Encuesta de Percepción del Riesgo Cibernético en Latinoamérica 2019

¿QUÉ ESTÁ OCURRIENDO? UN RIESGO CATASTRÓFICO

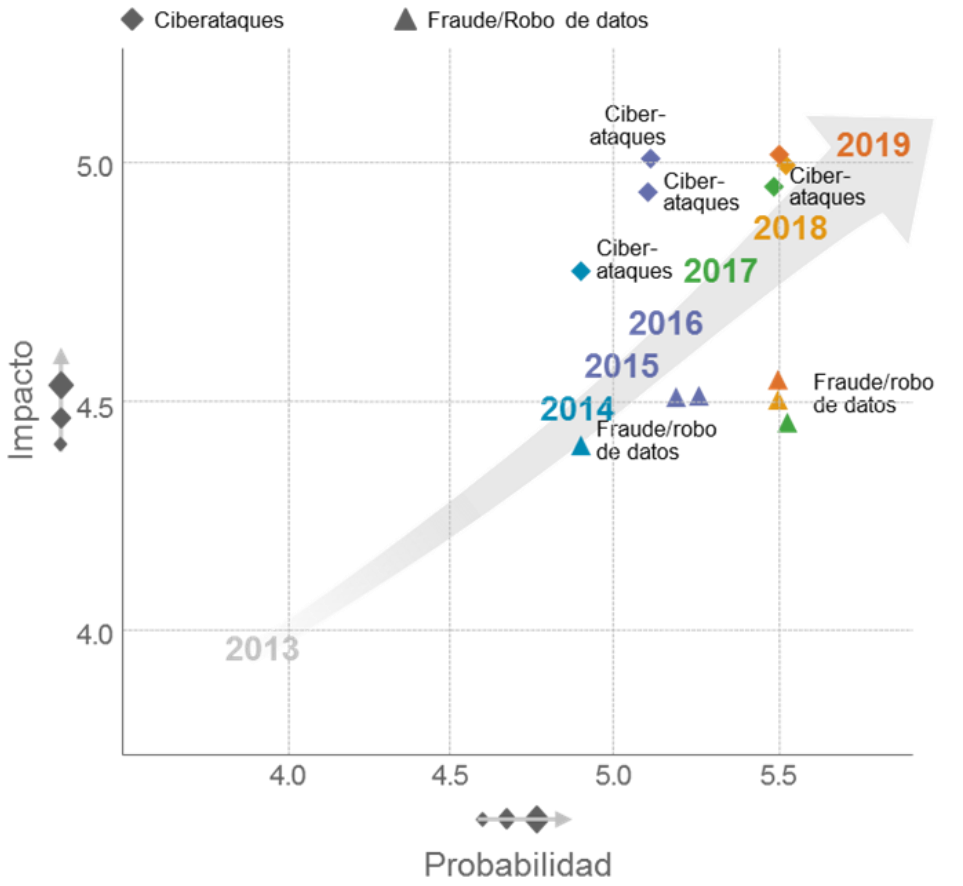
Los **ciber ataques y brechas de datos** están en el top 5 de los riesgos globales a nivel de **probabilidad e impacto.**

La **ciber dependencia** está calificada como el evento #2 que con mayor probabilidad **afectará el desarrollo del mundo** en los próximos 10 años, resaltando la fuerte interconexión de las **infraestructuras críticas** con el ciber riesgo.

El ciber riesgo es el 5to mayor riesgo para las **operaciones del negocio**, debido a que potencialmente puede parar el negocio de las compañías dependientes de la tecnología.

Los ciber ataques tendrán un **impacto** mayor que los desastres del medio ambiente y las enfermedades infecciosas, causando un daño tan grande como el colapso de un ecosistema, y solo un poco menos que los desastres naturales y la crisis por el agua en los próximos años.

Mapa de Percepción de Riesgos del World Economic Forum
(Evolución de ciberataques y fraude/robo de datos 2013–2019)



Fuente: World Economic Forum Global Risk Report, Marsh & McLennan Companies.Nota: Data de 2017-2019 ha sido ajustada para ser comparada, debido a un cambio en la escala.

MARSH

¿QUÉ ESTÁ OCURRIENDO? CIFRAS EN AUMENTO

54% de las organizaciones encuestadas en 10 países fueron víctimas de ataques de ransomware en 2017

Sophos – The State of Endpoint Security Today 2018

$3.86M es el costo promedio total de una brecha de datos a nivel global

Ponemon Institute - 2018 Cost of a Data Breach Study

$133K es el costo promedio de un ataque de ransomware

Sophos – The State of Endpoint Security Today 2018)

$6B es el costo estimado de los daños causados por el ciber-crimen para el 2021

Cybersecurity Ventures - 2019 Official Annual Cybercrime Report

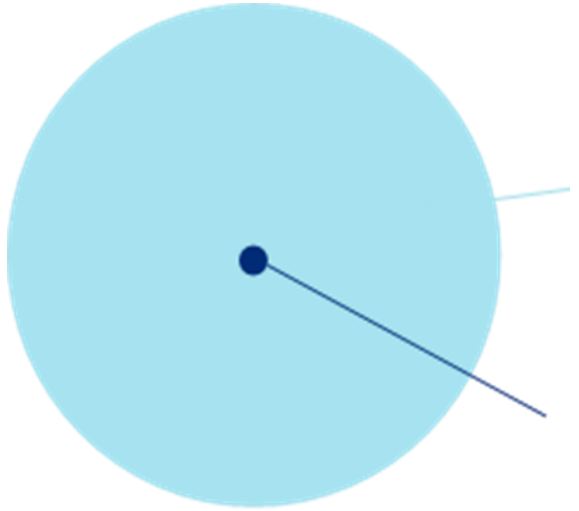
1,000M de ataques de malware fueron detectados en Latinoamérica en 2018

https://www.zdnet.com/article/latin-america-suffers-1-billion-malware-attacks-in-2018/

¿QUÉ ESTÁ OCURRIENDO? BAJA INVERSIÓN EN SEGUROS

Inversión en seguros de Property vs. Cyber (US)

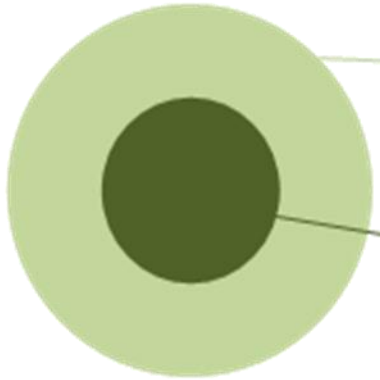
Cyber Risk



Impacto económico del ciber-crimen:
+500,000M $

Mercado de seguros cyber (US):
+4,000M $

Property Risk



Impacto económico de desastres naturales:
300,000M $

Mercado de seguros Property (US):
180,000M $

La infraestructura tecnológica debe ser tratada de manera análoga a las infraestructura física.

