Estudio de Gestión del Riesgo Cibernético en el Sector Financiero Latinoamericano 2023

Presentación de resultados

República Dominicana
Noviembre de 2023
Marsh Advisory

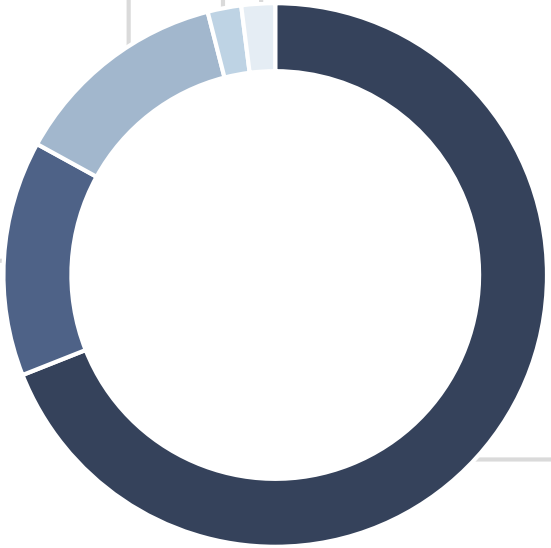
Entorno de riesgo global a corto plazo

Rango	Riesgos que se manifiestan actualmente
1	Crisis en el suministro energético
2	Crisis del costo de vida
3	Aumento de la inflación
4	Crisis en el suministro de alimentos
5	Ciberataques a infraestructuras críticas

Perspectivas a corto plazo

13%
Puntos de inflexión progresivos y crisis persistentes que producen resultados catastróficos

14%
Ligeramente volátil con ocasionales casos imprevistos localizados



2%
Volatilidad limitada con relativa estabilidad

2%
Estabilidad renovada con un resurgimiento de la resiliencia global

69%
Volatilidad constante en todas las economías e industrias, con múltiples perturbaciones que acentúan las trayectorias divergentes

Puntos clave de ciberseguridad

El **riesgo de ciberseguridad** se percibe como una de las principales amenazas a nivel global.

435%
Incremento de casos de ransomware en 2020. +70% el incremento 2021 y 2022.

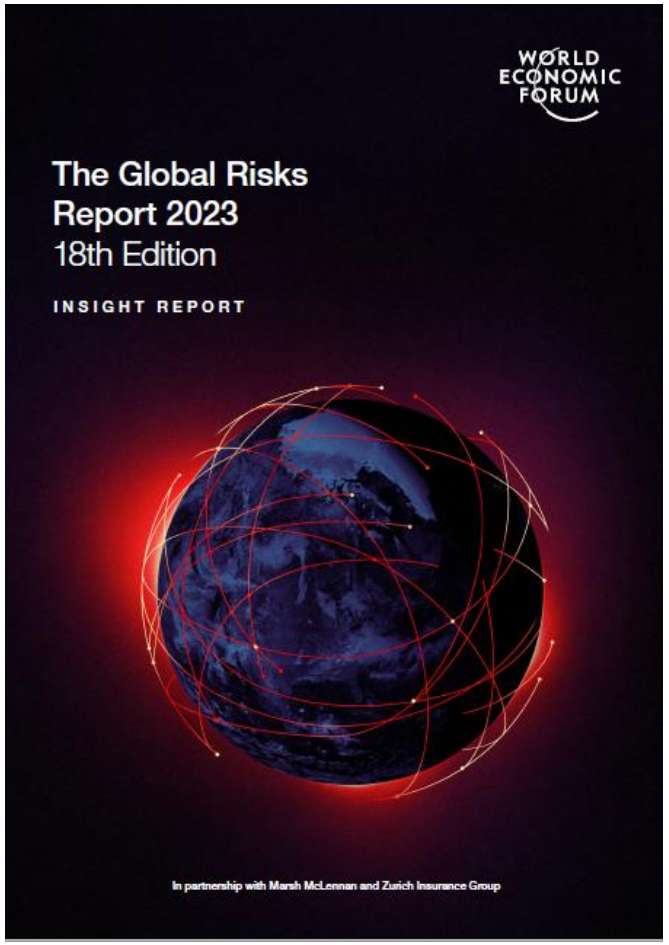
3 millones
Es el déficit de profesionales de ciberseguridad a nivel global.

95%
De los eventos de ciberseguridad se derivan de errores humanos.

6 a 10 segundos
Es el tiempo promedio de lectura de un correo electrónico.

Nota: Encuesta de Percepción de Riesgos Globales del FEM (1249 respuestas en todo el mundo).
Fuente: Foro Económico Mundial, análisis de MMC

Elaborado por el Foro Económico Mundial en colaboración con Marsh McLennan



	2025 — 2 años	2033 — 10 años
1	Crisis del costo de vida	Incapacidad para mitigar el cambio climático
2	Desastres naturales y fenómenos meteorológicos extremos	Incapacidad de adaptación al cambio climático
3	Confrontación geoeconómica	Desastres naturales y fenómenos meteorológicos extremos
4	Incapacidad para mitigar el cambio climático	Pérdida de biodiversidad y colapso de los ecosistemas
5	Deterioro de la cohesión social y polarización de la sociedad	Migración involuntaria a gran escala
6	Incidentes de daños al medioambiente a gran escala	Crisis de recursos naturales
7	Incapacidad de adaptación al cambio climático	Deterioro de la cohesión social y polarización de la sociedad
8	Ciberdelincuencia e inseguridad cibernética generalizadas	Ciberdelincuencia e inseguridad cibernética generalizadas
9	Crisis de recursos naturales	Confrontación geoeconómica
10	Migración involuntaria a gran escala	Incidentes de daños al medioambiente a gran escala

Económico Ambiental Geopolítico Social Tecnológico

Fuente: Foro Económico Mundial, Informe de Riesgos Globales 2022

.

Perspectivas de economías avanzadas frente a mercados emergentes

Economías avanzadas

Rango	Riesgo
1	Inflación rápida y/o sostenida
2	Crisis del costo de vida
3	Confrontación geoeconómica
4	Graves perturbaciones o volatilidad de los precios de los productos básicos
5	Crisis graves de suministro de productos básicos
6	Crisis de endeudamiento
7	Incapacidad de adaptación al cambio climático
8	Conflicto interestatal
9	Controversia geopolítica de los recursos estratégicos
10	Estallido de la burbuja de activos

Mercados emergentes

Rango	Riesgo
1	Crisis del costo de vida
2	Inflación rápida y/o sostenida
3	Crisis de endeudamiento
4	Crisis de empleo y medios de subsistencia
5	Falta de servicios digitales generalizados y desigualdad digital
6	Graves perturbaciones o volatilidad de los precios de los productos básicos
7	Crisis graves de suministro de productos básicos
8	Controversia geopolítica de los recursos estratégicos
9	Confrontación geoeconómica
10	Desastres naturales y fenómenos meteorológicos extremos

Observaciones clave

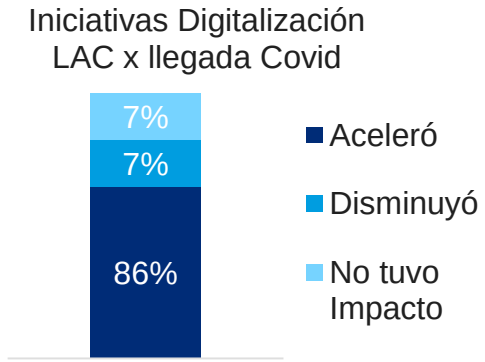
- El costo de vida, la inflación, la deuda, el precio/suministro de productos básicos y la amenaza de conflictos (económicos o de otro tipo) son las principales preocupaciones de los ejecutivos a nivel mundial
- Los ejecutivos en **economías avanzadas** se muestran especialmente cautos ante los riesgos geopolíticos (por ejemplo: conflictos interestatales, confrontación geoeconómica)
- Los ejecutivos en **mercados emergentes** reflejan inquietud por el acceso a los servicios digitales y los desastres naturales

