de contingencia para gestionar los riesgos que involucran estos sistemas.

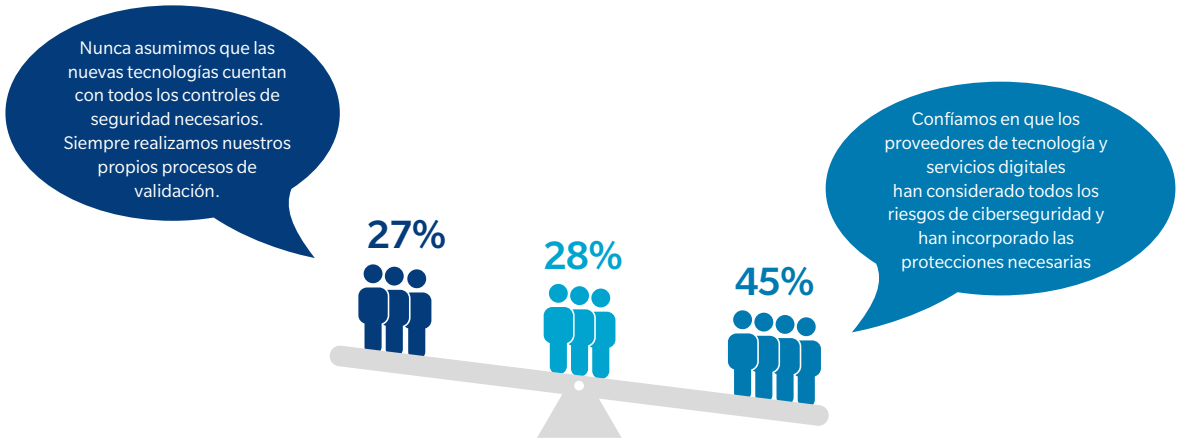
La evaluación del riesgo cibernético de nuevas tecnologías está muy asociada con la confianza que las organizaciones tienen, o carecen, de los proveedores que suministran estas tecnologías. Las tecnologías innovadoras no necesariamente deben representan una mayor exposición si son gestionadas adecuadamente. Algunas tecnologías pueden añadir nuevos riesgos si no se han implementado de acuerdo con estándares de seguridad óptimos, pero en muchos casos, la seguridad está integrada desde un inicio.

Un 45% de empresas en Latinoamérica asumen que sus proveedores tecnológicos han considerado todos los riesgos cibernéticos relevantes, y que no es necesario realizar más verificaciones. Por el contrario, tan solo un 27% asegura que "siempre realizan un procedimiento propio" para verificar las necesidades de seguridad y los controles que los proveedores implementan con respecto a las nuevas tecnologías (ver gráfica 10).

GRÁFICA 10

Casi la mitad de las empresas asume que los proveedores de tecnología han considerado todos los riesgos cibernéticos relevantes.

P: Indique cuál de las siguientes afirmaciones refleja mejor la actitud de su organización.



% de empresas que están de acuerdo con alguna de las afirmaciones.

Cada empresa deposita un cierto nivel de confianza en sus relaciones con sus proveedores y contratistas. Sin embargo, dada la importancia de las plataformas y servicios tecnológicos para los activos y operaciones centrales, debe asumirse una postura rigurosa de confianza y verificación que ayude a garantizar la validez y adecuación de las protecciones prometidas por terceros. Esta mayor vigilancia es especialmente importante cuando los nuevos procesos digitales son inherentes a los modelos de negocio de las empresas.

1/3 de los encuestados mencionó que su cadena de suministro representa un riesgo alto o considerable para su organización.

Riesgo en la cadena de suministro: hacia una responsabilidad social tecnológica

Con cadenas de suministro digitales cada vez más interdependientes, el riesgo cibernético debe convertirse en una responsabilidad colectiva

En un mundo en el que las cadenas de suministro están híper conectadas, existe una necesidad crítica de confianza entre socios, ya que la falta de confianza pone en serio riesgo el desempeño empresarial y la innovación. Toda organización necesita comprender, confiar y desempeñar un papel en la integridad y seguridad de los componentes y software de sus cadenas de suministro digital. El concepto de "responsabilidad social tecnológica" (el conocimiento y reconocimiento por parte de cada organización de su rol y obligaciones de seguridad cibernética dentro de la cadena de suministro) está ya en la agenda de muchos líderes de la industria.

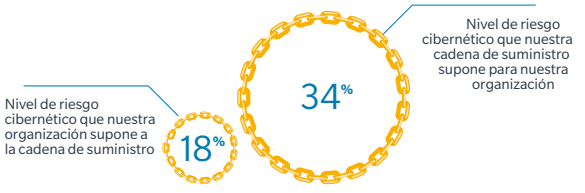
Sin embargo, aunque muchas organizaciones reconocen los riesgos potenciales que sus socios de la cadena de suministro pueden representar para su propia seguridad cibernética, la mayoría no visualiza el riesgo a la inversa. Hubo una notable discrepancia en la visión de muchas organizaciones con respecto al riesgo cibernético que enfrentan por los socios de la cadena de suministro, en comparación con el nivel de riesgo que su organización representa para sus contrapartes.

Uno de cada tres encuestados (34%) piensa que su cadena de suministro representa un riesgo alto para su organización (ver gráfica11). Al mismo tiempo, los encuestados mencionaron que existe el doble de probabilidad de que se materialice un riesgo en la cadena de suministro por culpa de terceros que por ellos mismos.

GRÁFICA 11

Muchas organizaciones están más preocupadas de que se materialice un riesgo en la cadena de suministro por terceros que por ellos mismos.

P: ¿Qué nivel de riesgo cibernético representa para su organización los terceros en la cadena de suministro? Y a la inversa: ¿qué nivel de riesgo representa su organización para la cadena de suministro?



% con respecto a cada riesgo como "alto" o "muy alto"

En general

25%

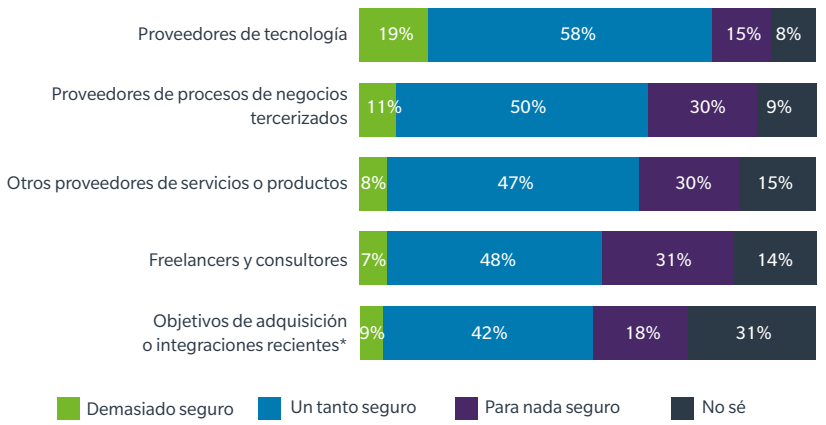
dijo "no confiar en absoluto" en su capacidad para prevenir las amenazas cibernéticas de al menos uno de sus socios externos.