¿Has dudado alguna vez en proteger la infraestructura física de tu empresa a través de un seguro?

¿Has construido un edificio sin que un experto valide las medidas de seguridad implementadas?

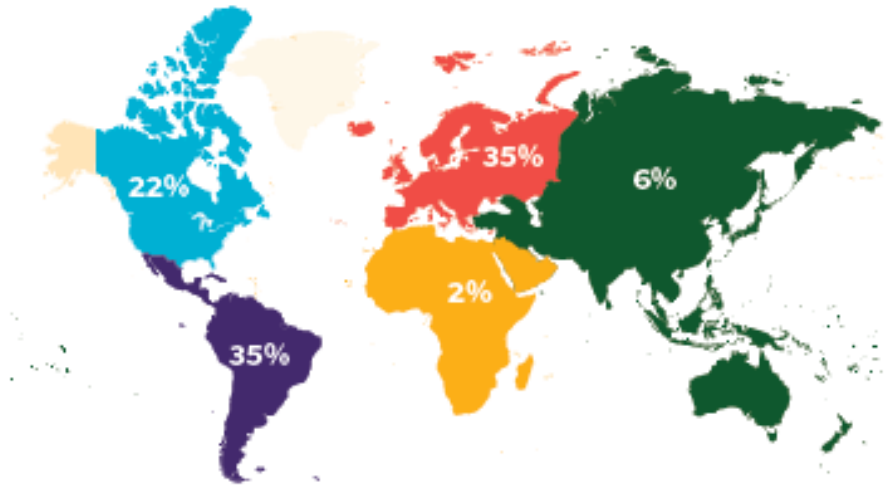
Marsh and MMC Estimates 2018.
** Marsh US clients, $1 billion+ revenues, 2018*

MARSH

PARTICIPANTES EN LA ENCUESTA

1.500 empresas / **531 en LAC**

Por región



Por tamaño

Por industria

*El **riesgo cibernético** no es un problema tecnológico que hay que resolver o eliminar es un **reto empresarial** que hay que **gestionar***

PRINCIPALES HALLAZGOS LAC

1 **Crece la preocupación** por el riesgo cibernético

73% lo considera una de las 5 principales preocupaciones para su organización (vs 47% en 2017). Para 21% es su amenaza #1.

2 **Aumenta el nivel de confianza** de las empresas en su **capacidad** para gestionar el riesgo cibernético

Sin embargo, todavía 30% desconfían totalmente de su capacidad para responder a un ciberincidente.

3 Hay una **brecha** entre esta preocupación/ confianza, y la **inversión** dedicada a su gestión

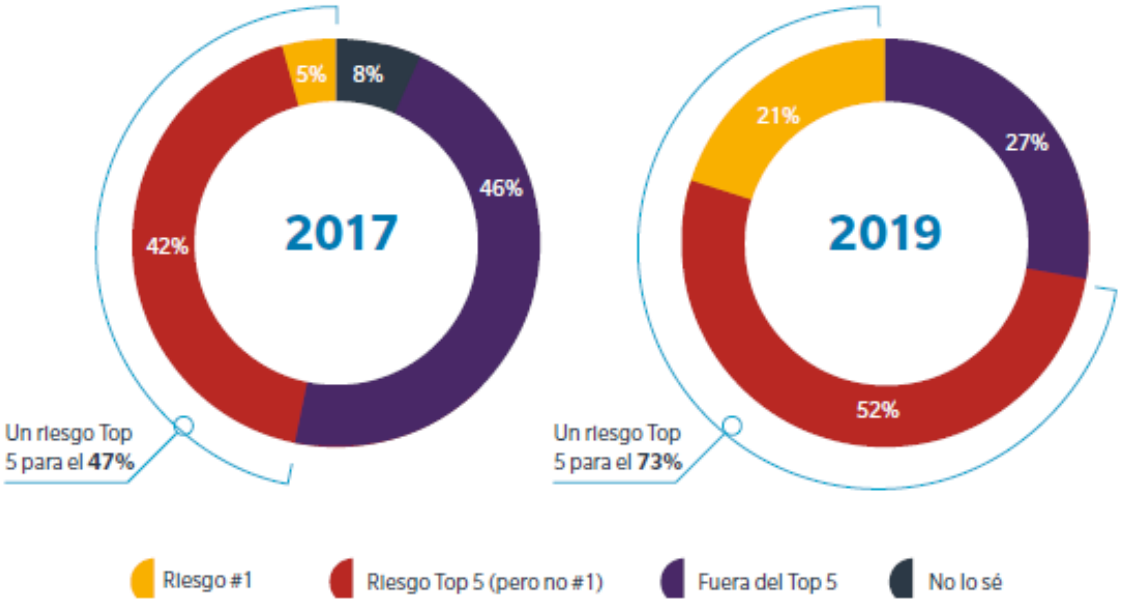
54% de la inversión para enfrentar el riesgo cibernético se centra en tecnología y prevención, no en la resiliencia: identificar, cuantificar, mitigar, transferir y planificar respuesta en caso de un ciberincidente.