Económico Ambiental Geopolítico Social Tecnológico

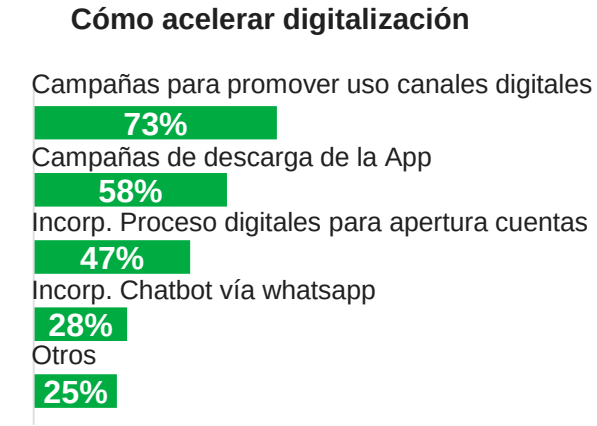
Nota: Encuesta de Opinión Ejecutiva del FEM (12,550 respuestas en todo el mundo). Los encuestados podían elegir hasta cinco riesgos que consideraban las mayores amenazas para su país en los próximos dos años.
Fuente: Foro Económico Mundial, análisis de MMC

(Re)evolución Digital

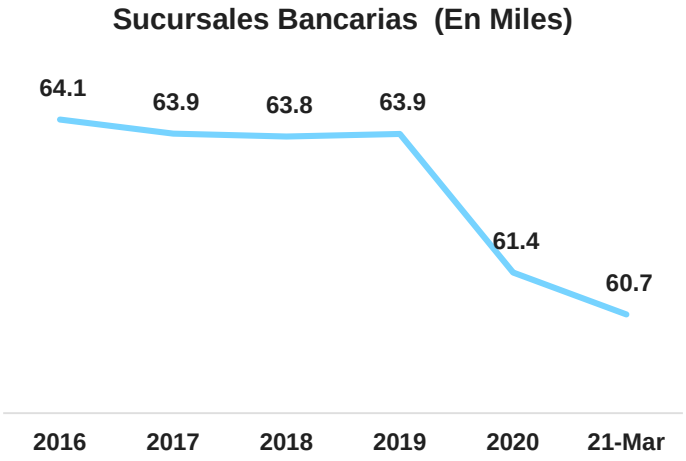
86% de los bancos de la región aceleraron iniciativas de digitalización



Fuente: Infocorp

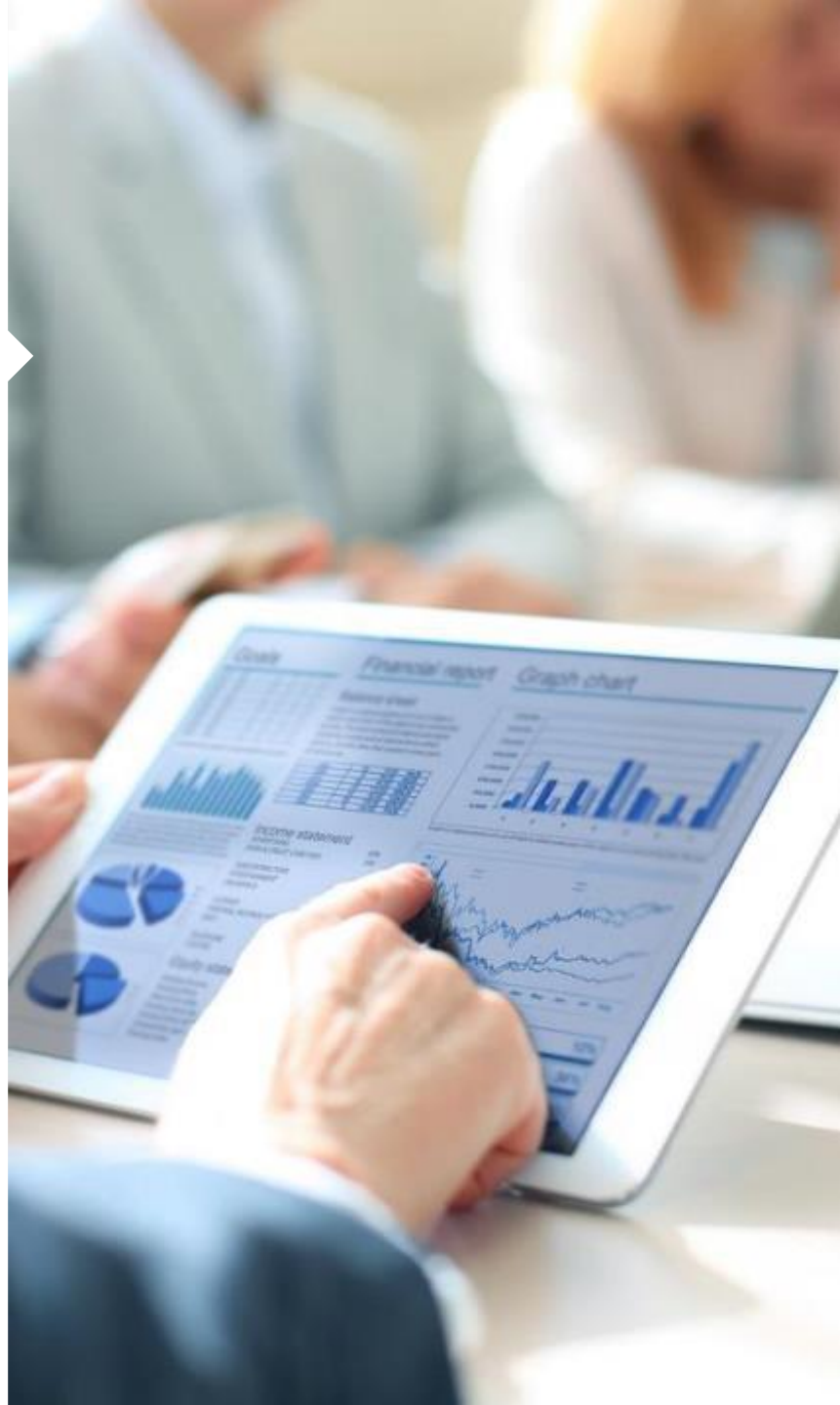


Fuente: Infocorp



Fuente: Felaban

La digitalización de muchas otras industrias en sus modelos de negocio ha forzado a que la banca invierta ampliamente para atender las necesidades de su base de clientes

