Marsh

Estudio de Gestión del Riesgo Cibernético en el Sector Financiero Latinoamericano

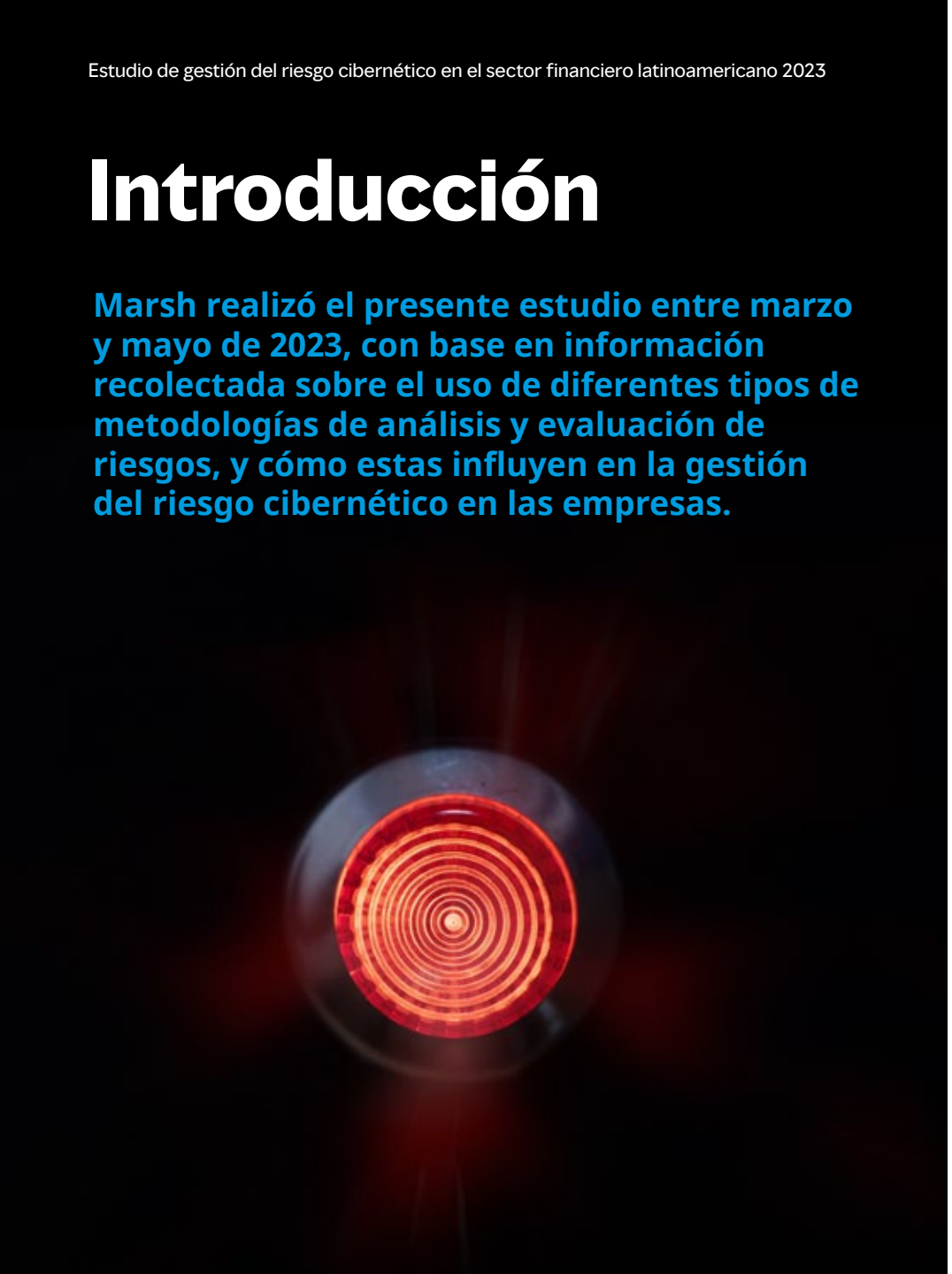
2023

A business of Marsh McLennan

Contenido

Introducción

Marsh realizó el presente estudio entre marzo y mayo de 2023, con base en información recolectada sobre el uso de diferentes tipos de metodologías de análisis y evaluación de riesgos, y cómo estas influyen en la gestión del riesgo cibernético en las empresas.



El objetivo del estudio es dar a conocer el panorama del riesgo cibernético en el sector financiero, proporcionar información relevante a las organizaciones sobre el uso de metodologías de análisis y evaluación de riesgos y ofrecerles recomendaciones prácticas que les permitan mejorar y madurar sus procesos de gestión de riesgos de seguridad de la información y ciberseguridad, específicamente en lo que se refiere al uso de metodologías de cuantificación de riesgos.

Las personas que fueron encuestadas están directamente involucradas en la gestión de riesgos de sus empresas, desempeñando cargos en las áreas de riesgos o seguridad de la información, y trabajan para empresas de diferentes tamaños del sector financiero en Latinoamérica.

¿Qué retos enfrentan las organizaciones en la gestión del riesgo? ¿Cuál es el impacto real de los riesgos en las organizaciones? ¿Cómo damos el siguiente paso hacia la implementación de metodologías cuantitativas de riesgos? El Estudio de Gestión del Riesgo Cibernético en el Sector Financiero 2023 de Marsh tiene las respuestas a estas y otras preguntas que nos permitirán entender por qué, hoy más que nunca, implementar metodologías cuantitativas de gestión de riesgos permitirá a las organizaciones comprender mejor la exposición que tienen frente al riesgo cibernético, optimizar las inversiones en seguridad y mejorar la toma de decisiones estratégicas.