La desconexión puede ser generada por la baja confianza de las organizaciones en sus habilidades para prevenir o mitigar el riesgo cibernético derivado de sus socios comerciales. El porcentaje de organizaciones que dijeron tener una "alta confianza" en mitigar las amenazas cibernéticas de sus socios de la cadena de suministro varió entre el 8% y el 19%, dependiendo del tipo de proveedor (ver gráfica12). En general, el 25% dijo "no confiar en absoluto" en su capacidad para prevenir las amenazas cibernéticas de al menos uno de sus proveedores.

GRÁFICA 12

Pocas empresas confían de verdad en su capacidad para gestionar el riesgo cibernético de terceros.

P: ¿Qué tan seguro está de la capacidad de su organización para prevenir/mitigar el riesgo cibernético de lo siguiente?



% de empresas que reportan diferentes niveles de confianza

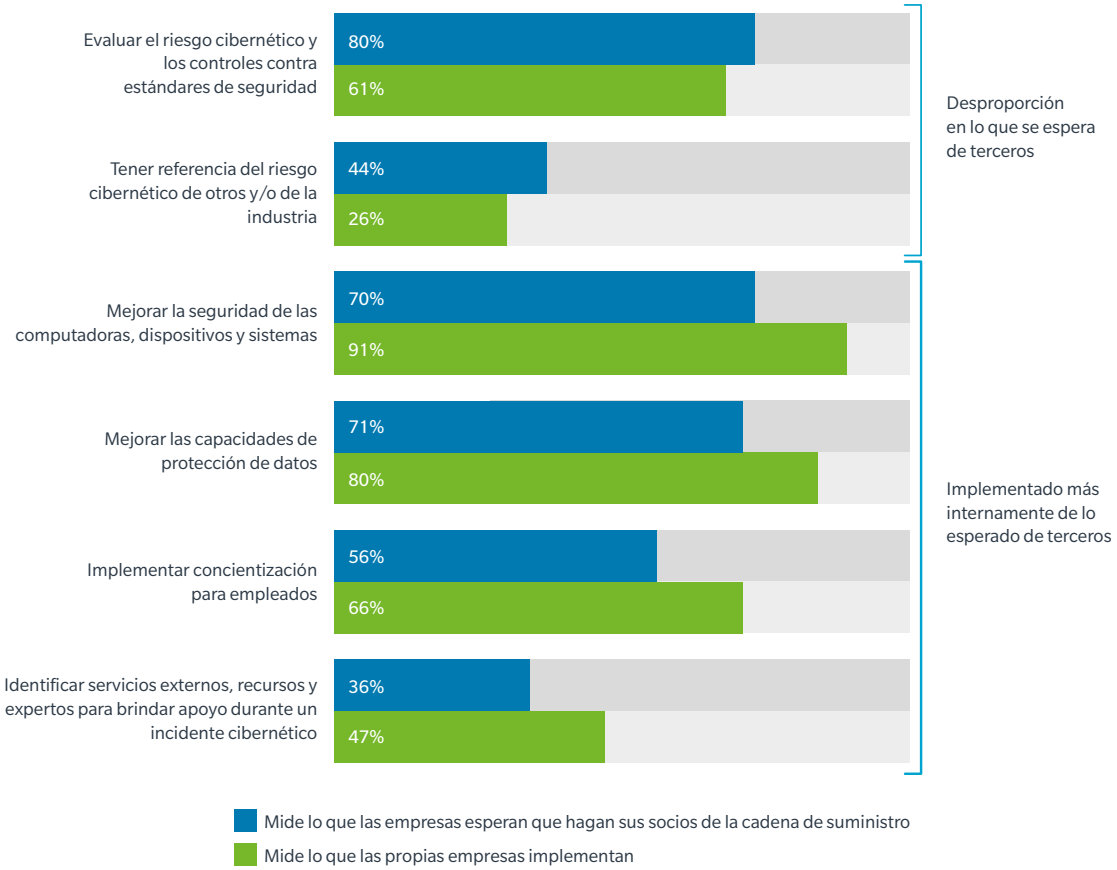
También hubo una disparidad entre las medidas y estándares de seguridad cibernética que las organizaciones se aplican a sí mismas, en comparación con las que esperan de sus proveedores (ver gráfica13). En general, los encuestados tenían más probabilidades de establecer medidas de gestión de riesgos cibernéticos más exigentes en su propia organización que para sus proveedores.

Por ejemplo, el 56% de las organizaciones dijeron que esperan que los proveedores en sus cadenas de suministro digital implementen medidas de concientización para sus empleados. Por su parte, el 66% de los encuestados dijo que su organización sí ha implementado tal requisito de manera interna. Dichas disparidades podrían llevar a las organizaciones a pensar que sus proveedores están menos preparados para gestionar el riesgo cibernético que ellos mismos, lo que disminuye la confianza de la organización en su cadena de suministro.

GRÁFICA
13

Existe una disparidad entre las medidas de ciberseguridad que las organizaciones esperan de sí mismas y las que esperan de terceros.

P: ¿Qué medidas de ciberseguridad espera que tomen sus socios / terceros de la cadena de suministro? Indique si su organización ha tomado las acciones específicas que se enumeran a continuación.



El rol del Gobierno genera opiniones encontradas

Las empresas ven una efectividad limitada de la regulación gubernamental para ayudar a gestionar el riesgo cibernético, pero desean recibir ayuda para gestionar los desafíos cibernéticos que no pueden abordar de manera efectiva por sí solas.

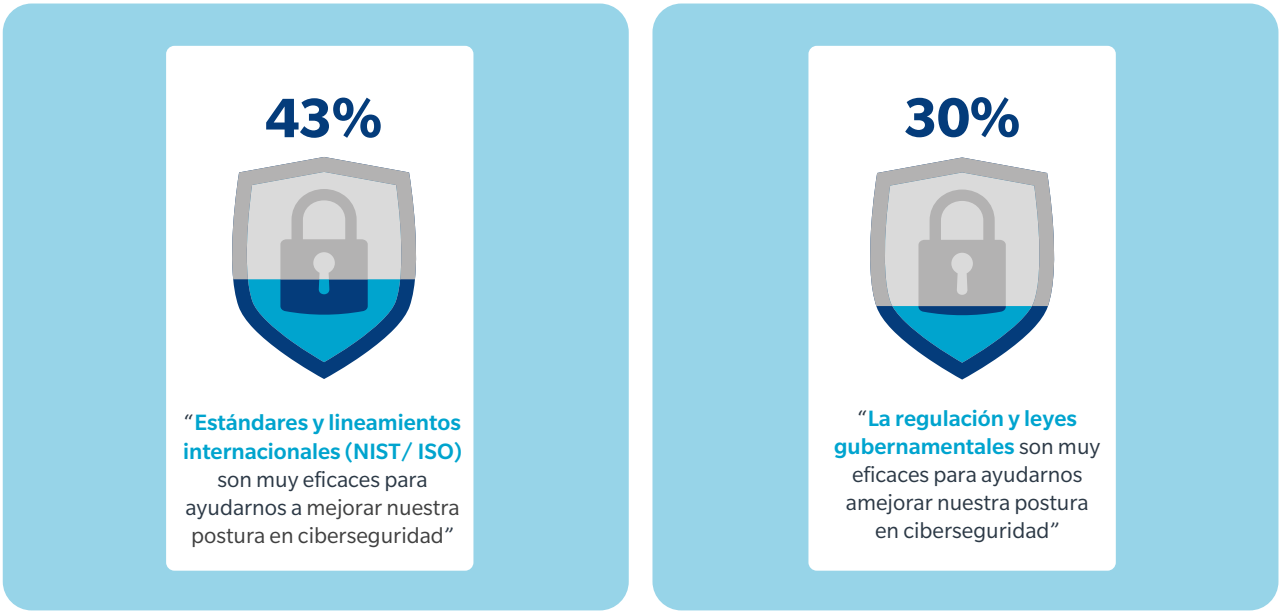
En los últimos años, los reguladores a nivel mundial han promulgado numerosas medidas para garantizar que las corporaciones y los ejecutivos sean más directamente responsables de una seguridad cibernética efectiva, y que los datos de los clientes estén protegidos. Muchas de estas regulaciones y marcos legales exigen un mayor grado de transparencia por parte de las organizaciones en el manejo de datos y en su preparación para la gestión del riesgo cibernético. El aumento de tales regulaciones complementa un conjunto de estándares de seguridad informática y cibernética, establecidos por reconocidos organismos internacionales como el NIST y la Organización Internacional de Normalización (ISO).