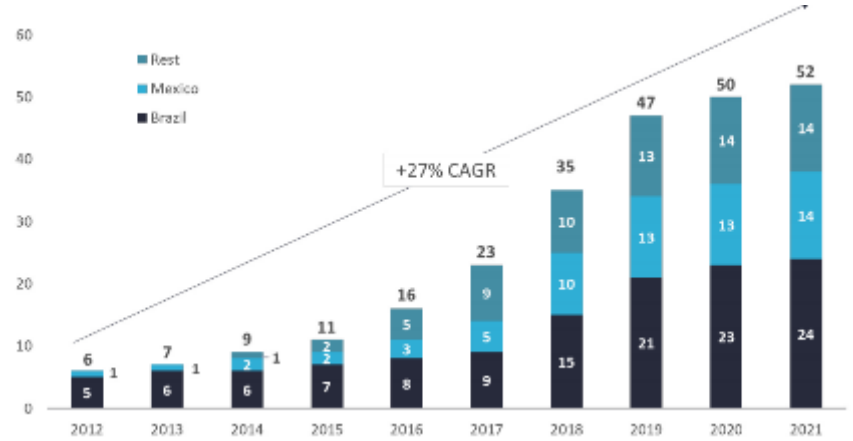


Marsh

(Re)evolución Digital

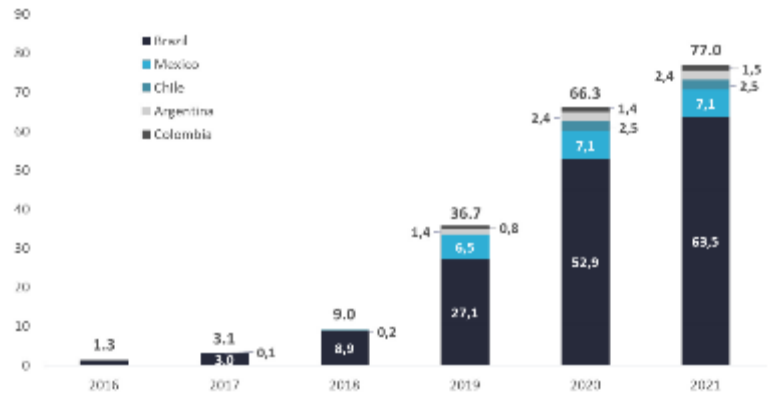
Nuevos hábitos del cliente, mayor penetración digital y favorable marco regulatorio ayudaron a disparar la banca digital… y luego el Covid lo terminó de acelerar

Número Bancos Digitales
2012 - 2021



Fuente: BPC, Fincog, Julio 2021

No. Clientes Neobancos
2012 - 2021



Fuente: BPC, *Fincog*, Julio 2021

82% de los clientes de los Neobancos están en Brasil

Top 10 de Neobancos concentran 90% de los clientes

Nubank, saldrá a bolsa con un IPO en 2021, valoración inicial de $40billones USD

Marsh

Marco Regulatorio

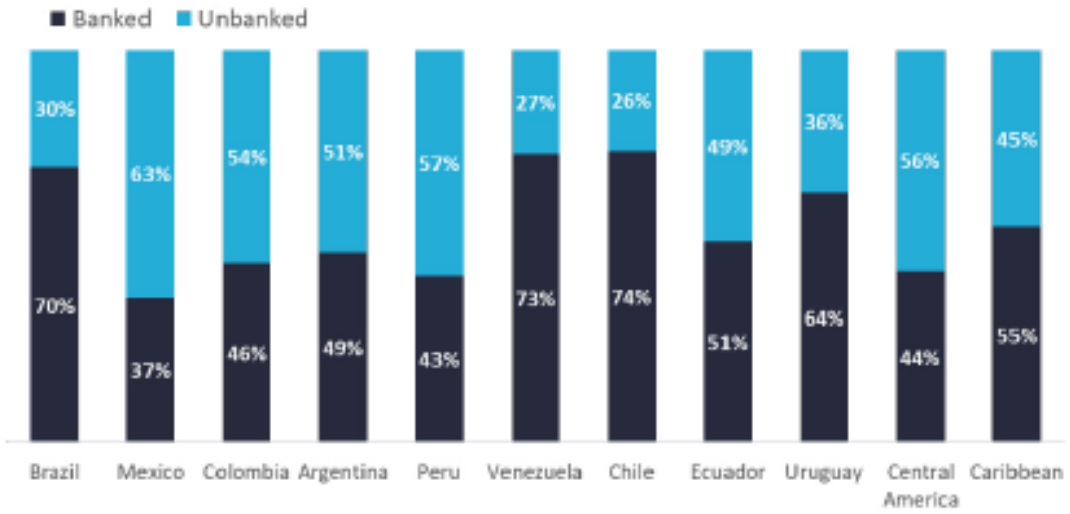
En lugar de ralentizar la evolución, reguladores ven con buenos ojos incorporar elementos Fintechs para futuras interaciones

Noviembre 2020, Banco Central de Brasil lanzó un sistema nacional de pagos llamado Pix.

Ley Fintech, 2018. 93 Fintechs sacando licencia de FTI (Financial Technology Institution)

2020 SFC lanzó primer fintech sandbox regulatorio – experimentar con modelos bancarios sin tener que cumplir requisitos tradicionales

Ley Fintech propuesta en Feb 2021.



Fuente: BPC, Fincog, Julio 2021. Global Findex Database by the World Bank

Marsh

Conozca a su Cliente

Primará el foco en el cliente, conveniencia, comunicación y costo

43% de la población adulta de la región es menor de 35 años – Nativos Digitales

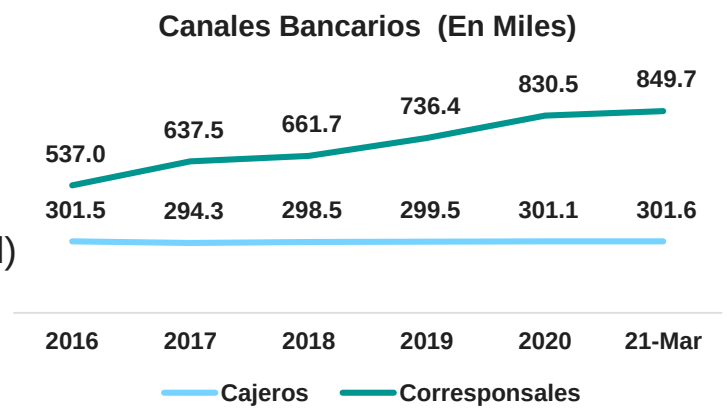
70% tiene acceso a celular inteligente actualmente (+ información, + agil)

Adopción de internet >72% (promedio mundial 60%)

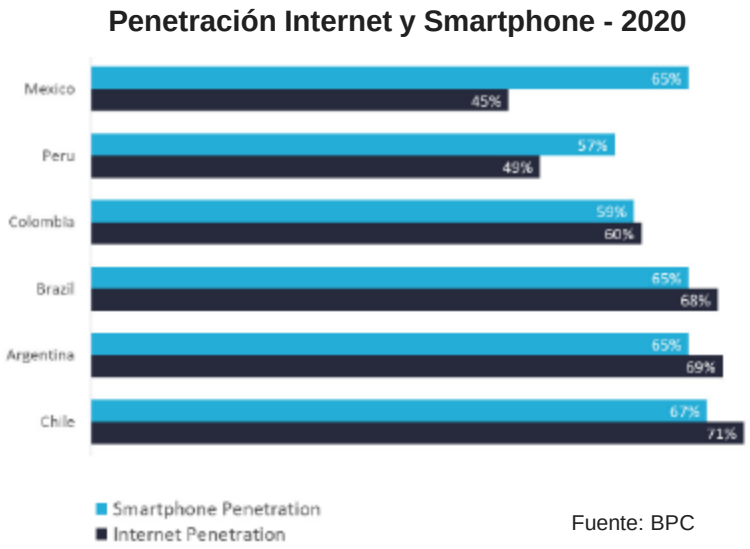
La pandemia ha acelerado el uso de soluciones digitales para la población en general.