Resumen Ejecutivo

La gestión del riesgo cibernético se ha convertido en una prioridad crítica para el sector financiero en un mundo cada vez más digitalizado. Las organizaciones se enfrentan a amenazas cibernéticas que aumentan en sofisticación y frecuencia, y que ponen en riesgo la seguridad de la información, la continuidad del negocio y la confianza de los clientes. Ante esta realidad, es fundamental adoptar enfoques que permitan gestionar los riesgos de seguridad de la información y ciberseguridad de manera efectiva.

La buena noticia es que las empresas han comprendido que para que esa gestión sea efectiva, es necesario tener una visión más clara de su exposición al riesgo, que les permita tomar decisiones informadas sobre la inversión en seguridad y priorizar medidas de protección. Para llegar a esa meta, los resultados de la encuesta realizada nos han permitido identificar cómo las empresas, a través de la implementación de diferentes tipos de metodologías de gestión de riesgo, han logrado entender cuál es su exposición al riesgo, aunque en ese camino, algunos retos y desafíos los han hecho entender la relevancia de mejorar y madurar estos procesos. A continuación mencionamos los principales hallazgos:

Panorama del riesgo cibernético en el sector financiero

- Se ha presentado un aumento en la sofisticación y frecuencia de los ataques cibernéticos en el sector financiero. Los ataques de ingeniería social siguen siendo una de las amenazas más comunes y efectivas, y que más han afectado a las organizaciones encuestadas.
- Se percibe entre los encuestados que adicional a los ataques de ingeniería social, los ataques de malware y, particularmente, ransomware, fraude por medios electrónicos, y ataques a través de proveedores y terceros, se seguirán incrementando en los próximos años.

Evaluación del riesgo de seguridad de la información y ciberseguridad

- El uso de metodologías de análisis cualitativo y semicuantitativo para el análisis y evaluación de riesgos de seguridad de la información y ciberseguridad, siguen siendo las más utilizadas por las organizaciones. Solo el 28% de los encuestados informan que usan metodologías cuantitativas.
- El 64% de las empresas que utilizan metodologías cualitativas, y el 44% de las que utilizan metodologías semicuantitativas han considerado cambiarlas debido a que:
  - No se puede determinar el valor de la pérdida esperada para los riesgos evaluados.
  - Las escalas utilizadas en metodología de análisis de riesgos son subjetivas.
  - Los resultados de los análisis de riesgos son insuficientes para la toma de decisiones.
- El 71% de las organizaciones que cuentan con metodologías cuantitativas indican que los resultados arrojados por este tipo de metodologías les ha permitido:
  - Aprobación de grandes iniciativas y proyectos en seguridad de la información y ciberseguridad.
  - Priorización de recursos de mitigación de riesgos según el impacto en el negocio de los riesgos evaluados.
  - 78% de los encuestados indicaron que les ha permitido la contratación de personal adicional.
- Adicionalmente, el 57% de las organizaciones que cuentan con metodologías cuantitativas indicaron que, con base en los resultados obtenidos de la ejecución de esta metodología, se ha modificado el presupuesto destinado a ciberseguridad; y el 43% ha contratado un seguro de riesgo cibernético.

Definición de los escenarios de riesgos

Muchas organizaciones no le asignan adecuados recursos y tiempo a la definición de escenarios de riesgo de seguridad de la información y ciberseguridad, lo cual tiene un efecto directo en los resultados de sus evaluaciones de riesgo debido a que los escenarios no terminan siendo entendidos en su totalidad, dificultando la definición de sus niveles de probabilidad y de impacto.

- Una tercera parte de las organizaciones encuestadas reporta que los escenarios de riesgos son definidos por personal experto o tomados de hechos reales ocurridos en la industria. Sin embargo, el 17% de los encuestados reconocen que se presentan retos en la definición de los escenarios, debido a que hay diferentes factores que influyen en la definición de los mismos, como los agentes de amenaza que pueden explorar las vulnerabilidades y los vectores de ataques, entre otros.
- El 23% de las organizaciones consideran que los escenarios definidos no son lo suficientemente claros para todas las personas involucradas en el análisis, por lo cual no se identifican adecuadamente las consecuencias de la materialización del riesgo en el negocio.

Datos utilizados durante las evaluaciones de riesgos

Teniendo en cuenta la relevancia de tener datos confiables para determinar el impacto y la probabilidad de ocurrencia de un riesgo que enfrente la organización, identificamos que las empresas encuestadas obtienen estos datos de la siguiente manera:

- El 80% de los encuestados obtiene la información de incidentes de seguridad ocurridos en la organización y de los incidentes ocurridos en la industria o en la región.
- El 66% de los encuestados obtiene la información de personal experto de la organización.
- El 10% de los encuestados indicó que también utilizan información de los análisis internos realizados por la organización, de publicaciones de compañías expertas, información entregada por el SOC, y de las métricas internas de apetito y tolerancia al riesgo.

Principales retos y dificultades en la gestión de riesgos

Gestionar los diferentes tipos de riesgos en las organizaciones no es una tarea sencilla, y menos cuando no se cuenta con metodologías adecuadamente definidas para gestionar cada uno de ellos. Cuando se trata de riesgos de seguridad de la información y ciberseguridad, la mitad de los encuestados identificaron las siguientes dificultades que enfrentan sus organizaciones durante la gestión de este tipo de riesgos:

- Falta de conocimiento de las personas sobre gestión de riesgos.
- Desconocimiento, por parte de los empleados, de la metodología de análisis de riesgos de la organización.
- Desconocimiento de los valores estimados de los activos críticos de la organización.