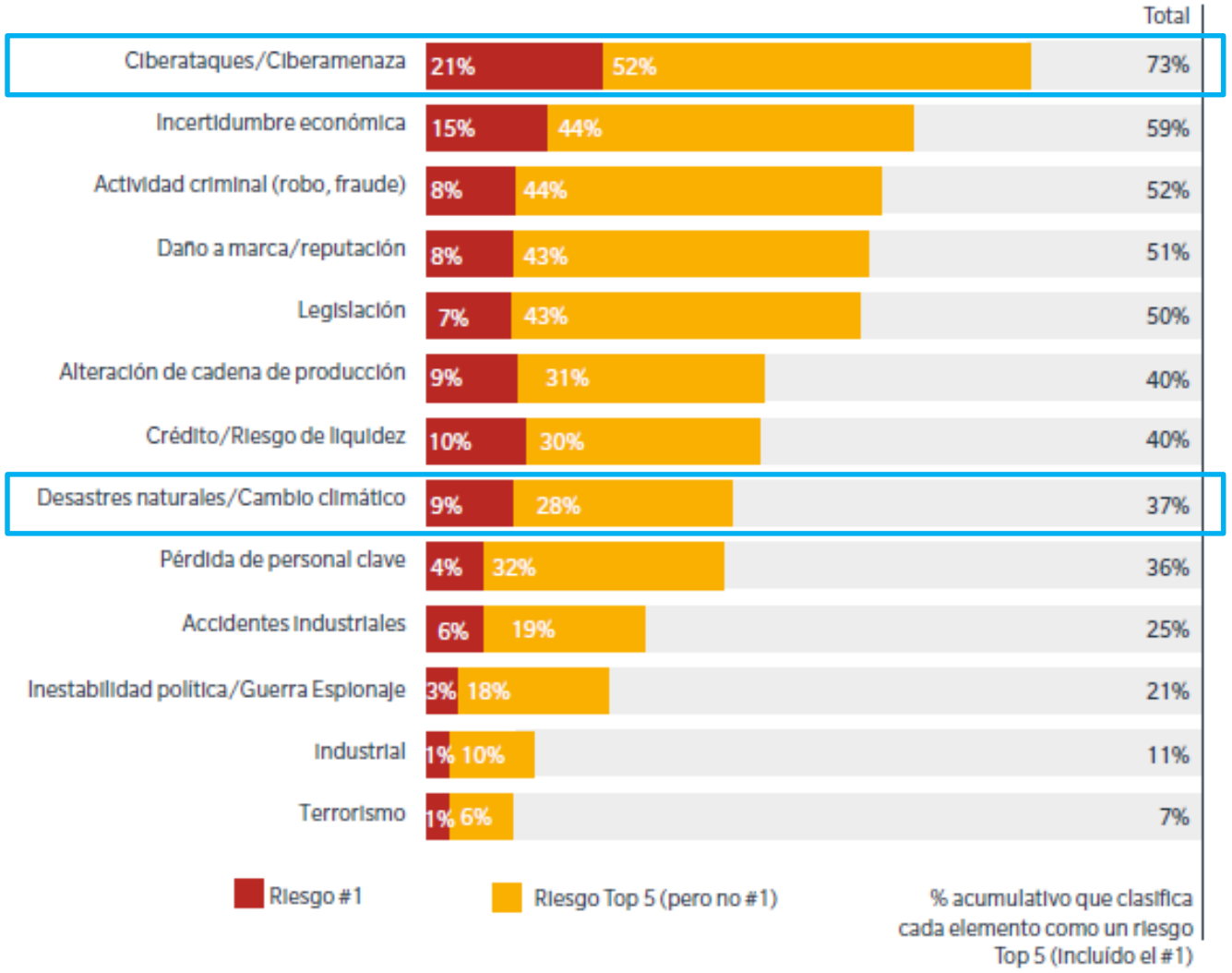
4 **Crece** el número de empresas que cuentan con un **seguro de riesgo cibernético**

Un 29% de empresas encuestadas en LAC tienen seguro, pero estamos lejos todavía de la media global (47%). El porcentajes es mayor entre las grandes empresas (40%), y entre las que cuantifican su riesgo (52%).

La preocupación acerca del riesgo cibernético se incrementa y se consolida como uno de los principales 5 riesgos para las organizaciones