Más de la mitad de la población no está bancarizada, se convierte en una oportunidad en el contexto digital y post-pandemia

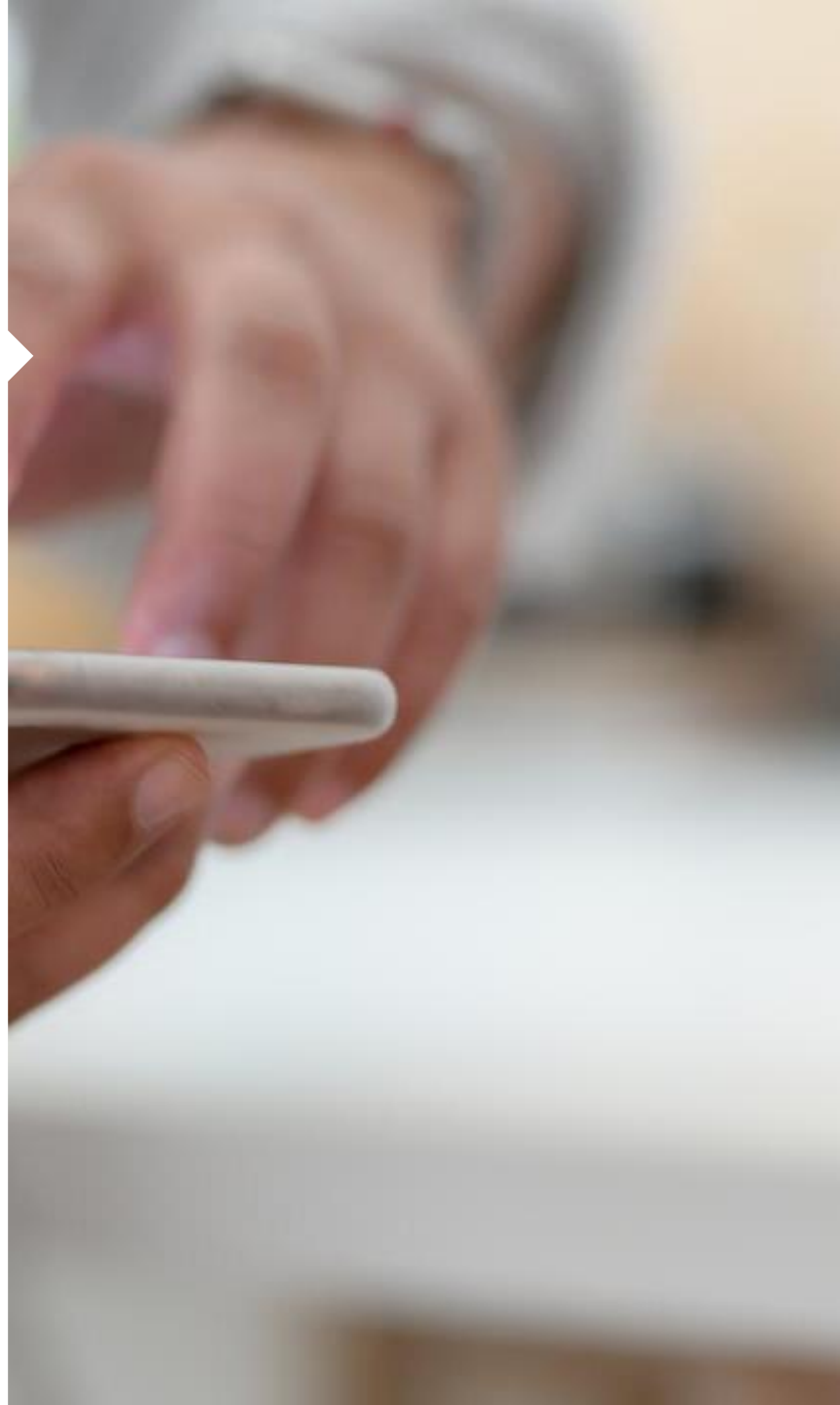
Más empoderado, + personalización y voz propia sobre qué hacer



Fuente: Felaban



Fuente: BPC



Marsh

Marsh

Estudio de Gestión del Riesgo Cibernético en el Sector Financiero Latinoamericano

2023

A business of Marsh McLennan

¿Cuál es el impacto real de los riesgos en las organizaciones

¿Qué retos enfrentan las organizaciones en la gestión del riesgo?

¿Cómo damos el siguiente paso hacia la implementación de metodologías cuantitativas de riesgos?

CIO

¿**Cuánto riesgo** tenemos? ¿Estamos **gastando mucho o poco** en mitigación?

CRO

¿Se solucionaron los problemas de **alta prioridad?**

CEO

“No queremos ser el próximo titular de las victimas de ciberataque, ¿estamos **haciendo lo suficiente** para minimizar el riesgo?”

CISO

“¿Estamos gastando nuestro **presupuesto** de ciberseguridad en los recursos adecuados? **¿Cuál es el ROSI?**

Riesgos

“xPd%y/ uo%jd0 hTfrX#, tr&5iu! hTo/u”, uR hX&dtfR 30%”

Panorama del riesgo cibernético en el sector financiero

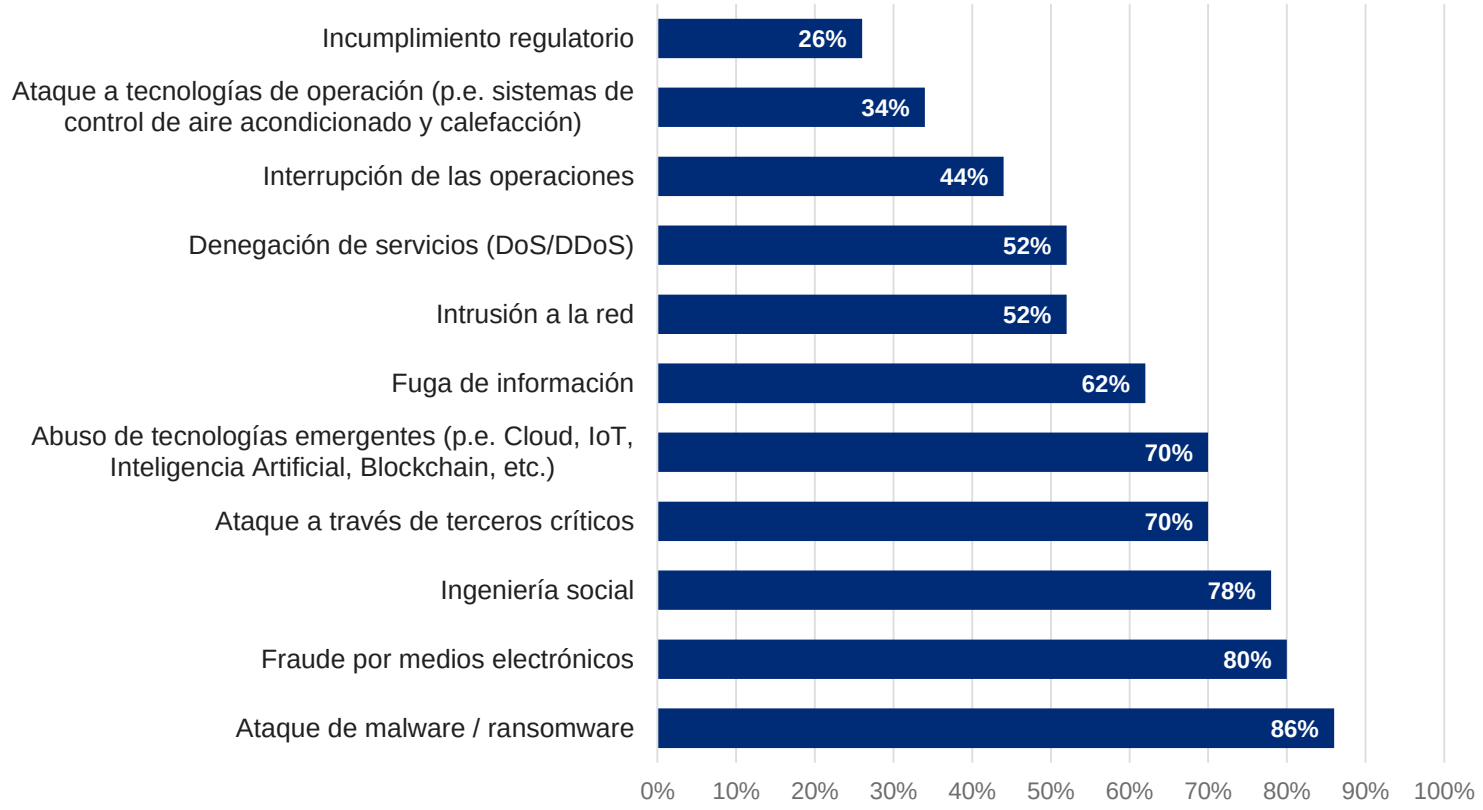
Con base en los resultados obtenidos, se puede corroborar que la **ingeniería social** sigue teniendo el mayor índice de materialización en las empresas encuestadas.