Impacto de los riesgos en las organizaciones

Según los factores que se analicen durante los análisis y evaluaciones de riesgos, las estimaciones realizadas por las organizaciones frente a las afectaciones económicas de los riesgos materializados pueden variar significativamente o ser bastantes cercanas. Al respecto, identificamos los siguientes resultados sobre los análisis que han realizado las organizaciones de las cifras de un riesgo materializado frente a la estimación del mismo riesgo:

- El 23% de los encuestados indicó que el impacto del riesgo materializado fue similar al impacto estimado.
- El 17% indicó que no tenían una metodología de cuantificación para estimar el impacto de los riesgos.
- El 40% de los encuestados indicó que no se les han materializado los riesgos que la organización ha analizado. Sin embargo, en estas organizaciones se han materializado los siguientes riesgos, los cuales deberían incluirse en los análisis debido a que son riesgos cuya frecuencia ha aumentado en los últimos años:

  - Fraude por medios electrónicos
  - Ingeniería social
  - Interrupción de las operaciones
  - Ataque de malware / ransomware
  - Ataque a través de terceros críticos
  - Incumplimiento regulatorio

Retos de la cuantificación de riesgos

Si bien los beneficios de cuantificar los riesgos y conocer la exposición al riesgo en las empresas son bastantes, cuando las organizaciones han tomado la decisión de implementar metodologías de cuantificación de riesgos, han enfrentado algunos retos y desafíos como son:

- **Disponibilidad y calidad de los datos**

  El 57% de los encuestados confirmaron que carecen de información histórica, ya sea porque los riesgos analizados no han ocurrido en la empresa o porque hay muy pocos datos de los incidentes que se analizan a nivel global. El 36% indicó que hay ausencia de datos para definir los rangos de cuantificación.

- **Capacidad y experiencia en análisis cuantitativo:**

  las organizaciones pueden enfrentar desafíos para adquirir y desarrollar capacidades internas de análisis cuantitativos, estadísticas y modelado de riesgos.

- **Interpretación y comunicación de resultados:**

  Los resultados obtenidos a través de metodologías cuantitativas pueden ser complejos y requieren una adecuada interpretación y comunicación. El 36% de los encuestados confirmaron que los resultados son difíciles de interpretar por parte de los stakeholders, y que los valores asociados con la pérdida esperada de los riesgos evaluados se consideran demasiado altos para la organización.

- **Costos y recursos:**

  La adopción de metodologías de cuantificación de riesgos puede requerir inversiones en términos de recursos financieros, tecnológicos y humanos.

Panorama de ciberriesgos en el sector financiero

El panorama de ciberriesgos en el sector financiero ha experimentado cambios significativos en los últimos años, con un aumento en la sofisticación y la frecuencia de los ataques cibernéticos, lo cual ha llevado a la materialización de diversos riesgos, como lo confirmaron quienes participaron en este estudio. Sin embargo, antes de ver algunas cifras que nos permitan entender cómo estos riesgos se han manifestado en las empresas del sector financiero, veamos una breve descripción de los principales riesgos que han afectado a este sector:

Fraude por medios electrónicos

Hace referencia a cualquier tipo de esquema de fraude en el cual se utiliza el correo electrónico, sitios web, salas de chat o foros para presentar solicitudes fraudulentas a posibles víctimas, para realizar transacciones fraudulentas o para transmitir las ganancias del fraude a entidades financieras u otras personas relacionadas con el esquema.

Ingeniería social

Es el acto de engañar a una persona para que revele información confidencial, obtenga acceso no autorizado o realice una acción en contra de su voluntad.

Fuga de información

Corresponde a la liberación intencional o no intencional de información a un entorno no confiable. Es la transmisión no autorizada de datos desde dentro de una organización a un destino o destinatario externo.

Interrupción de las operaciones

Pérdida de ganancias debido a que el negocio no puede operar por la manifestación de un desastre, un incidente tecnológico, un ataque que no permite se realicen las actividades para generar valor.

Ataque de malware / ransomware

El ataque de malware hace referencia al uso de cualquier tipo de software malicioso diseñado para causar daño a una computadora, servidor, red o infraestructura informática, o afectar la confidencialidad, integridad o disponibilidad de la información.

El ransomware es un tipo de malware que busca bloquear el acceso a los archivos a través de mecanismos de cifrado, y en muchos casos extraer información de la organización. Posteriormente, exige un rescate, generalmente en forma de criptomoneda, para restaurar el acceso a los archivos y no publicar la información robada.

Intrusión a la red

Es un acceso no autorizado a la red aprovechando alguna vulnerabilidad. Las intrusiones pueden ser pasivas, en las que la penetración se logra sigilosamente y sin detección; o activas, en las que se efectúan cambios en los recursos de la red.

Denegación de servicios (DoS/DDoS)

Corresponde a un tipo de ataque diseñado para hacer que un servicio sea inaccesible. Para el usuario, parece que el sitio simplemente dejó de mostrar contenido, pero para las empresas, podría significar que los sistemas en línea de los que dependen han dejado de responder.

Un ataque de denegación de servicio (DoS) utiliza solo una pequeña cantidad de sistemas atacantes (posiblemente solo uno) para sobrecargar el objetivo. Por su parte, en un ataque de denegación de servicio distribuido (DDoS), el atacante utiliza una gran cantidad de equipos para que cada uno genere una pequeña cantidad de solicitudes que, sumadas, sobrecargan el objetivo.

Ataque a través de terceros críticos

El riesgo de un ataque a través de terceros es la probabilidad de que la organización experimente un evento adverso (por ejemplo, violación de datos, interrupción operativa o daño a la reputación) por un ataque que no está dirigido directamente a su organización, sino a un tercero que le provee servicios y tiene acceso a su información o tiene interconexión con su red o sus aplicaciones.

Abuso de tecnologías emergentes

Hace referencia al uso inadecuado o aprovechamiento de vulnerabilidades en sistemas basados en nuevas tecnologías (p.e. Cloud, IoT, Inteligencia Artificial, Blockchain, etc.) por parte de un atacante o un usuario malintencionado.