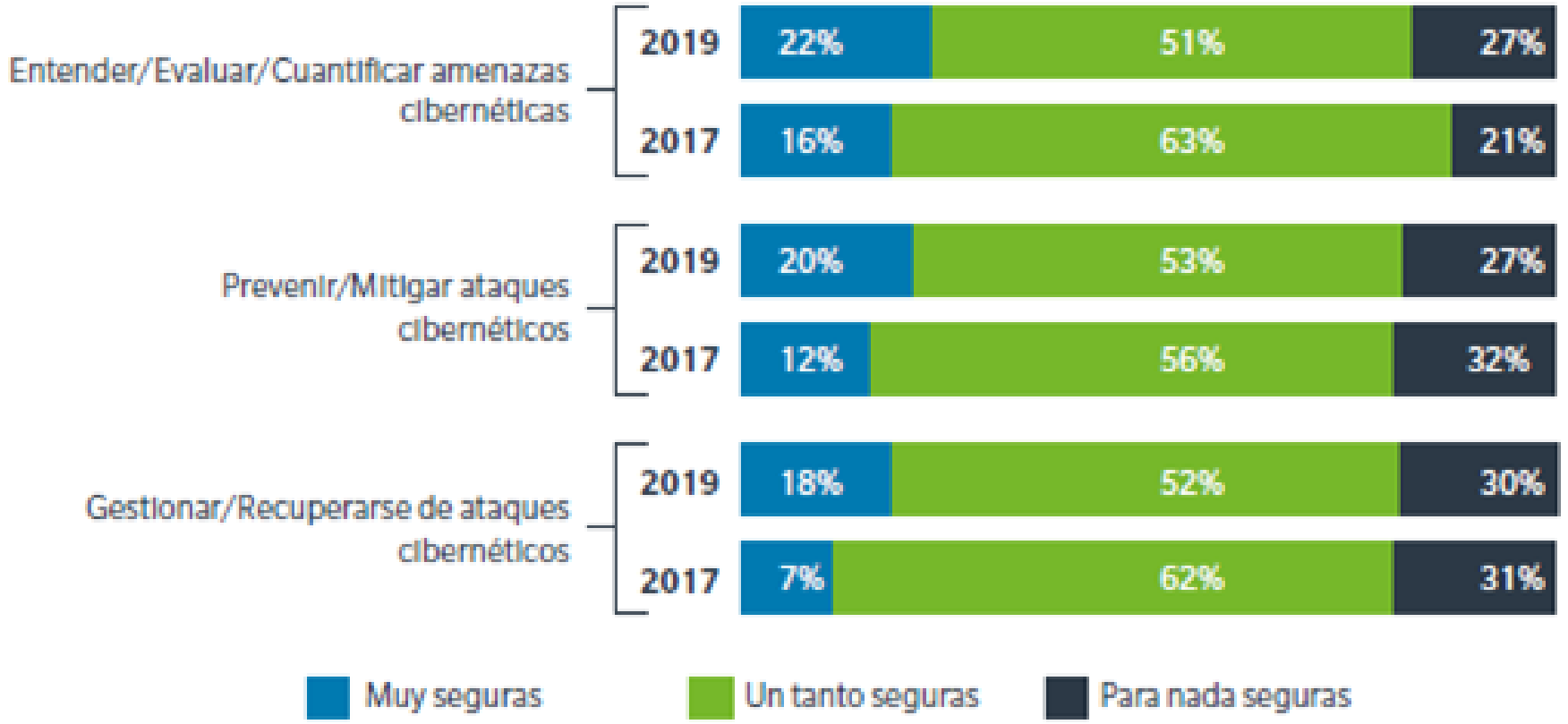
21% prioridad #1
73% prioridad Top 5





La preocupación sobre el riesgo cibernético es alta, pero la confianza de las organizaciones es baja

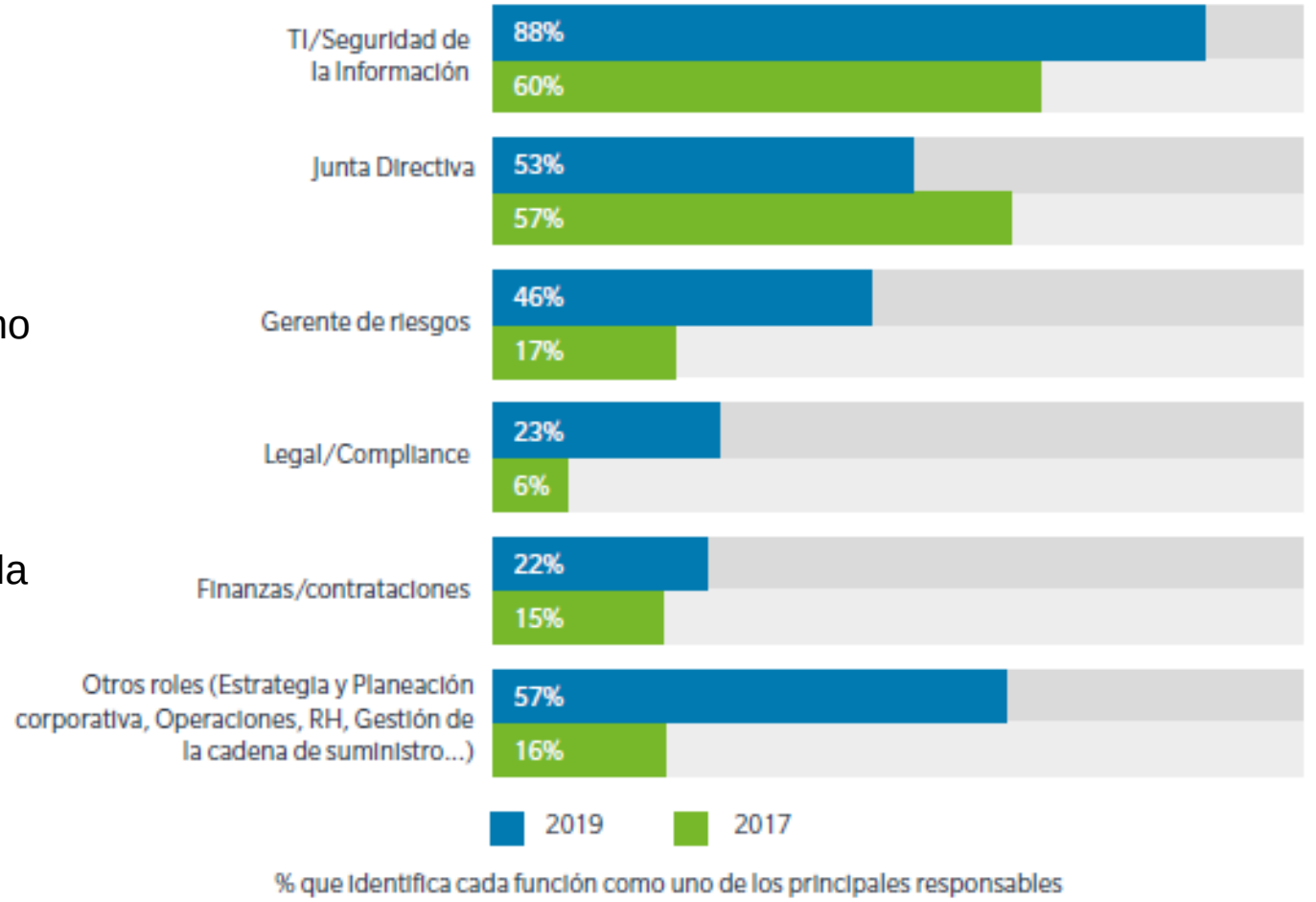
Aumenta ligeramente la confianza de las empresas en **3 áreas críticas** de la resiliencia cibernética:



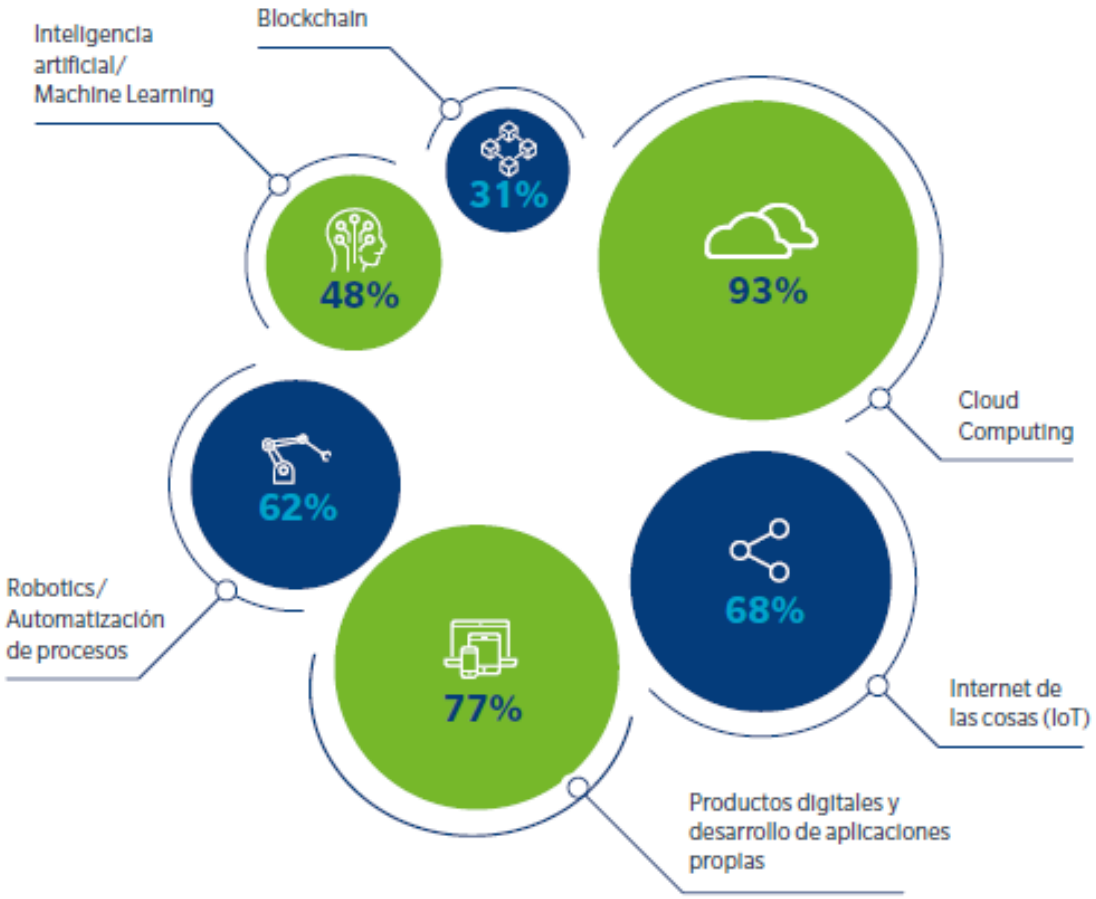
Preocupa que todavía 1 de cada 3 no confíen nada en su capacidad de resiliencia.

Tecnología/Seguridad de la Información continúa siendo percibido como el responsable del riesgo cibernético

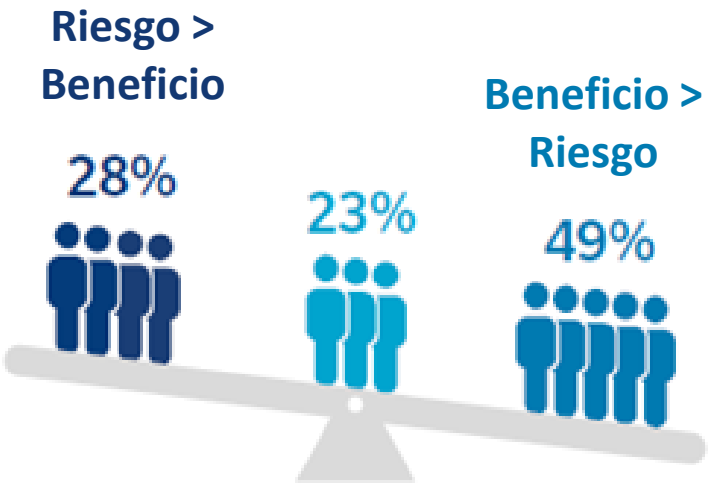
- La responsabilidad de la gestión recae principalmente en los equipos de **Tecnología y Seguridad de la Información**.
- Crece la importancia del **Gerente de Riesgos** como responsable del ciber-riesgo:
  46% en 2019 vs. 17% en 2017
- Aunque la **Junta Directiva** es un actor clave, preocupa que dediquen menos de un día al año a la gestión del ciber-riesgo.



La mayoría de las organizaciones están adoptando tecnologías emergentes, a pesar de los riesgos que generan



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



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

Las medidas técnicas de ciberseguridad están encabezando la lista de las inversiones para la gestión del ciber-riesgo

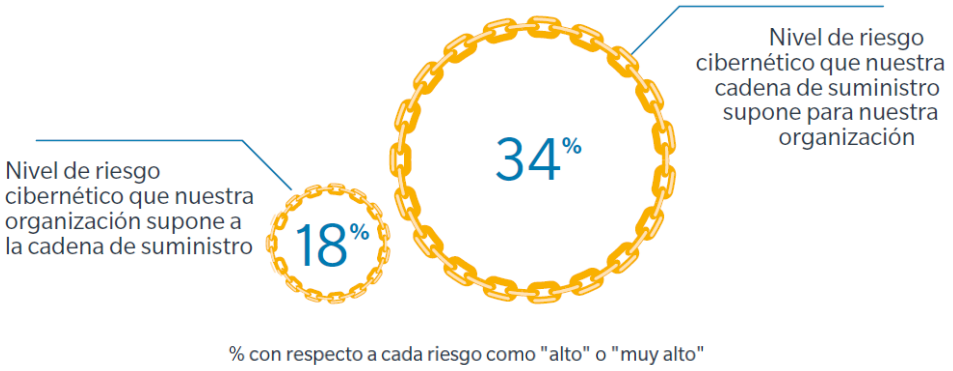
- La mayoría de las organizaciones invierten en tecnología para la gestión del riesgo cibernético, pero no están invirtiendo en la misma proporción, en medidas de planificación, transferencia y respuesta.
- Centran principalmente su estrategia en **medidas técnicas de seguridad de dispositivos y sistemas** (81%) y en la **protección de datos** (73%).
- La **capacitación a la alta gerencia** (28%), la evaluación de riesgos en la **cadena de suministro** (31%) o el **modelamiento de escenarios** de pérdidas (28%) no son prioritarias entre las inversiones para la gestión del riesgo cibernético, lo que supone un alto riesgo para la organización.