Los atacantes utilizan correos electrónicos, mensajes de texto y llamadas telefónicas falsas para engañar a las personas y obtener información confidencial, como contraseñas, o números de tarjetas de crédito o tokens (OTP).

Panorama del riesgo cibernético en el sector financiero

En algunos países como Perú, Colombia, México y República Dominicana, es donde se observa que los riesgos mencionados anteriormente se han materializado con mayor frecuencia en las organizaciones encuestadas.

En **República Dominicana** y Perú **más del 60% de las organizaciones se han visto afectadas por el fraude por medios electrónicos y la ingeniería social**; mientras que en el caso de Colombia esta cifra se encuentra entre el 42% y el 50%, respectivamente.
En México es del 43% cuando se trata de ingeniería social.



Percepción de los riesgos que se incrementarán en los próximos años

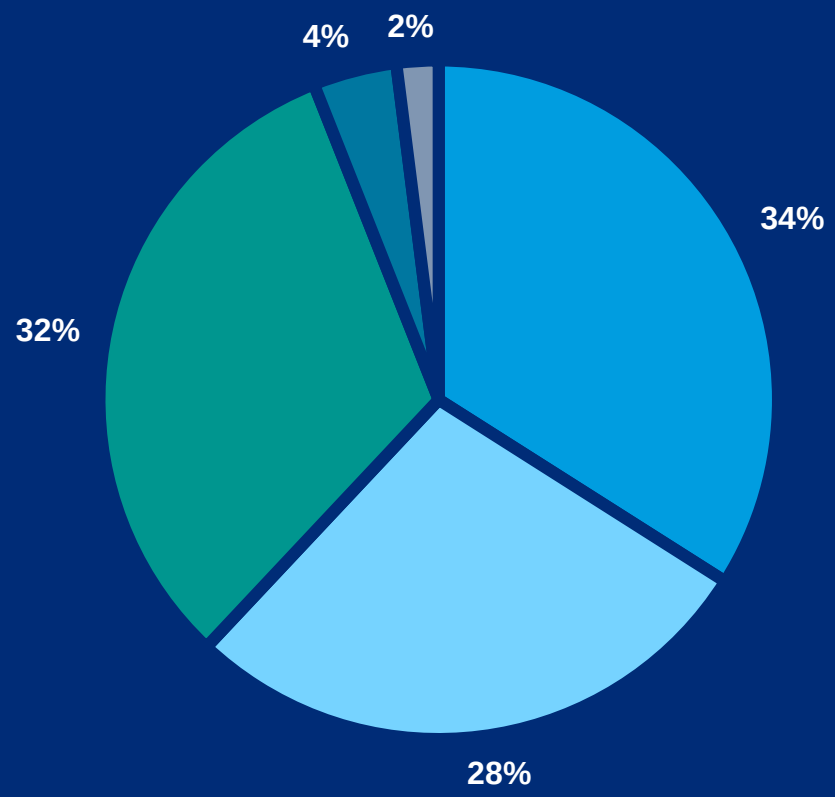
(*) Otros: errores humanos

¿Cómo estamos evaluando el riesgo de seguridad de la información y ciberseguridad?

Metodologías de evaluación

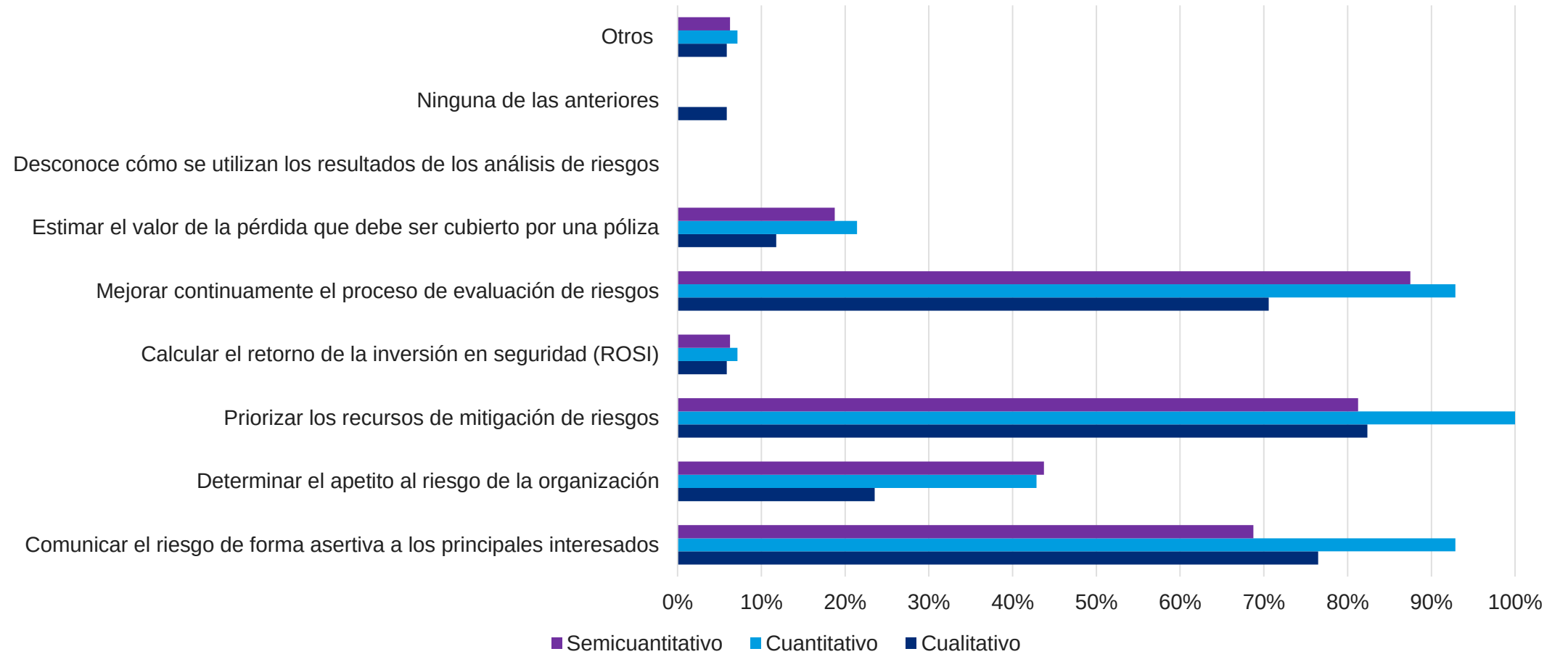
Los resultados arrojados por la encuesta demuestran que el uso de metodologías de análisis cualitativo y semicuantitativo para el análisis y evaluación de riesgos de seguridad de la información siguen siendo las más utilizadas por las organizaciones.

Solo el 28% de los encuestados informan que usan metodologías cuantitativas.