Ataque a tecnologías de operación

Ataque a sistemas que controlan equipos industriales, procesos y eventos (p.e. sistemas de control de aire acondicionado y calefacción) con el objetivo de afectar las operaciones de la organización.

Incumplimiento regulatorio

El incumplimiento regulatorio o normativo hace referencia al riesgo que se manifiesta cuando las organizaciones no logran cumplir con las obligaciones regulatorias (normativas o no) a las cuales se encuentran sujetas, se les aplican multas o sanciones.

Con base en los resultados obtenidos, se puede corroborar que los ataques de ingeniería social siguen siendo una de las amenazas más comunes y efectivas, y que más han afectado a las organizaciones encuestadas. Los atacantes utilizan correos electrónicos, mensajes de texto y llamadas telefónicas falsas para engañar a las personas y obtener información confidencial como contraseñas, números de tarjetas de crédito o tokens (OTP). Por otro lado, estos ataques también pueden estar relacionados a estafas para lograr que la víctima realice transferencias no autorizadas al suplantar la identidad de un cliente, proveedor o ejecutivo de la compañía. En otros casos, la ingeniería social termina siendo el punto de acceso para ataques más sofisticados, como en casos de amenazas persistentes avanzadas. Según el reporte Phishing Activity Trends* del Anti-Phishing Working Group, durante el último trimestre de 2022 los ataques de phishing formaron el 27.7% de los ataques al sector financiero, lo que representó la cantidad más alta para ese riesgo durante el año. A este riesgo le siguen el fraude por medios electrónicos y la interrupción de las operaciones.

Riesgos que se han materializado en las organizaciones

* https://docs.apwg.org/reports/apwg_trends_report_q4_2022.pdf?_ga=2.223694107.1444245937.1685549801-1851616714.1685549801&_gl=1*a6y1wn*_ga*MTg1MTYxNjcxNC4xNjg1NTQ5ODAx*_ga_55RF0RHXSR*MTY4NTU0OTgwMS4xLjEuMTY4NTU0OTgyMy4wLjAuMA

Como se mencionó anteriormente, se ha presentado un aumento en la sofisticación y frecuencia de los ataques cibernéticos en el sector financiero. Desafortunadamente, se percibe entre los encuestados que adicional a los ataques de ingeniería social, los siguientes riesgos se seguirán incrementando en los próximos años:

Ataques de malware/ransomware

Los ciberdelincuentes han dirigido sus ataques hacia instituciones financieras, aprovechando su dependencia tecnológica y la criticidad de sus datos, así como la relevancia de los reguladores en este sector. Acorde al reporte de Sophos, The State of Ransomware in Financial Services 2022*, 55% de las entidades de servicios financieros fueron atacados por ransomware en el 2021; dentro de estos ataques, el 54% fueron exitosos al cifrar los datos de las organizaciones.

Fraude por medios electrónicos

De acuerdo al State of Fraud Benchmark Report 2022* de Alloy, el 70% de las instituciones financieras que hicieron parte del estudio mencionaron que fueron víctimas de por lo menos US$500,000 por fraude en el 2022.

Ataques a proveedores y terceros

Los ciberdelincuentes se están enfocando cada vez más en la cadena de suministro y los socios comerciales de las instituciones financieras. Atacar a un proveedor puede proporcionarles acceso indirecto a los sistemas de una entidad financiera. Acorde al 2022 Third Party Breach Report* de Black Kite, la industria financiera ocupa el cuarto lugar entre las industrias más afectadas por brechas de datos de terceros con un 4%. Cybersecurity Dive menciona que el 98% de las organizaciones a nivel mundial tienen integraciones con al menos un tercero que ha sido afectado por un ataque en por lo menos los últimos dos años.

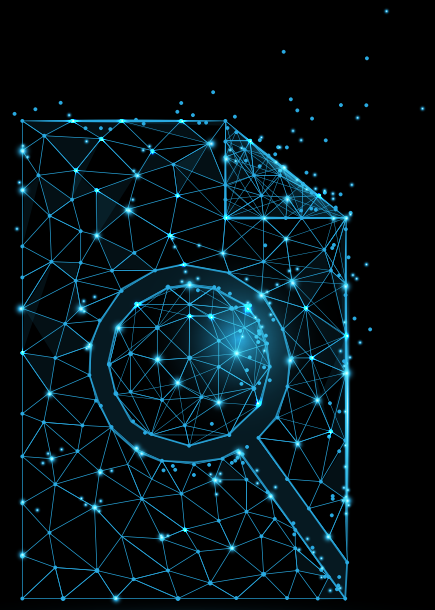
* https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-financial-services
* https://www.alloy.com/state-of-fraud-benchmark-report
* https://blackkite.com/wp-content/uploads/2022/01/Third-Party-Breach-Report-2022.pdf
* https://securityscorecard.com/blog/close-encounters-of-the-third-and-fourth-party-kind-blog/

Percepción de los riesgos que se incrementarán en los próximos años

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.

Metodologías de evaluación

Actualmente, las organizaciones utilizan diferentes tipos de metodologías al momento de realizar análisis y evaluaciones de riesgos de seguridad de la información y ciberseguridad. Entre estas se incluyen: metodologías cualitativas, semicuantitativas y cuantitativas.



Los resultados arrojados por la encuesta demuestran que el uso de metodologías cualitativas y semicuantitativas 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.**

Aunque el 4% de los encuestados indicaron que no cuentan con una metodología específica para el análisis de riesgos de seguridad de la información, los demás encuestados indicaron que el uso de metodologías especializadas en la gestión del riesgo de seguridad de la información y ciberseguridad les ha permitido:

- Comunicar el riesgo de forma asertiva a los principales interesados
- Priorizar los recursos de mitigación de riesgos
- Mejorar continuamente el proceso de evaluación de riesgos

A continuación detallamos cómo funcionan cada una de las metodologías mencionadas anteriormente, cuáles son sus beneficios y limitaciones, qué estándares de referencia existen para la gestión de riesgos y cuáles herramientas se utilizan.