La tecnología de ciberseguridad y la mitigación están encabezando la lista de las futuras inversiones para la gestión de este riesgo

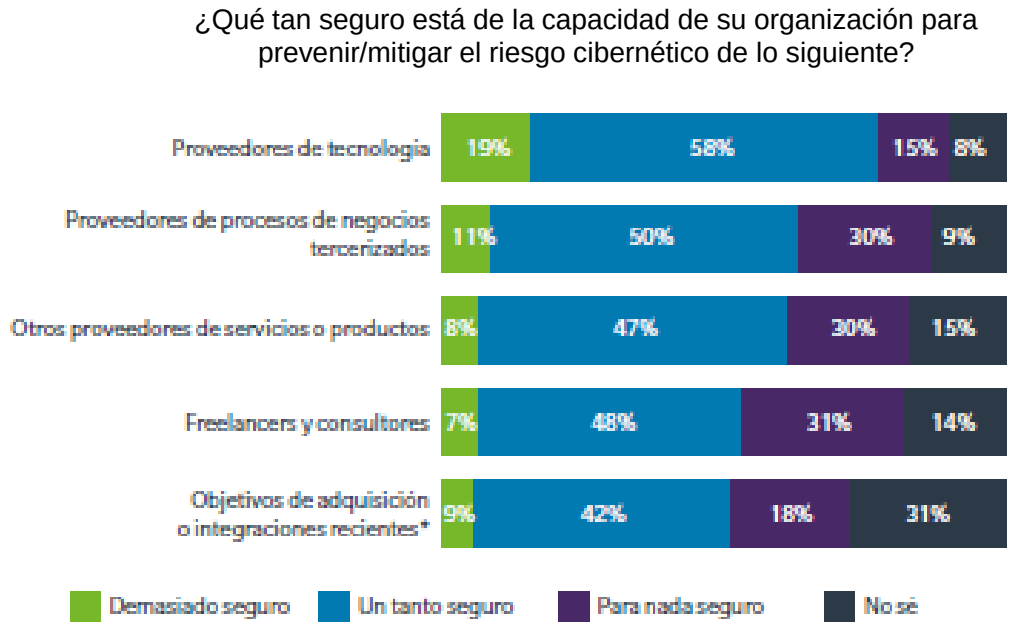
- 54% de la inversión en ciberseguridad para los próximos años se centra en **tecnología y mitigación**.
- Sin embargo, la mayoría no está priorizando sus recursos en crear **verdadera resiliencia**: identificar, cuantificar, mitigar, transferir y planificar su respuesta.
- 62% dijo que un **ataque/incidente** cibernético en su empresa sería el principal detonante del crecimiento de la inversión en ciberseguridad.
- Para el 56%, la adopción de **nuevas tecnologías** ayudará a generar una mayor inversión en ciberseguridad.

Las organizaciones consideran que los terceros representan un mayor riesgo a la cadena de suministro que ellas mismas

- **Disparidad de percepción**: las organizaciones tienden a pensar que sus proveedores están menos preparados para gestionar el riesgo cibernético que ellos mismos.



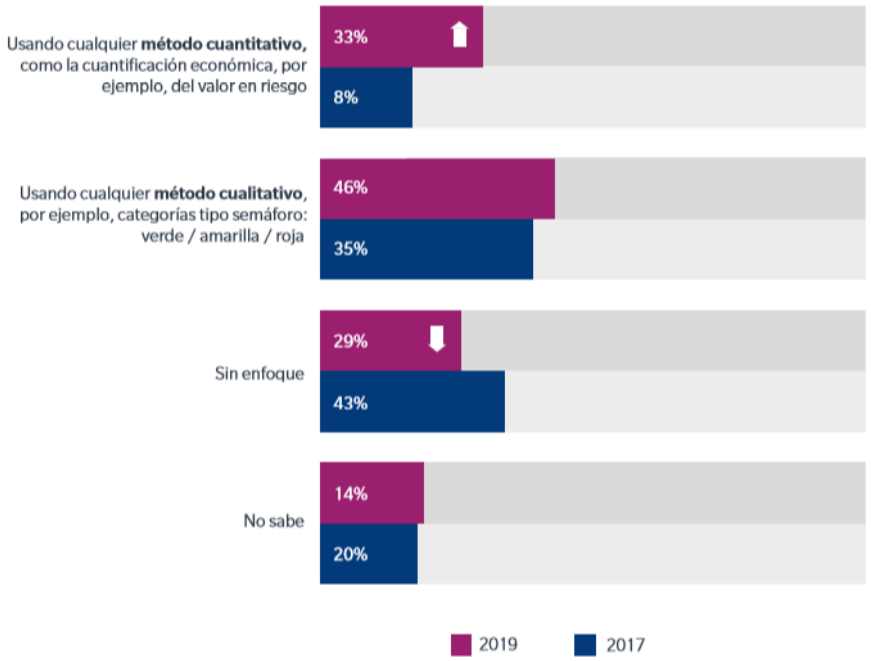
- El 25% no confía en absoluto en su capacidad para prevenir los amenazas cibernéticas de al menos uno de sus socios comerciales.