- Metodología de análisis cualitativo
- Metodología de análisis cuantitativo
- Metodología de análisis semicuantitativo
- No cuenta con una metodología de análisis de riesgos de SI
- No sabe

¿Cómo estamos evaluando el riesgo de seguridad de la información y ciberseguridad?



Principales retos y dificultades en la gestión de riesgos

Falta de conocimiento de las personas sobre gestión de riesgos **(52%)**

Desconocimiento de la metodología de análisis de riesgos de la organización **(44%)**

Desconocimiento de los valores estimados de los activos críticos de la organización **(52%)**

Evolución constante de las amenazas

Complejidad de los sistemas y tecnologías

Cambios normativos y de cumplimiento

Escasez de talento especializado - Falta de conciencia y cultura de seguridad

Gestión del riesgo en la cadena de suministro

...los riesgos a los cuales se

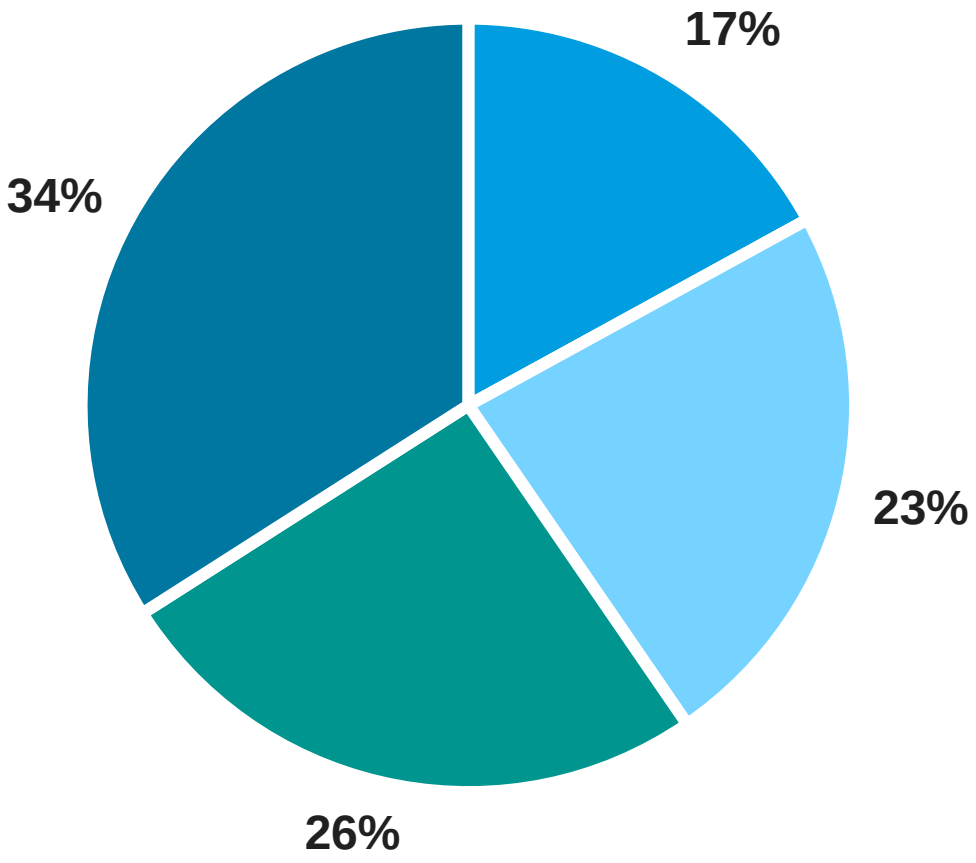
Principales retos y dificultades en la gestión de riesgos

Falta de conocimiento de las personas sobre gestión de riesgos	Desconocimiento de la metodología de análisis de riesgos de la organización	Desconocimiento de los valores estimados de los activos críticos de la organización	Evolución constante de las amenazas	Complejidad de los sistemas y tecnologías
Invertir en capacitación y desarrollo interno	Entrenamiento en gestión de riesgos	Inventariar los activos de información	Mantenerse actualizado	Generar y mantener actualizado un inventario de los activos
		Evaluaciones de activos de información	Implementar soluciones de seguridad y mantenerlas actualizadas	Aplicar prácticas de seguridad en el diseño

Principales retos y dificultades en la gestión de riesgos

Escasez de talento especializado	Cambios normativos y de cumplimiento	Gestión del riesgo en la cadena de suministro	Falta de conciencia y cultura de seguridad
Invertir en capacitación y desarrollo interno	Mantenerse informado sobre las leyes y regulaciones	Evaluar proveedores	Programas de capacitación y concientización
Alianzas con universidades	Establecer un programa de cumplimiento	Establecer acuerdos contractuales	Liderazgo y compromiso
Trabajar con proveedores de gestión de riesgos			

¿Cómo se definen los escenarios en las organizaciones?



- **Es difícil definir los escenarios de riesgos** debido a que hay diferentes factores que influyen en la definición de los mismos (agentes de amenaza, vulnerabilidades, vectores de ataques, etc).
- **No son lo suficientemente claros** para todas las personas involucradas en el análisis, por lo cual, no se identifican claramente las consecuencias de la materialización del riesgo en el negocio
- **Son claros para todas las personas** que realizan la evaluación del riesgo, por lo cual pueden identificar claramente las consecuencias de la materialización del riesgo en el negocio
- **Son definidos por personal experto** y/o tomados de hechos reales ocurridos en la industria

¿Cuáles son las fuentes que utilizan las organizaciones para determinar el riesgo?

Es importante que se tengan a la mano, fuentes de información tanto internas como externas con el fin de que todos los participantes a los talleres de riesgos, tengan un panorama más claro de los riesgos y amenazas que enfrenta la organización.

Impacto de los riesgos en las organizaciones

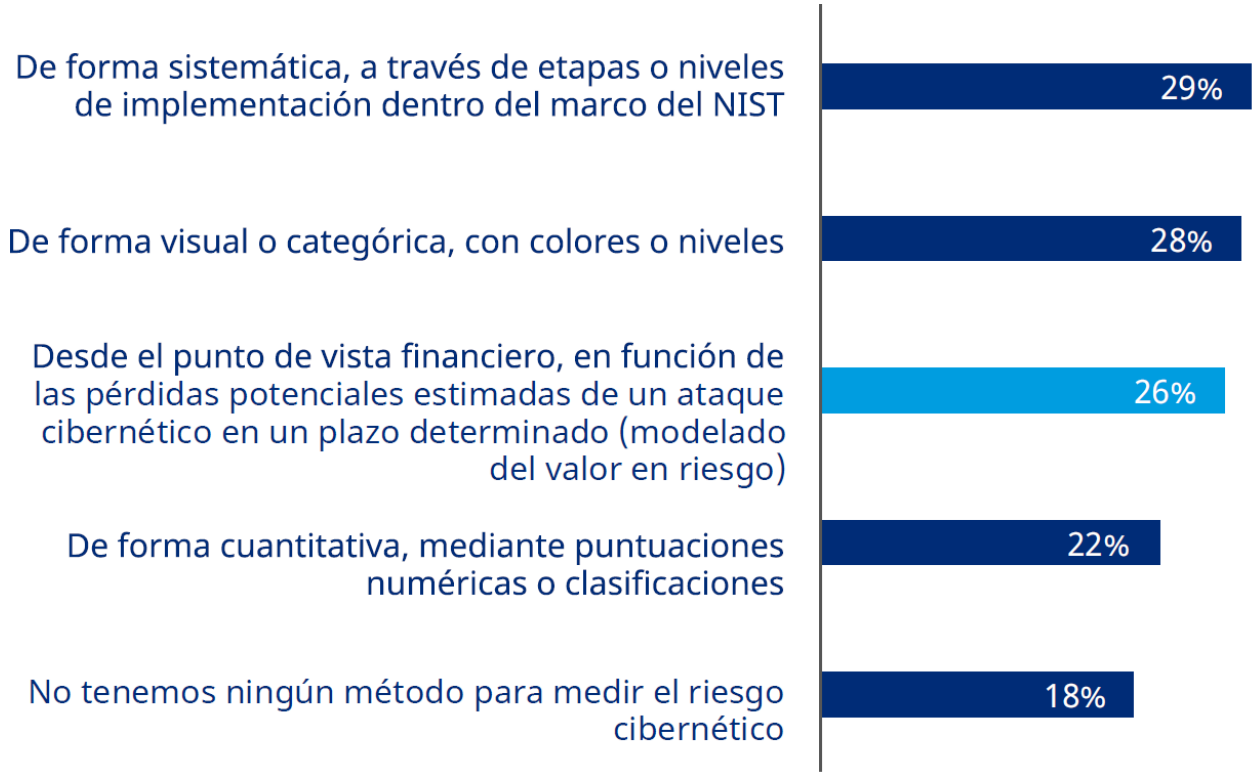
Un incidente de seguridad puede generar pérdidas en diversos aspectos a nivel organizacional