Metodologías cualitativas de evaluación de ciberriesgos

Las metodologías cualitativas se basan en las percepciones de las partes interesadas con respecto a la probabilidad de que ocurran riesgos en la organización, e intentan medir su impacto en la reputación de la empresa, las perspectivas financieras y otros factores. La mayoría de las veces, en la evaluación cualitativa se asignan valores sobre una base comparativa u ordinal, como puede ser alto, medio y bajo, o una escala del 1 al 10.

Entre los beneficios que se identifican de este tipo de metodología encontramos:

- El análisis cualitativo es un enfoque de evaluación simple, donde no hay cálculos complejos.
- Determinar el valor monetario de los activos no siempre es necesario, dependerá que la escala de evaluación del impacto que se haya definido.
- Ayuda a evaluar los riesgos de una manera rápida y sencilla.
- Es una metodología adecuada para empresas que están iniciando su proceso de gestión de riesgos.

Por otra parte, se identifican en ocasiones las siguientes limitaciones:

- El análisis se vuelve ambiguo cuando múltiples riesgos caen en la misma categoría, lo que no permite en muchos casos priorizar adecuadamente los riesgos, según lo indicado por el 12% de los encuestados.
- Las escalas utilizadas en la metodología son subjetivas, según lo indicado por el 23% de los encuestados.
- No se puede determinar el valor de la pérdida esperada para los riesgos evaluados, según lo indicado por el 65% de los encuestados.
- Con los resultados arrojados por esta metodología, no se puede realizar análisis de costo / beneficio para las estrategias de mitigación de riesgos, esto como consecuencia del punto anterior.

Las técnicas y herramientas para el análisis cualitativo de riesgos incluyen la evaluación de la probabilidad y el impacto del riesgo, la matriz de probabilidad e impacto, la evaluación de la calidad de los datos del riesgo, la categorización del riesgo, la evaluación de la urgencia del riesgo y el juicio de expertos.

Metodologías semicuantitativas de evaluación de ciberriesgos

Una evaluación de riesgos semicuantitativa es un tipo de evaluación que combina elementos de evaluaciones de riesgos cuantitativas y cualitativas. En una evaluación de riesgos semicuantitativa, algunos aspectos de la evaluación de riesgos se cuantifican mediante una escala numérica, mientras que otros elementos se evalúan mediante juicios subjetivos y opiniones de expertos. La meta es ofrecer una escala con un rango lo suficientemente amplio como para que el riesgo pueda evaluarse con precisión, lo que la hace más fácil de priorizar un gran número de riesgos en comparación con lo que sería mediante un rango cualitativo normal.

Los formatos en Excel son las herramientas más utilizadas para la ejecución de las metodologías de análisis de riesgos cualitativa y semicuantitativa de seguridad de la información y ciberseguridad, con un 65% de los participantes indicando que los usan. Otros encuestados indicaron usar herramientas de análisis cualitativo de riesgos, y solo el 6% desconocía si se utilizaba una herramienta para realizar análisis de riesgos.

Entre los beneficios que se identifican de este tipo de metodología encontramos:

- Tiene un enfoque más consistente y riguroso para evaluar, y comparar riesgos y estrategias de gestión de riesgos que la evaluación cualitativa de riesgos.
- Al tener un rango más amplio de evaluación, permite priorizar mejor los riesgos que en la metodología cualitativa.
- No requiere posibles cálculos complejos, como en la evaluación cuantitativa.

Por otra parte, se identifican en ocasiones las siguientes limitaciones:

- No permite en muchos casos priorizar adecuadamente los riesgos, según lo indicado por el 25% de los encuestados.
- Las escalas utilizadas en la metodología son subjetivas, según lo indicado por el 37% de los encuestados.
- No se puede determinar el valor de la pérdida esperada para los riesgos evaluados, según lo indicado por el 44% de los encuestados.
- Con los resultados arrojados por esta metodología, no se puede realizar análisis de costo / beneficio para las estrategias de mitigación de riesgos, esto como consecuencia del punto anterior.

Metodologías cuantitativas de evaluación de ciberriesgos

Los análisis de riesgos cuantitativos proporcionan información objetiva y datos más precisos que el análisis cualitativo, porque se basan en datos realistas y medibles, utilizados para calcular los valores de impacto que podría generar el riesgo con la probabilidad de ocurrencia. Los resultados generalmente se expresan en términos monetarios y reflejan cuánto dinero puede perder la organización como resultado de los riesgos citados.

Debido a la posibilidad de medir y replicar sus datos, un análisis de riesgo cuantitativo es una de las herramientas más confiables y efectivas para ejecutar. Lo anterior porque proporciona información precisa que los líderes de las empresas pueden usar para determinar el impacto de los riesgos y la cantidad de recursos en los que deben invertir para planificar sus estrategias.

Entre los beneficios que se identifican de este tipo de metodología encontramos:

- El análisis cuantitativo se basa en procesos y métricas objetivos, eliminando la subjetividad.
- El valor de los activos y las opciones de mitigación de riesgos se comprenden bien.
- Las evaluaciones de costo-beneficio se emplean en gran medida, lo que ayuda a la alta dirección a tomar decisiones sobre las estrategias para gestionar los riesgos de una manera más informada, priorizando los riesgos más críticos para la organización.
- Los resultados se expresan en términos económicos, lo que permite comunicar de manera efectiva la exposición al riesgo a la alta dirección y se asignen adecuadamente los recursos para gestionar los riesgos, como lo confirman la totalidad de las organizaciones encuestadas que cuentan con metodologías cuantitativas.
- Ayuda a comprender con precisión las áreas de alto riesgo y la exposición al riesgo en términos financieros.