En general, las organizaciones de Latinoamérica consideran que los estándares internacionales de la industria, que pueden implementar en sus empresas de forma voluntaria, son más efectivos que las normativas gubernamentales para ayudarles a mejorar sus estrategias de ciberseguridad (43% vs 30%).

GRÁFICA 14

Menos de la mitad de las empresas en Latinoamérica consideran que las regulaciones gubernamentales o los lineamientos de la industria son efectivos para mejorar la ciberseguridad.

P: Para cada una de las siguientes declaraciones, indique qué opción refleja mejor las opiniones de su empresa.



El área principal de diferencia en la actitud hacia la regulación cibernética se relacionó con los ataques cibernéticos originados por los propios gobiernos, ya sean nacionales o extranjeros (ver gráfica15). En este contexto, una mayoría de los encuestados (61%) dijo estar muy preocupado por el impacto de este tipo de ciberataques.

De acuerdo a lo anterior, el 55% de las organizaciones dijo que es necesario que los gobiernos hagan más para proteger a la empresa privada de ciberataques originados por estos actores, algo que ocurre no solo en Latinoamérica, sino que es una constante a nivel mundial. Estos resultados muestran que, si bien las empresas generalmente prefieren un enfoque independiente para administrar sus asuntos de seguridad cibernética y riesgo cibernético, en lo relacionado a los ataques gubernamentales es una clara excepción.

GRÁFICA 15

Empresas que piden ayuda gubernamental para enfrentar ciberataques de gobiernos

P: Para cada una de las siguientes declaraciones, seleccione una o más opciones que reflejen las opiniones de su organización.

61%

"Estamos **muy preocupados** por el potencial daño que los **ciberataques de gobiernos** puedan causar a nuestra organización".

55%

"El gobierno **necesita hacer más** para ayudar a proteger al sector privado de **ciberataques de gobiernos".**

Cultura e inversión en seguridad y resiliencia cibernética

La gestión eficaz del riesgo cibernético requiere una evaluación cuantitativa del riesgo. Aunque cada vez más empresas miden este riesgo económicamente, queda un largo camino por recorrer para que todas las organizaciones adopten esta práctica, y utilicen esa cuantificación para tomar decisiones acertadas de inversión.

Las inversiones en tecnología de ciberseguridad están aumentando rápidamente y superando con creces el gasto en seguros cibernéticos. Se pronostica que el mercado global de seguros cibernéticos, medido por volumen de primas emitidas, será de aproximadamente US$8,000 millones en 2020, en comparación con un mercado global de ciberseguridad de US$124,000 millones.

Muchas organizaciones centran su estrategia de gestión del riesgo cibernético en la prevención, mediante la inversión en defensas cibernéticas tecnológicas de primera línea. Mientras tanto, el gasto en otras herramientas y recursos para la gestión del riesgo cibernético, como el seguro o la capacitación para la respuesta ante eventos o ataques cibernéticos, sigue siendo una fracción del presupuesto de tecnología. Esto sugiere que muchas organizaciones continúan creyendo que pueden eliminar o mitigar su riesgo cibernético a través de la tecnología, y no mediante una amplia gama de medidas de planificación, transferencia y respuesta.

Las mejores prácticas no requieren de una paridad del gasto, sino más bien de una estrategia de inversión que, reflejando el perfil de riesgo y las necesidades de una organización, aproveche los roles complementarios de la tecnología y los seguros para disuadir los ciberataques cuando sea posible, y transferir el riesgo de aquellos que no pueden evitarse. Sin embargo, el énfasis en el gasto en tecnología de ciberseguridad sobre otras medidas revela que muchas empresas aún no han aceptado esta verdad.

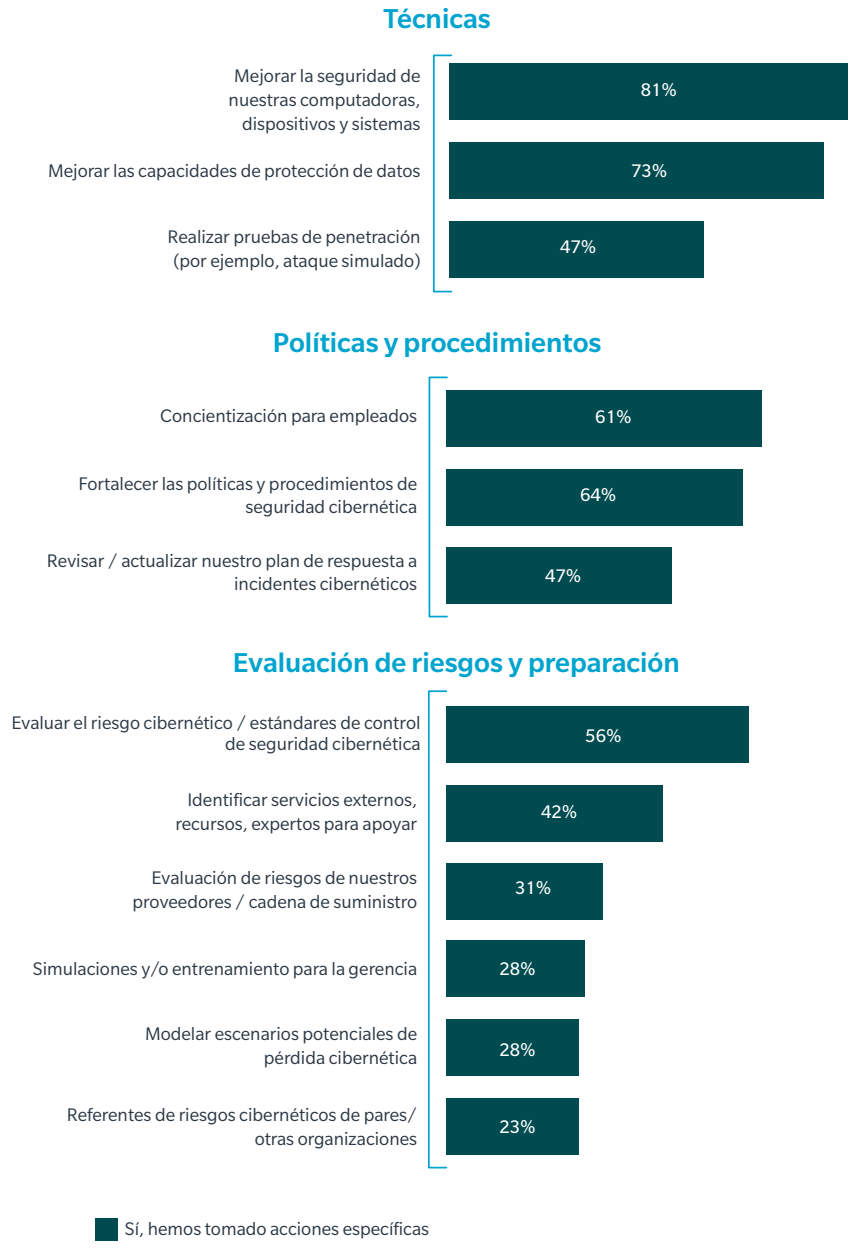
La gran mayoría de los encuestados aseguró que han implementado una o más mejoras técnicas en los últimos 12 a 24 meses (ver gráfica 16). Sin embargo, se tomaron menos iniciativas relacionadas con la capacitación/concienciación de los empleados, o con los planes de respuesta ante incidentes cibernéticos.