1. Pérdida de ingresos
2. Afectación de la reputación
3. Costos de restauración
4. Costos de brechas de datos
5. Fraude o robo de dinero
6. Multas y sanciones / Costos de litigios
7. Costos de respuesta ante ciberincidentes
8. Ciberextorsión

¿Conoce cuál es el verdadero costo del riesgo cibernético en su organización?

Muchas organizaciones aún no miden el riesgo cibernético en términos financieros, lo que afecta su capacidad para comunicar efectivamente las principales ciberamenazas

Método utilizado para medir la exposición al riesgo cibernético



Fuente: Estado de la resiliencia cibernética 2022 Marsh - Microsoft

Solo el

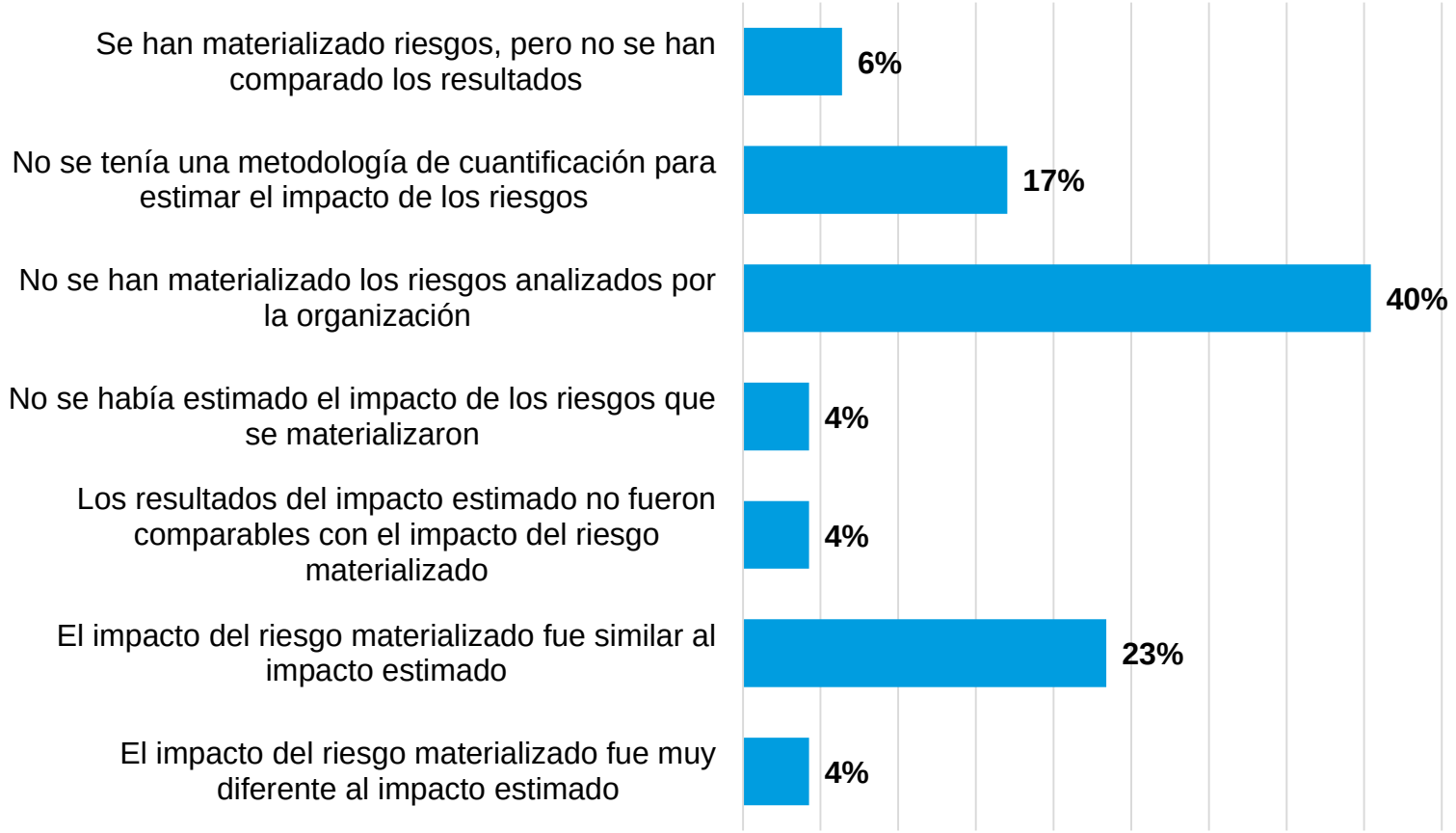
26%

de los encuestados indicaron que su organización medía el riesgo cibernético en términos financieros

Marsh

Impacto de los riesgos en las organizaciones

Solo el 23% de los encuestados informan que el impacto del riesgo materializado fue similar al impacto del riesgo estimado



¿Por qué cuantificar el ciberriesgo?

Comparación y priorización de riesgos

Retorno a la inversión en Seguridad (ROSI)

Comunicación más clara y efectiva

Apoyo a la toma de decisiones basada en datos

Cumplimiento regulatorio y exigencias del mercado

Mayor precisión en la evaluación de riesgos

Integración con otros procesos de gestión

...los riesgos a los cuales se

¿Por qué cuantificar el ciberriesgo?

Comunicación a los stakeholders

Priorizar las implementaciones y mejoras de ciberseguridad en línea con el posible impacto potencial para la organización.