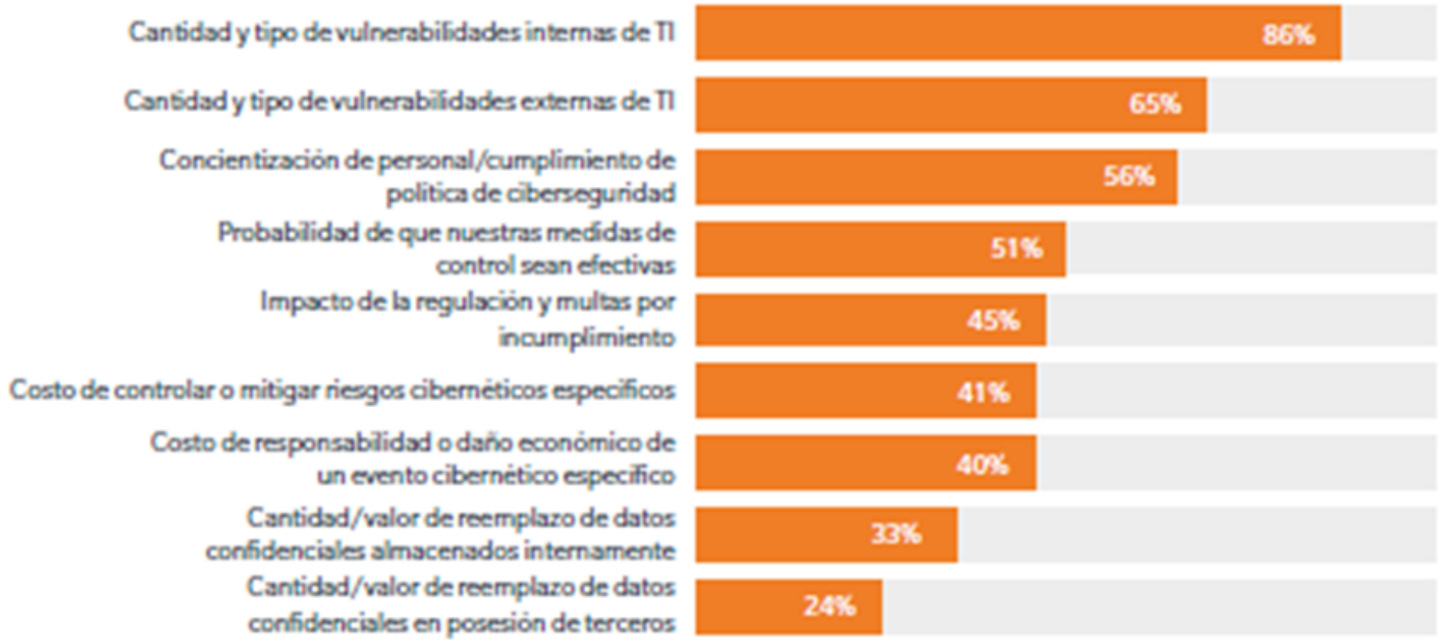


Debemos tratar de construir una responsabilidad social tecnológica en toda la cadena.

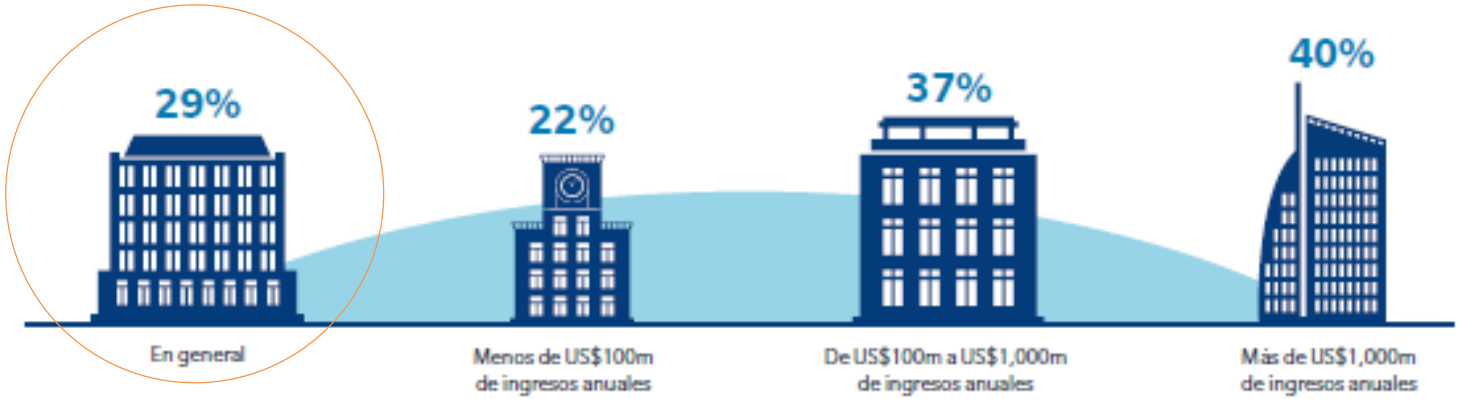
33% de las organizaciones en Latinoamérica están usando métodos cuantitativos para expresar el riesgo cibernético en términos económicos

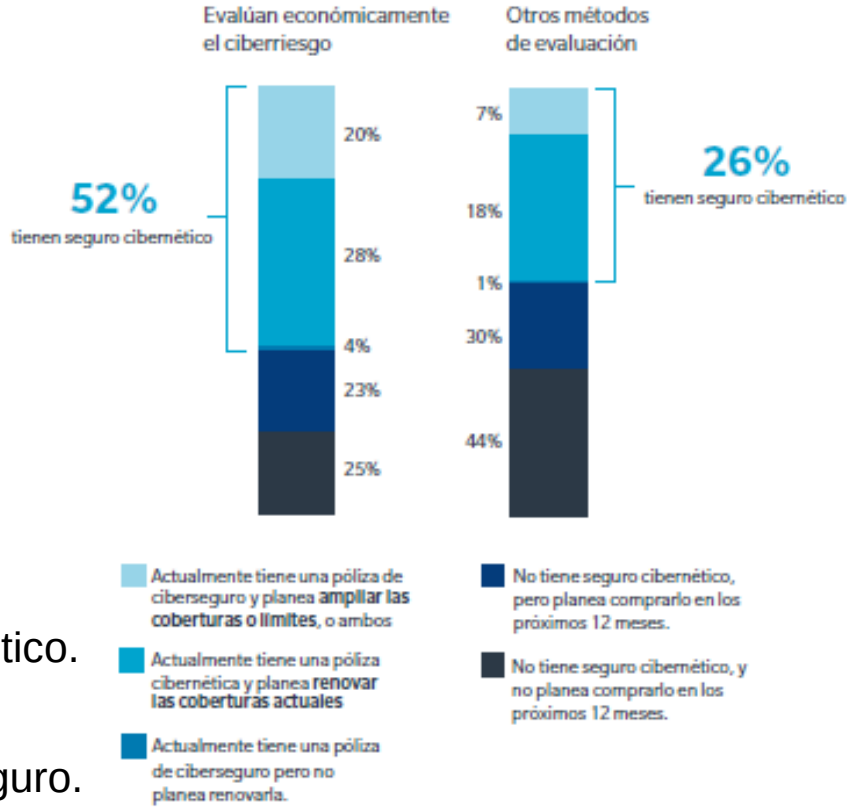
- 1 de cada 3 empresas cuantifican económicamente su exposición al riesgo: **33%** vs **8%** en 2017.
- Más del doble de organizaciones **evalúan o miden** el riesgo cibernético a través de la cantidad y tipo de vulnerabilidades, en comparación con las que evalúan los costos potenciales, multas y pérdidas