Por lo general, las acciones que menos realizaron las empresas en el último año fueron aquellas estrechamente relacionadas con la evaluación y modelado del riesgo cibernético. Resulta preocupante el hecho de que sólo un 28% declare haber trabajado en el modelaje de escenarios de pérdidas potenciales antes un ataque o siniestro cibernético, o en la capacitación de sus líderes.

GRÁFICA 16

Las acciones de resiliencia cibernética tienden a enfocarse en medidas técnicas.

P: Indique si su organización ha tomado las acciones que se enumeran a continuación en los últimos 12 / 24 meses.

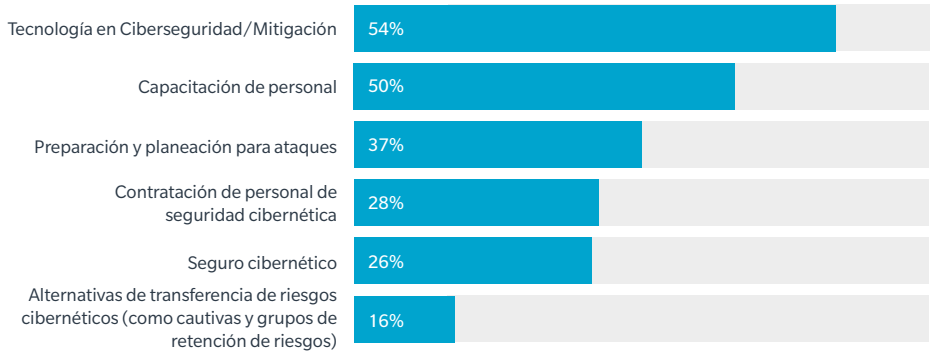


Mirando hacia el futuro, todo indica que estas tendencias continuarán. Entre las áreas en las que las empresas planean aumentar el gasto en gestión de riesgos en los próximos tres años, más de la mitad citó la tecnología/mitigación de seguridad cibernética, mucho más que en todas las demás áreas (ver gráfica 17). Sin embargo, resulta alentador que la capacitación sea una de las áreas en las que se planea mayor inversión.

GRÁFICA 17

Las inversiones en gestión de riesgos se centran en tecnologías de ciberseguridad y mitigación.

P: ¿Cómo espera que evolucionen sus inversiones en las siguientes áreas de gestión de riesgos en los próximos tres años?

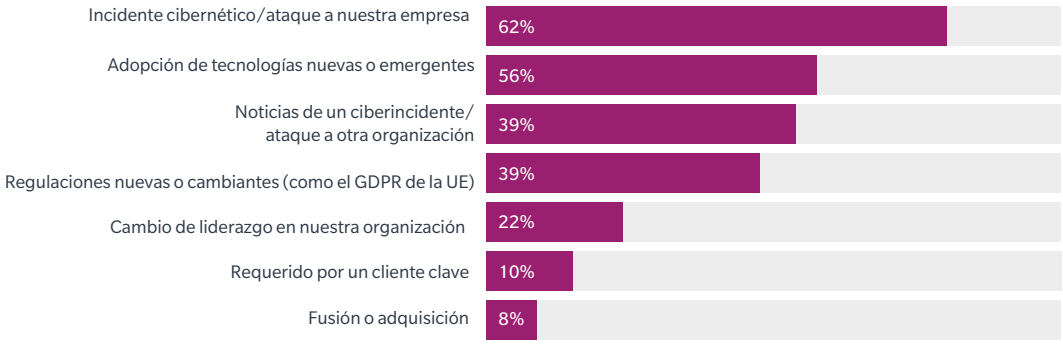


Si bien el incremento de la inversión en tecnología es una buena noticia, es preocupante el hecho de que este gasto no vaya acompañado de un aumento correspondiente en el uso de marcos económicos (como la cuantificación del riesgo cibernético) que permitan una mejora en la toma de decisiones informadas para la inversión. Es absolutamente crucial para las organizaciones poder medir la efectividad de la reducción del riesgo o permitir la comparación con otras inversiones corporativas de riesgo. De hecho, muchas organizaciones parecen tener una postura reactiva hacia el riesgo cibernético, ya que el factor más citado para aumentar la inversión fue que ocurra un incidente cibernético (ver gráfica 18). Mucho menos común fue que los líderes empresariales iniciaran proactivamente un nuevo enfoque en la inversión en riesgo cibernético.

GRÁFICA 18

Los incidentes cibernéticos son el principal detonante del aumento de la inversión en gestión del riesgo cibernético.

P: ¿Qué factor tendrá mayor impacto para que se incremente el presupuesto dedicado a las siguientes áreas de gestión del riesgo cibernético?