- Entender el **retorno de la inversión en ciberseguridad** y la posible afectación para la organización en caso de su materialización
- **Evaluar el presupuesto de ciberseguridad** en línea con el posible impacto económico
- **Definir los límites del seguro de riesgo** cibernético a contratar

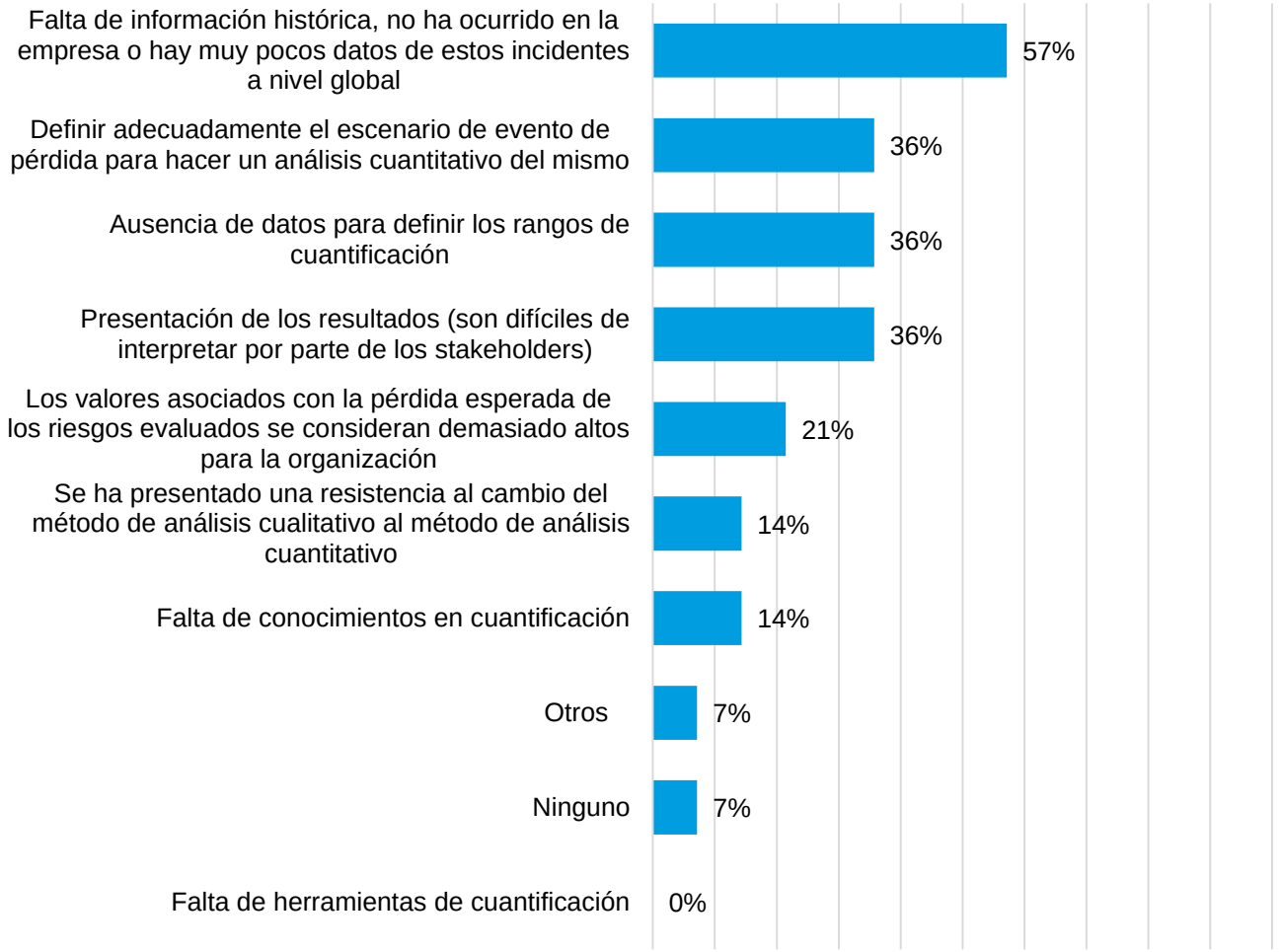
Entender el impacto potencial de los principales ciberriesgos en la organización, identificar aquellos que superan los niveles de tolerancia y asegurar que se definan planes de tratamiento apropiados y oportunos.

- Brindar un **enfoque más estratégico** a su gestión
- Estructurar estrategias de seguridad de la información y ciberseguridad basadas en riesgos y en el impacto financiero de la organización
- **Preparar casos de negocio** sustentados en la posible pérdida ante la materialización de ciberriesgos

- **Entender el impacto de los principales ciberriesgos en la organización**.
- **Brindar los recursos adecuados** para la implementación de las estrategias de ciberseguridad y supervisar su progreso y cumplimiento de objetivos

Retos de la cuantificación de riesgos

- Los enfoques cuantitativos **pueden ser a veces complejos** y requerir más tiempo que los enfoques cualitativos, lo que limita su escalabilidad.
- Según el enfoque que se le quiera dar, es necesario contar con una **herramienta de gestión de riesgos automatizada** y una base de datos asociada.
- Requiere de **personal capacitado y entrenado** para poder ejecutar la metodología y las herramientas utilizadas
- Depende en gran medida de la **disponibilidad de datos fiables.**
- Requiere una evolución a través de **múltiples iteraciones** para asegurar su correcto funcionamiento en la organización



Retos de la cuantificación de riesgos

Disponibilidad y calidad de los datos	Capacidad y experiencia en análisis cuantitativo	Interpretación y comunicación de resultados	Costos y recursos
Fuentes internas	Evaluar las capacidades y conocimientos de las organización	Desarrollar informes y visualizaciones claras y comprensibles	Análisis costo-beneficio para justificar la inversión en cuantificación
Fuentes externas	Proporcionar capacidad y desarrollo profesional	Resultados alineados con los objetivos y las necesidades de los responsables de la toma de decisiones	Asignar presupuesto adecuado para recursos tecnológicos, herramientas de análisis y personal capacitado
Opinión de expertos	Contratación de personal experto o asesoría de consultores externos		

CIO

¿Cuánto riesgo tenemos? ¿Estamos gastando mucho o poco en mitigación?

CRO

¿Se solucionaron los problemas de alta prioridad?

CEO

“No queremos ser el próximo titular de las victimas de ciberataque, ¿estamos haciendo lo suficiente para minimizar el riesgo?”

CISO

“¿Estamos gastando nuestro presupuesto de ciberseguridad en los recursos adecuados? ¿Cuál es el ROSI?

Riesgos

“Les voy a mostrar el reporte de cuantificación de riesgos. Este responderá todas sus preguntas”.

Recomendaciones

Gestionar el riesgo cibernético es una prioridad crítica para el sector financiero al enfrentarse a amenazas cibernéticas que aumentan en sofisticación y frecuencia que ponen en riesgo la seguridad de la información, la continuidad del negocio y la confianza de los clientes.
Ante esta realidad, es importante tener en cuenta las siguientes recomendaciones:

Identificación y evaluación de activos de información

Implementar metodologías de análisis cuantitativo de riesgos

Establecer estrategias de gestión del riesgo

Comunicación estratégica del riesgo cibernético

Análisis del impacto de los riesgos

Gestión del riesgo en la cadena de suministro

Mantenerse actualizado

Capacitación y entrenamiento

Recopilación y análisis de datos para la cuantificación de riesgos

Conclusiones

1

Las bandas de cibercriminales están operando activamente en la región, por lo que debemos definir nuestra estrategia de ciberseguridad pensando que un ataque es inminente.

2

Es importante definir mecanismos para demostrar el retorno a la inversión en proyectos de seguridad como una forma de buscar recursos alineados a los objetivos y apetito de riesgo de la organización.

3

El entorno de riesgos nos obliga a reevaluar las prioridades a nivel de seguridad y ciberseguridad, desde los controles que venimos implementando hasta la evaluación de esquemas de transferencia como el seguro de riesgo cibernético.

Marsh

Estudio de gestión del riesgo cibernético en el Sector Financiero 2023

Ángela Paola Cubillos

Líder de Consultoría en Riesgo Cibernético para Colombia

angela.cubillos@Marsh.com

César Rodríguez

Líder de Consultoría de Marsh Advisory para República Dominicana

Cesar.Rodriguez@marsh.com

MarshMcLennan

We are leaders in risk, strategy and people. One company, with four global businesses, united by a shared purpose to make a difference in the moments that matter.

Marsh GuyCarpenter Mercer OliverWyman

Tienes algunas Preguntas?