La oferta del seguro de riesgo cibernético va ganando relevancia en el mercado Latinoamericano





- 1 de cada 3 empresas en Latinoamérica cuentan con seguro de riesgo cibernético.
- Latinoamérica todavía está lejos de la media del resto del mundo: 47%
- Las PYMES son las más vulnerables a ciberataques, pero solo 22% tienen seguro.
- Las empresas que cuantifican económicamente su riesgo cibernético suelen ser las que adquieren más seguros de riesgo cibernético.

Se percibe mayor efectividad en los estándares de ciberseguridad de la industria que en la regulación para mejorar la postura de ciberseguridad

- Las organizaciones consideran que los **estándares internacionales de seguridad y ciberseguridad** (p.e. NIST, ISO 2700X, etc.), que pueden implementar de forma voluntaria, son más efectivos que las regulaciones para ayudarles a **mejorar sus estrategias** de ciberseguridad: 43% vs 30%.

- 3 de cada 5 empresas están muy preocupadas por el potencial impacto de los **ciberataques promovidos por gobiernos** (locales o internacionales), y piden más medidas de **protección** a sus gobiernos ante este tipo de ataques.

¿QUÉ DEBERÍAN HACER LAS EMPRESAS?

Disonancia entre la criticidad del riesgo cibernético y las responsabilidades de los roles estratégicos	Crear una fuerte **cultura organizacional de ciberseguridad** liderada desde la alta gerencia (con políticas y procedimientos transversales y recursos priorizados).
La cuantificación del riesgo cibernético es clave para la toma de decisiones estratégicas informadas	**Cuantificar el riesgo** cibernético para tomar **decisiones informadas** para la mitigación y transferencia del riesgo.
El riesgo cibernético no es una barrera para la adopción de tecnologías emergentes.	**Evaluar** las implicaciones del riesgo cibernético de las **nuevas tecnologías** como un proceso continuo a lo largo del todo el ciclo de vida.
Las cadenas de suministro están interconectadas digitalmente, y el riesgo es colectivo.	Administrar el riesgo de la **cadena de suministro** como un problema colectivo, exigiendo la aplicación de estándares de seguridad y ciberseguridad mínimos en terceros.
Las amenazas cibernéticas a nivel país son críticas y no pueden ser gestionadas sin el apoyo del Gobierno.	Establecer **alianzas público-privadas** para tener estándares de ciberseguridad robustos para hacer frente al riesgo cibernético.
La oferta del seguro de riesgo cibernético va ganando relevancia en el mercado Latinoamericano	Evaluar la contratación del **seguro de riesgo cibernético**, como un mecanismo de transferencia del riesgo complementario a la mitigación, a fin de reducir el impacto de los incidentes significativos.

CONCLUSIONES

- A medida que el riesgo cibernético se vuelve cada vez más complejo y desafiante, la **confianza** de las empresas en su **capacidad para gestionarlo** ha aumentado ligeramente, y hay signos alentadores de adopción de mejores prácticas.

- La realidad es que el riesgo cibernético **no se puede eliminar**. Por ello, y para lograr una **verdadera resiliencia organizacional**, las empresas necesitan gestionarlo de forma **integral**:
  - Desarrollar capacidades para **comprender**, **evaluar y cuantificar el riesgo cibernético**.
  - Invertir en recursos/herramientas para **responder y recuperarse** ante incidentes cibernéticos.

- Sin embargo, la encuesta muestra que existe una gran **brecha** entre la prioridad en la agenda corporativa del riesgo cibernético y el nivel general de madurez organizacional para su adecuada gestión.

- Las **cadenas de suministro** son digitalmente interdependientes y la confianza (o no) en la capacidad de resiliencia cibernética de terceros es clave para un estado de ciberseguridad integral. Debería tratarse como un riesgo colectivo, con estándares comunes a lo largo de toda la cadena.

¿CÓMO PUEDE AYUDAR MARSH?

Marsh cuenta con un equipo global de especialistas para ayudar a las empresas a **gestionar de manera adecuada su riesgo cibernético,** a través del **diseño de estrategias** para la mitigación y transferencia.

Entendimiento

- Análisis de Ciber-riesgos
- Evaluación de madurez de ciberseguridad
- Evaluación de ciber-riesgos con terceros
- Cyber Chemistry - Evaluación de la cultura de ciberseguridad
- Evaluación de cultura

Cuantificación

- Cyber Value-at-Risk
- CyberXQ: cuantificación de brechas de seguridad basada en escenarios
- Cyence – Evaluación del entorno de amenazas cibernéticas
- Cyber IDEAL – Cuantificación de violación de datos externos

Gestión

- Definición de la estrategia de ciberseguridad
- Preparación de respuesta ante ciberincidentes
- Simulaciones de ciber-crisis
- Seguro de riesgo cibernético

¿Preguntas?

Para más información, contacten con:

Paulina.Velez@marsh.com
Edson.Villar@marsh.com