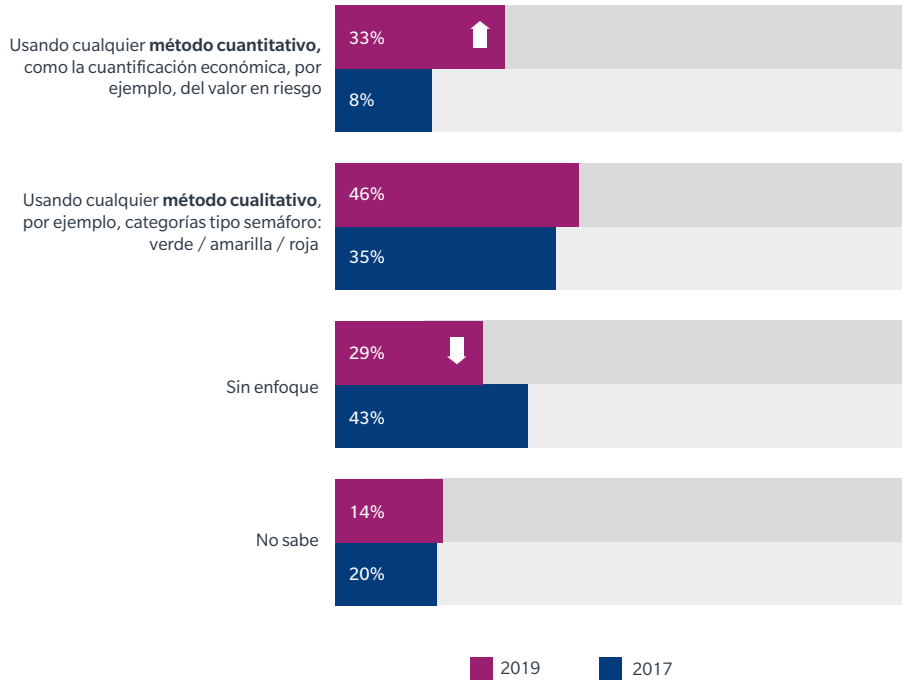


Resulta alentador comprobar que está avanzando el uso de métodos cuantitativos para expresar las exposiciones al riesgo cibernético en nuestra región (ver gráfica 19). La proporción de organizaciones de Latinoamérica que utilizaron dichos métodos se cuadriplicó desde 2017, del 8% al 33%. Sin embargo, todavía dos de cada tres empresas (67%) no los usa. Por otro lado, disminuyó la proporción de encuestados que dijeron no tener un enfoque para evaluar formal o sistemáticamente su exposición al riesgo cibernético: del 43% en 2017, al 29%. en 2019

GRÁFICA 19

La medición cuantitativa de la exposición al riesgo cibernético ha aumentado sustancialmente desde 2017, pero sigue siendo baja en general.

P: En general, ¿cómo mide o expresa su organización su exposición al riesgo cibernético?



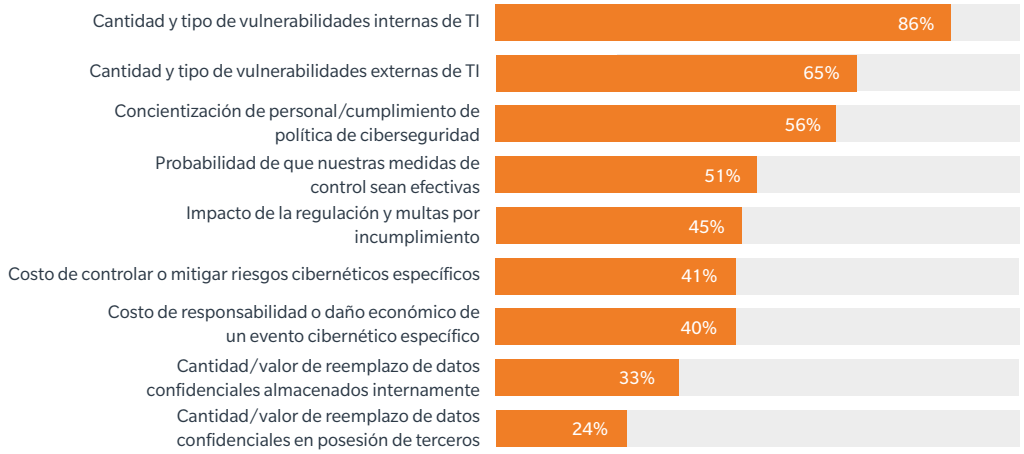
La mayoría de los encuestados en 2019 (67%) no expresan sus exposiciones al riesgo cibernético cuantitativamente ni tampoco usan datos cuantitativos para impulsar las decisiones de inversión. Esto puede deberse a la falta de experiencia en la organización con respecto a estas metodologías, a la falta de recursos (tiempo y dinero), o al hecho de que muchas compañías sigan considerando las amenazas cibernéticas como un problema tecnológico más que como un riesgo económico. Esta última posición está respaldada por el hecho de que más del doble de organizaciones evalúan el riesgo cibernético contando las vulnerabilidades de TI en comparación con las que evalúan los costos potenciales, multas y pérdidas (ver gráfica 20).

Al margen de cómo se exprese el riesgo cibernético, las áreas consideradas al realizar evaluaciones también varian ampliamente. Las organizaciones que realizan alguna forma de evaluación del riesgo cibernético tienden a centrarse en contabilizar las vulnerabilidades técnicas, en lugar de enfocarse en los costos de remediación o recuperación, multas u otras responsabilidades.

GRÁFICA 20

Los métodos de evaluación de riesgos se centran en las vulnerabilidades técnicas, pero no consideran adecuadamente los aspectos económicos de la exposición cibernética.

P: ¿Cuál de las siguientes opciones considera su organización en su evaluación/medición del riesgo cibernético?