Por otra parte, se identifican en ocasiones las siguientes limitaciones:

- 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.

Herramientas para la cuantificación de riesgos

El 79% de los encuestados indicaron que para la ejecución de las metodologías de análisis de riesgos utilizan alguna herramienta de cuantificación, entre las cuales se podrían encontrar RiskLens, FAIR-U y Evaluator, entre otras.

Estas herramientas se basan en el modelo FAIR de Open Group* , el cual es el modelo cuantitativo más conocido designado como estándar internacional. FAIR ha formado la base de muchas implementaciones empresariales de análisis de riesgo cuantitativo. Varias empresas de software han estado utilizando el modelo FAIR para crear plataformas que agilizan la recopilación de datos y los cálculos de riesgo. Estas plataformas de software pueden ayudar a los expertos en riesgos a realizar análisis de riesgos cuantitativos o evaluaciones de riesgos cuantitativas utilizando el modelo FAIR. Los resultados van desde puntos de datos recopilados del negocio hasta tablas de pérdidas previamente completadas.

Con la ayuda de la tecnología, los responsables de la toma de decisiones no tienen que clasificar montones de información y números. La aplicación ejecutará los datos a través del modelo FAIR y creará resultados de resumen que son fáciles de entender y evaluar. La exposición al riesgo generalmente se expresa en términos financieros para una mejor legibilidad.

* https://www.opengroup.org/open-fair

A continuación incluimos una breve descripción de las herramientas utilizadas por los encuestados:

RiskLens

RiskLens es una herramienta que le permite a las organizaciones el uso de soluciones basadas en el estándar FAIR para el manejo de riesgos cibernéticos de manera cuantitativa. La herramienta permite el manejo de riesgos en términos financieros, la priorización y justificación de las iniciativas de ciberseguridad, poder cumplir con los requerimientos regulatorios y de privacidad a los que se encuentran obligados las organizaciones y una toma de decisiones informada.

1

FAIR-U

FAIR-U es una herramienta que forma parte del FAIR Institute, la cual permite poner en práctica los conceptos de cuantificación en las organizaciones y realizar análisis de riesgo basados en FAIR. Si bien no es la herramienta de cuantificación más completa, permite poner a prueba el modelo de cuantificación antes de adquirir una herramienta comercial para las organizaciones.

2

Evaluator

Evaluator es un kit de herramientas de análisis de riesgos cuantitativo open source basado en OpenFAIR y estándares de análisis de riesgos. Este kit permite a las organizaciones ejecutar análisis de riesgos enfocados en datos con características repetibles y cuantificables.

3

Estándares de referencia de gestión de riesgos

Para realizar una adecuada gestión de los riesgos a los que se enfrentan las organizaciones, las compañías disponen de varios estándares y marcos internacionales que pueden ayudarlos a identificar y evaluar sus riesgos, y reducirlos a un nivel aceptable. A continuación se presenta una lista de algunos estándares sugeridos:

ISO 31000

Si bien ISO 31000 es el estándar que permite a las organizaciones tener un panorama general sobre la gestión de riesgos, y define directrices que cualquier empresa debe seguir para considerar el riesgo como un elemento de valor, para los temas de seguridad de la información y ciberseguridad se puede complementar con estándares como ISO 27005.

ISO 27001 / ISO 27005

Para las metodologías de gestión de riesgos de seguridad de la información y ciberseguridad, en la mayoría de las ocasiones se toma en cuenta la familia de la ISO 27000, especialmente el conjunto de herramientas de riesgo cibernético liderado por la ISO 27001, la cual contiene los requisitos para la implementación de un sistema de gestión de la seguridad de la información en las empresas. Adicional a esto se encuentra la ISO 27005, la cual menciona las directrices y guías para gestionar el riesgo de seguridad de la información que pudiera llegar a afectar a las organizaciones.

NIST SP 800-30

Es una publicación especial del Instituto Nacional de Estándares y Tecnología (NIST) que se enfoca específicamente en la gestión de riesgos de seguridad de la información. Esta guía proporciona orientación sobre cómo realizar evaluaciones de riesgos, desde la identificación de activos y amenazas, hasta la estimación de las consecuencias y la probabilidad de que ocurran los eventos de riesgo.

FAIR

Dentro de los estándares que se toman en cuenta para la cuantificación, el más utilizado actualmente es el FAIR (Factor Analysis of Information Risk), el cual ayuda a las organizaciones a establecer una metodología cuantitativa que permite la medición del riesgo de acuerdo con factores que estén asociados a los costos que se podrían presentar durante la materialización de un riesgo. Adicionalmente, permite la modelación de escenarios de riesgo más complejos. El uso de este estándar permite en varias ocasiones la integración con herramientas como RiskLens para el cálculo del riesgo.

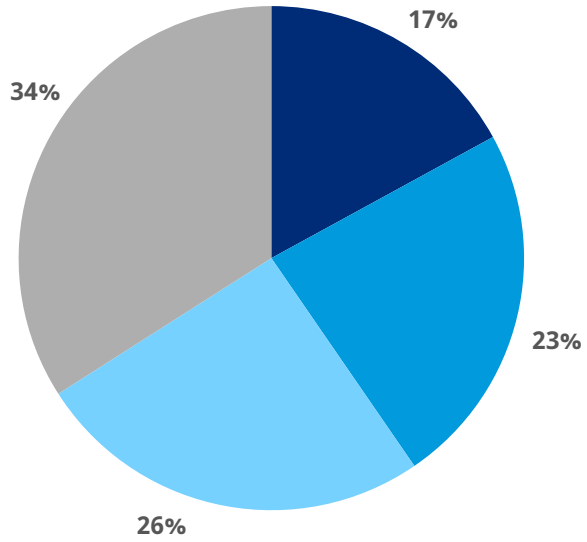
¿Cómo definir un escenario de ciberriesgos correctamente?