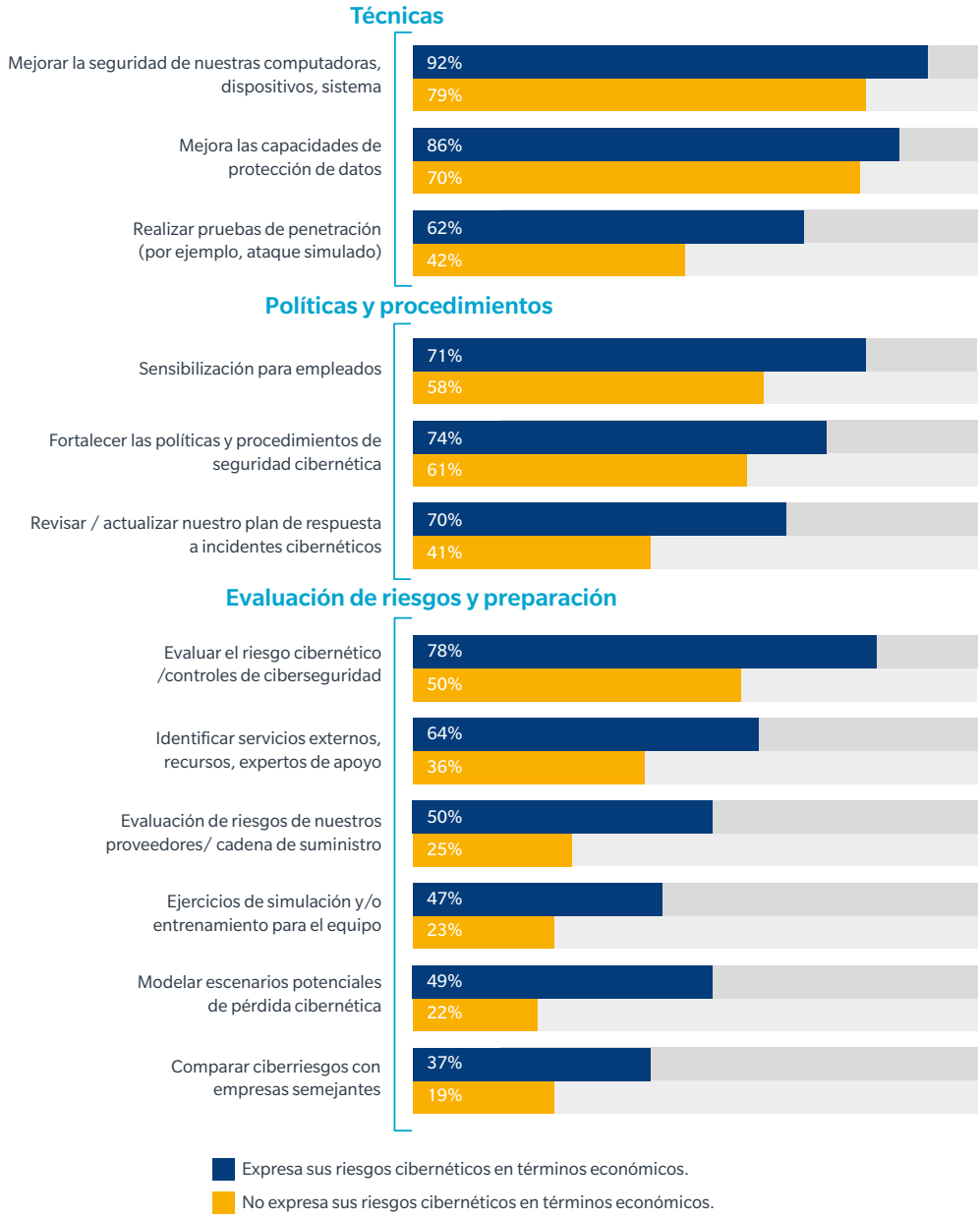


Las organizaciones que expresan su riesgo cibernético en términos económicos tienden a implementar en mayor medida una amplia gama de actividades de evaluación, planificación y capacitación que complementan las medidas técnicas, y que son esenciales para desarrollar la resiliencia cibernética (ver gráfica 21). Esto implica la transferencia de riesgos hacia el seguro, el establecimiento de procedimientos y políticas, y un enfoque integral para la evaluación de riesgos, incluida la evaluación de proveedores y cadenas de suministro.

GRÁFICA 21

Las empresas que realizan la cuantificación económica del riesgo cibernético tienen más probabilidades de equilibrar las acciones técnicas y no técnicas.

P: Indique si su organización ha tomado las acciones específicas que se enumeran a continuación en los últimos 12 a 24 meses.



Seguro cibernético

No todos los riesgos cibernéticos pueden mitigarse a través de la tecnología o las políticas corporativas. Las pérdidas generadas por eventos de baja frecuencia y alta intensidad pueden impactar de forma crítica las finanzas y operaciones de una organización. Por eso, la transferencia del riesgo a través de un seguro es esencial.

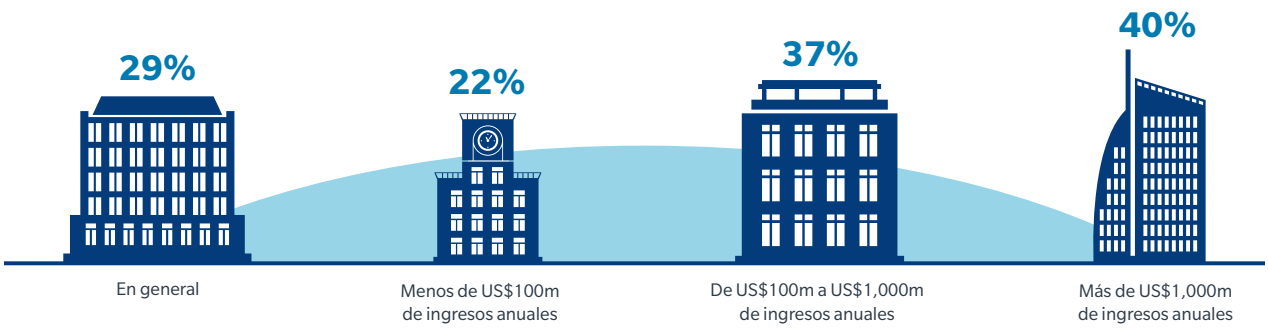
En Latinoamérica, el 29% de las empresas asegura contar con una cobertura de seguro cibernético (ver gráfica 22), frente al 47% de la media global. Sin embargo, este porcentaje varía en función del tamaño de la empresa: mientras que más de una tercera parte de las medianas (37%) y grandes (40%) organizaciones tienen este seguro, solo un 22% de las pequeñas lo compran. Igualmente, si comparamos estas cifras con las globales, nuestra región todavía está lejos de unos niveles óptimos de aseguramiento.

Las inversiones en tecnología de ciberseguridad están aumentando rápidamente y superando con creces el gasto en seguros cibernéticos. Se pronostica que el mercado global de estos seguros (medido en valor de primas emitidas), será de aproximadamente US$8,000 millones para 2020, en comparación con un mercado global de ciberseguridad de US$124,000 millones.

GRÁFICA 22

Las empresas medianas y grandes tienen más probabilidades de tener un ciberseguro

P: ¿Cuenta su organización con un seguro cibernético?

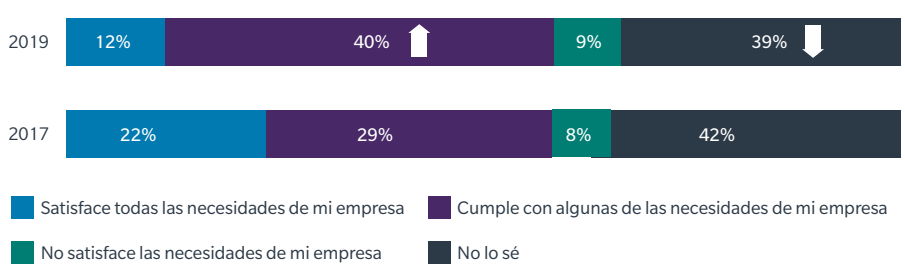


Desde 2017, la confianza de las empresas en la capacidad del seguro cibernético para protegerles de alguna manera contra las pérdidas de un siniestro aumentó (40% vs 29% en 2017). Sin embargo, si tomamos el conjunto de firmas que asegura que sus coberturas satisfacen todas o algunas de sus necesidades de protección cibernética, la confianza se mantiene estable (ver gráfica 23). El desafío para las aseguradoras a futuro es aumentar la confianza entre el sector empresarial de que el seguro cibernético puede satisfacer adecuadamente todas sus necesidades organizacionales, ya que este porcentaje disminuyó con respecto a 2017 (12% vs 22%).

GRÁFICA 23

La confianza en la capacidad del ciberseguro para satisfacer algunas de las necesidades de una organización creció.

P: Complete la oración seleccionando una de las siguientes opciones: El seguro cibernético disponible en el mercado actual ...

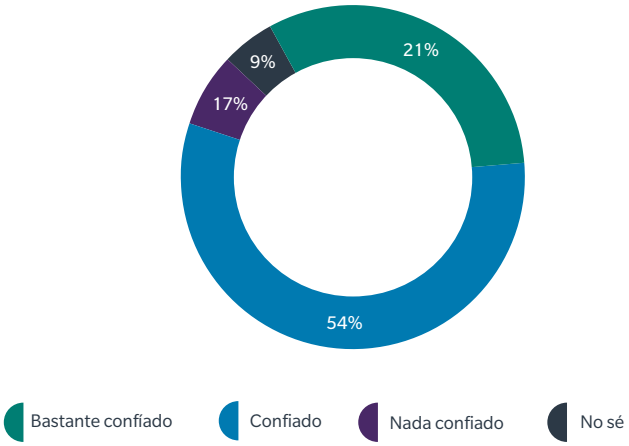


Una de cada cinco empresas (21%) dice estar muy confiada en la capacidad de respuesta de sus pólizas de seguro cibernético, lo que sumado a aquellas que se sienten razonablemente confiadas (54%), hace que podamos asegurar que la mayoría de organizaciones en Latinoamérica se sienten bien protegidas con sus actuales pólizas. Sin embargo, un 17% aseguró no confiar en esta capacidad de su seguro (ver gráfica 24).

GRÁFICA 24

El 75% de las organizaciones confían en que sus pólizas de seguro cubrirán los costos de un siniestro cibernético.

P: ¿Qué tan seguro está de que las coberturas dentro del programa de seguros de su organización (pólizas cibernéticas u otras) cubrirán los costos en caso de un evento cibernético?



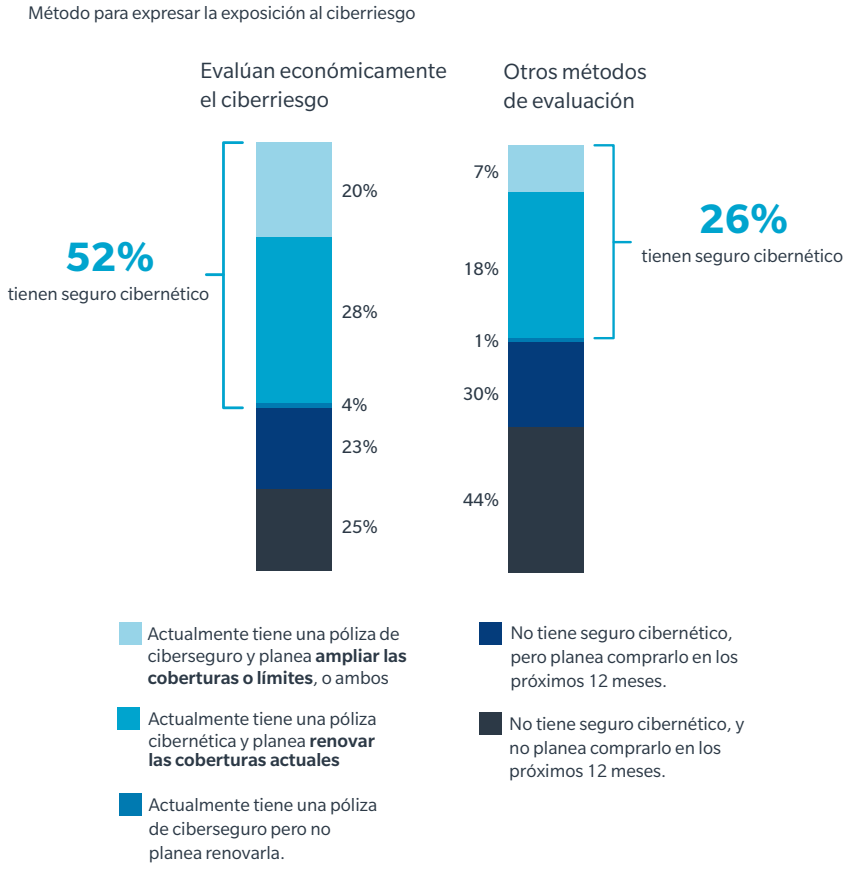
Las organizaciones que usan métodos de cuantificación económica para evaluar su exposición al riesgo cibernético, tienden a comprar más un seguro cibernético que aquellas que usan solo métodos cualitativos o ningúno: 52% vs 26% (ver gráfica 25). Esto se debe a que las primeras están mejor informadas y dispuestas a capitalizar el valor del seguro cibernético. Además, estas empresas, aseguran que planean renovar (28%) o ampliar (20%) sus coberturas y/o límites.

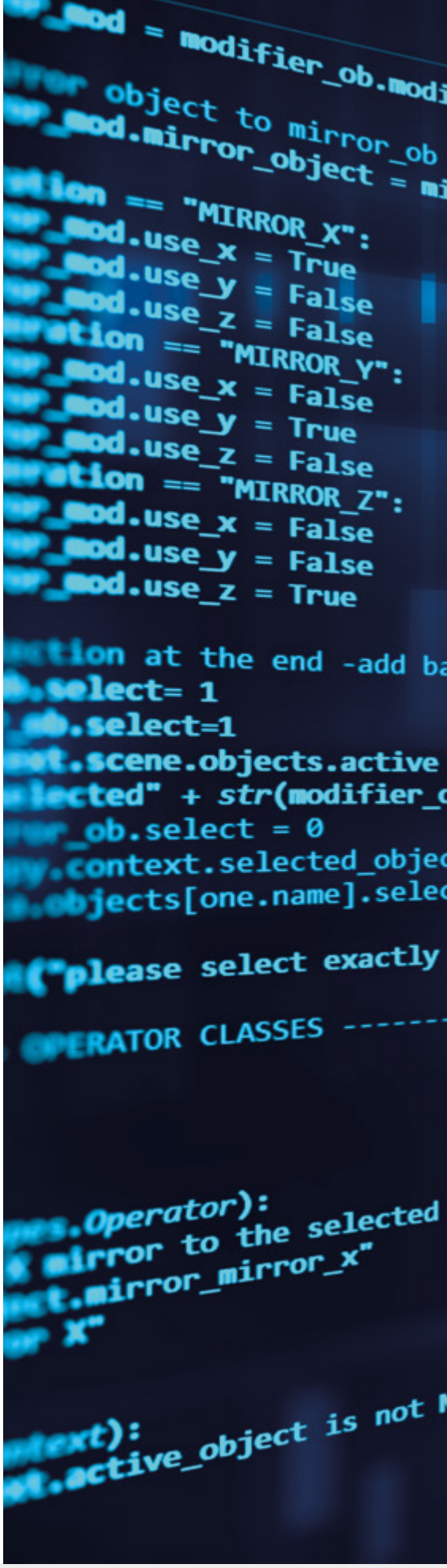
Resulta preocupante que en ambos escenarios un gran porcentaje de empresas todavía ni tienen ni planean compar un seguro: 25% entre las que cuantifican económicamente el riesgo, y 44% entre las usan otros métodos de evaluación.

GRÁFICA 25

Las organizaciones que utilizan métodos económicos de evaluación de riesgos cibernéticos tienen más probabilidades de comprar seguros cibernéticos y aumentar las coberturas actuales.

P: ¿Cuál es el estado de su organización con respecto al seguro cibernético?