Derivado de los ejercicios de evaluación de riesgos que Marsh realiza en sus clientes, se ha observado que el tiempo y análisis dedicado por las organizaciones a la definición de los escenarios de riesgos en muchos casos no es el recomendable, por lo cual, los escenarios de riesgos y sus posibles impactos, no terminan siendo lo suficientemente claros para quienes realizan la evaluación de los riesgos. Lo anterior trae como consecuencia que, al determinar la probabilidad y el impacto de los riesgos definidos, cada persona realice sus propias suposiciones y, consecuentemente, los resultados varíen demasiado de una persona a otra.

Ahora bien, es importante aclarar que siempre se tendrán que hacer suposiciones cuando se hacen análisis de riesgos, porque finalmente se estará haciendo una estimación del impacto que los escenarios podrán causar en la organización, y sobre esto siempre habrá un cierto nivel de incertidumbre. Sin embargo, estas suposiciones deberían reducirse al mínimo y deberán ser claras para todas las personas involucradas durante el análisis de los riesgos.

De acuerdo con el análisis de la información recolectada de la encuesta, identificamos que en el 34% de las organizaciones, los escenarios de riesgos son definidos por personal experto o tomados de hechos reales ocurridos en la industria. El resto de los encuestados identifican que se presentan retos en la definición de los escenarios, debido a que hay diferentes factores que influyen en su definición, como los agentes de amenaza que pueden explotar las vulnerabilidades y los vectores de ataques, entre otros.

Definición de los escenarios de riesgos 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.

Adicionalmente, una vez se identifican los escenarios de riesgos que se quieren evaluar, el 23% de las organizaciones consideran que los escenarios definidos 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.

Es por esto que es importante entrenar al personal involucrado en la gestión de riesgos y dedicar tiempo suficiente para definir adecuadamente los escenarios de riesgos, con el fin de obtener mejores resultados durante el análisis y cuantificación. Esto permitirá disminuir las suposiciones que se hagan alrededor de cada escenario de riesgo analizado y obtener resultados más precisos.

Para tener una idea de cómo podría ser una forma adecuada de definir los escenarios de riesgos, según lo definido por FAIR*, los escenarios de riesgos deberían incluir:

- El activo que puede ser impactado y generaría una pérdida.
- El agente de amenaza que es capaz de actuar contra el activo y explotar sus vulnerabilidades. En el caso del sector financiero, se estima que 56% de los incidentes de ciberseguridad materializados en organizaciones que pertenecen a este sector, provienen de amenazas externas, y 36% internas*.
- El efecto que se causaría sobre el activo y que corresponde al daño a la confidencialidad, integridad o disponibilidad de este, causado por el agente de amenaza.
- Finalmente, pudiera incluirse el método por el cual el agente de amenaza intenta impactar el activo, es decir, el vector de ataque.

¿Qué fuentes de datos utilizamos para mejorar la metodología de gestión de riesgos?

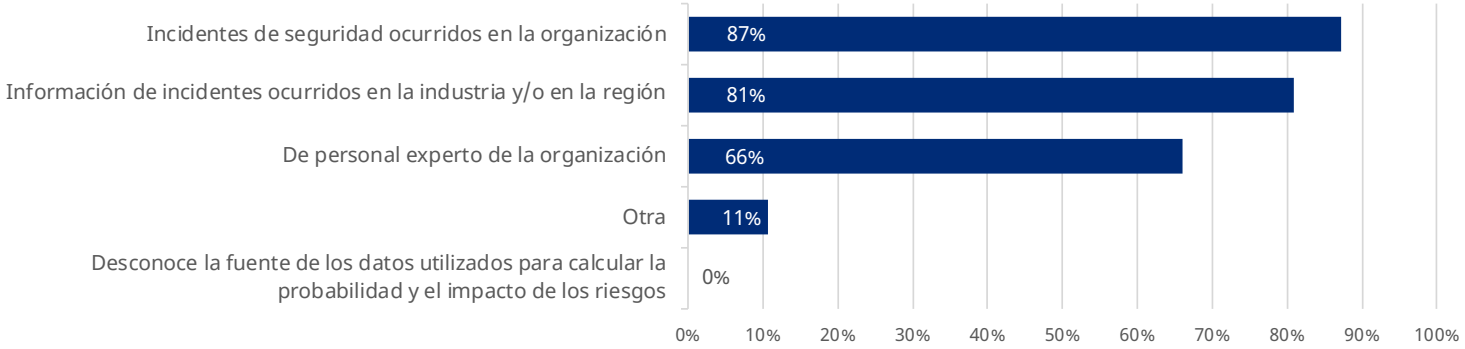
Cuando se hacen talleres de evaluación de riesgo, adicional a entrenar al personal involucrado en la gestión de riesgos y la metodología que tiene la organización para evaluarlos, es necesario que se tengan a la mano fuentes de información tanto internas como externas, con el fin de que todos los participantes tengan un panorama más claro de los riesgos y amenazas que enfrenta la organización. Adicionalmente, esta información será un insumo fundamental para poder hacer un análisis adecuado sobre la probabilidad de ocurrencia y el impacto generado por los riesgos que se evaluarán.