Conclusiones

A medida que el riesgo cibernético se vuelve cada vez más complejo y desafiante, existen signos alentadores en nuestra Encuesta de Percepción del Riesgo Cibernético en Latinoamérica 2019, de que las empresas, de manera lenta pero segura, están comenzando a implementar las mejores prácticas en la gestión del riesgo cibernético. Casi todas las organizaciones encuestadas reconocen su magnitud: muchas están cambiando los aspectos de su enfoque para que coincida con la amenaza, y la mayoría está realizando un buen trabajo en la ciberseguridad tradicional.

Las organizaciones con más experiencia están construyendo una resiliencia cibernética a través de estrategias más integrales y equilibradas para el manejo del riesgo cibernético, en lugar de concentrase únicamente en la prevención. Estos enfoques más complejos explican la necesidad de desarrollar capacidades para comprender, evaluar y cuantificar el riesgo cibernético en primer lugar, así como agregar las herramientas y recursos para responder y recuperarse de incidentes cibernéticos cuando ocurren de manera inevitable.

No obstante, la encuesta de este año muestra que permanece una brecha considerable entre la ubicación del riesgo cibernético en la agenda corporativa y el nivel general de madurez organizacional en la gestión de riesgos. Muchas empresas a nivel mundial podrían beneficiarse si aplican los principios de una gestión de riesgos estratégica a su enfoque de riesgo cibernético, respaldados por más experiencia, recursos y atención de los miembros directivos a medida que desarrollan resiliencia cibernética.

En la era del "Internet de las Cosas" con cadenas de suministro digitalmente dependientes y tecnología innovadora, las prácticas y mentalidades del ayer no son suficientes, y en realidad pueden inhibir la innovación. Optimizar la seguridad desde el "castillo" (la organización de mentalidad cerrada) hacia la comunidad en general es más difícil, pero inevitable. Requiere un cambio de centrarse únicamente en la seguridad empresarial a asumir la responsabilidad de la seguridad en toda la red de la cadena de suministro.

A nivel práctico, la encuesta de este año apunta a una serie de mejores prácticas que emplean las empresas más resilientes, y que todas las empresas deberían considerar adoptar:

- Crear una fuerte cultura organizacional de seguridad cibernética, con estándares claros y compartidos para gobierno corporativo, rendición de cuentas, recursos, y acciones.
- Cuantificar el riesgo cibernético para tener decisiones mejor informadas de asignación de capital, permitir la medición del rendimiento y enmarcar el riesgo cibernético en los mismos términos económicos que otros riesgos empresariales.
- Evaluar las implicaciones del riesgo cibernético de las nuevas tecnologías como un proceso continuo y prospectivo a lo largo del ciclo de vida de las mismas.
- Administrar el riesgo de la cadena de suministro como un problema colectivo, reconociendo la necesidad de confianza y estándares de seguridad compartidos en toda la red, incluido el impacto cibernético de la organización en sus socios.
- Buscar y apoyar alianzas público-privadas en torno a problemas críticos del riesgo cibernético que puedan brindar protecciones más sólidas y estándares básicos de mejores prácticas.

Con el aumento de la confianza organizacional en la capacidad de gestionar el riesgo cibernético, más empresas reconocen claramente la naturaleza crítica de la amenaza y comienzan a buscar y adoptar las mejores prácticas. La gestión efectiva del riesgo cibernético requiere un enfoque integral que emplee la evaluación, medición, mitigación, transferencia y planificación del riesgo, y el programa óptimo dependerá del perfil de riesgo y la tolerancia únicos de cada empresa. Aun así, estas recomendaciones abordan muchos de los aspectos comunes y más urgentes del riesgo cibernético con el que las organizaciones se enfrentan hoy en día, y deben verse como señales a lo largo del camino hacia la construcción de una verdadera resiliencia cibernética.

Metodología

Este informe se basa en los hallazgos de la Encuesta de Percepción del Riesgo Cibernético en Latinoamérica 2019 (parte de una encuesta global), realizada entre febrero y marzo de 2019.

Un total de 531 líderes empresariales de Latinoamérica participaron en la encuesta, con representación de una gama de funciones clave entre las que se incluyen gestión de riesgos, tecnología de la información / seguridad de la información, finanzas, legal/ cumplimiento, funcionarios de la C-suite y juntas directivas.

Demografía de la encuesta

Geografía

Distribución de los encuestados por país	
Colombia	34%
Brasil	18%
México	16%
Perú	12%
Argentina	8%
Otros	12%

Industrias

Sectores industriales en los que operan principalmente las empresas encuestadas
Manufactura/Automotriz
Minoristas/Mayoristas
Instituciones financieras
Energía/Electricidad
Salud/Ciencias humanas
Transportación/Ferroviaria/Marítima
Comunicaciones, Medios de comunicación y Tecnología
Servicios profesionales
Bienes Raíces
Química
Construcción
Educación
Entidades públicas/Sin fines de lucro
Minería/Metales/Minerales
Aviación/Aeroespacial

ACERCA DE MARSH

Marsh es el corredor de seguros y asesor de riesgos líder a nivel mundial. Con más de 35,000 colegas que operan en más de 130 países, Marsh sirve a clientes comerciales e individuales con soluciones de riesgo basadas en datos y servicios de asesoramiento. Marsh es una subsidiaria de propiedad total de **Marsh & McLennan Companies** (NYSE: MMC), firma líder mundial de servicios profesionales en las áreas de riesgo, estrategia y talento. Con ingresos anuales de más de US$15 mil millones y 75,000 colegas en todo el mundo, MMC ayuda a los clientes a navegar en un entorno cada vez más dinámico y complejo a través de cuatro empresas líderes en el mercado: **Marsh, Guy Carpenter, Mercer y Oliver Wyman. Sigue a Marsh en Twitter @MarshGlobal; LinkedIn; Facebook; y YouTube, osuscríbase a BRINK**.

ACERCA DE MICROSOFT

Microsoft (Nasdaq "MSFT" @microsoft) facilita la transformación digital para la era de una nube inteligente y una ventaja inteligente. Su misión es capacitar a cada persona y cada organización en el planeta para conseguir más logros. El equipo de Diplomacia Digital de Microsoft, que se asoció con Marsh en este informe, combina experiencia técnica y visión de políticas públicas para desarrollar políticas públicas que mejoren la seguridad y la estabilidad del ciberespacio, y permitan la transformación digital de las sociedades de todo el mundo.

RECONOCIMIENTOS

Marsh y Microsoft agradecen a B2B International por su ayuda para diseñar, analizar e informar los resultados de esta encuesta. B2B International es la firma líder a nivel mundial de investigación de mercado de empresa-a-empresa. Se especializa en el desarrollo de programas personalizados de investigación de mercado y conocimiento para algunas de las principales marcas industriales, financieras y tecnológicas del mundo. B2B International cuenta con 600 de las 1,500 corporaciones más grandes entre sus clientes. B2B International es parte del giroscopio, Dentsu Aegis Network, la agencia creativa dedicada al b2b dedicada.

Para más información sobre las soluciones de gestión de riesgos cibernéticos de Marsh, puede escribirnos a cyber.risk@marsh.com, o contacte a su representante local. Visite la página web de Marsh de su país.

Para más información sobre las opciones de seguridad de Microsoft, visite: www.microsoft.com/es-mx/security.