* https://www.fairinstitute.org/blog/in-a-fair-risk-analysis-dont-collect-data-till-you-scope
* https://www.orangecyberdefense.com/global/security-navigator

Sobre esto, consultamos a los encuestados sobre las fuentes de las cuales obtienen los datos para determinar la probabilidad de ocurrencia y el impacto generado por un riesgo de seguridad de la información y ciberseguridad en la organización, obteniendo los siguientes resultados:

- El 87% obtiene información de los incidentes de seguridad que se han materializado en la organización.
- Más del 80% obtienen la información de incidentes de seguridad ocurridos en la organización y de los incidentes ocurridos en la industria o en la región.
- El 66% obtiene la información de personal experto de la organización.
- El 11% de los encuestados indicaron que también utilizan información de los análisis internos realizados por la organización, hacen uso de publicaciones de compañías expertas, información entregada por el SOC y de las métricas internas de apetito y tolerancia al riesgo.

Fuentes de las cuáles se obtienen los datos para los análisis de riesgos



Como se mencionaba anteriormente, para asegurar que los resultados de las evaluaciones de riesgos sean confiables y precisas, se aconseja utilizar fuentes de datos internas y externas como las siguientes:

Fuentes de datos internas

Permiten conocer los tipos de eventos que ocurren en la organización, la frecuencia específica para la empresa y su impacto. Entre las fuentes de datos internas que se pueden consultar se encuentran: reportes de incidentes, resultados de auditorías, resultados de escaneos de vulnerabilidades, registros de accesos a los sistemas, análisis de pérdidas financieras, reclamos de seguros, entre otros.

Fuentes de datos externas

Complementan la información recolectada al interior de la organización con detalles de incidentes ocurridos en la industria o región. Se pueden encontrar fuentes de información externas como las siguiente:

1. **Informes y estadísticas:**

   Algunas organizaciones e instituciones de la industria suelen publicar informes y estadísticas sobre incidentes de seguridad, tendencias de riesgos y mejores prácticas de seguridad. Estos informes pueden ayudar a obtener una perspectiva más amplia sobre los riesgos que puede enfrentar una organización. Por ejemplo, en la página web de Marsh, las organizaciones pueden encontrar este tipo de informes que son de gran utilidad para los análisis de riesgos. Algunos de los informes generados son:

   - El Estado de la Resiliencia Cibernética
   - Encuesta de Ciberseguridad en Sistemas de Control Industrial en Latinoamérica
   - Informe de Riesgos Globales 2023

2. **Inteligencia de amenazas y ciberseguridad:**

   Las fuentes de inteligencia de amenazas y ciberseguridad, como informes de proveedores de seguridad, agencias de inteligencia y organizaciones especializadas, pueden proporcionar información actualizada sobre las últimas amenazas, tácticas de ataque y vulnerabilidades conocidas. Del mismo modo, Marsh cuenta con una base de datos de pérdidas globales que puede ser empleada para brindar información valiosa a los clientes en aspectos relacionados con el seguro de riesgo cibernético y con la gestión del riesgo cibernético. Adicionalmente, entidades como el FS-ISAC pueden brindar inteligencia de amenazas enfocada en la industria financiera.

3. **Regulaciones y marcos de cumplimiento:**

   Las regulaciones y los marcos de cumplimiento, como PCI DSS, leyes de protección de datos personales, entre otros, pueden proporcionar orientación sobre los riesgos y las medidas de seguridad requeridas para ciertos tipos de datos o sectores específicos.

4. **Inteligencia de amenazas y ciberseguridad:**

   Participar en comunidades y foros de seguridad en línea, asistir a conferencias y eventos de seguridad cibernética, puede brindar acceso a conocimientos y experiencias compartidas por profesionales de la ciberseguridad y expertos en el campo.

Opinión de expertos:

También es importante que, durante el proceso de obtención de información, consultar la opinión de los expertos que están dentro y fuera de la organización, y que con su conocimiento pueden aportar información valiosa y sugerir ajustes a la información previamente recolectada, de forma que se adapte a la realidad de la organización. Dentro de la organización, el involucramiento de los expertos de las diferentes áreas de la empresa dependerá del evento de pérdida que se requiere analizar y las áreas que se verán impactadas. Sin embargo, es importante tener presente que es necesario capacitar previamente a los expertos, de forma que puedan expresar su conocimiento en los términos definidos en las metodologías de gestión de riesgos y dejar, adicionalmente, documentadas las suposiciones sobre las cuales se hace la evaluación de los riesgos para tenerlas en cuenta en el momento de presentar los resultados.

Retos en la gestión de riesgos

Gestionar los diferentes tipos de riesgos en las organizaciones no es una tarea sencilla, y menos si no se cuentan con lineamientos y metodologías específicas para gestionar cada uno de ellos. Cuando se trata de riesgos de seguridad de la información y ciberseguridad, la mitad de los encuestados identificaron ciertas dificultades que enfrentan sus organizaciones durante la gestión de este tipo de riesgos. Una de ellas es la falta de conocimiento de las personas sobre gestión de riesgos. Esta falta de conocimiento lleva a las organizaciones a contar con personal que no podría realizar identificación de los riesgos a los cuales se encuentran expuestos y, por lo tanto, no estar al tanto de las medidas que deban tomar o las acciones que deben evitar para que estos riesgos no se materialicen.

Principales retos que enfrentan las organizaciones durante la gestión de riesgos de seguridad de la información y ciberseguridad

También se identifica que hay desconocimiento por parte de los empleados de la metodología de análisis de riesgos de la organización y, adicionalmente, de los valores estimados de los activos críticos de la organización. Como consecuencia de estos dos aspectos, pudiera darse que los análisis y evaluaciones de riesgos podrían arrojar resultados poco confiables e imprecisos, ya que es una información muy relevante al momento de estimar los costos asociados con el impacto económico de una afectación sobre el activo evaluado. Aquí hay que analizar si las organizaciones ya han identificados sus activos de información más críticos, los han clasificado y conocen el valor de estos para la empresa y sus procesos de negocio.

Adicional a lo anterior, durante los procesos de gestión de riesgos de seguridad de la información y ciberseguridad, las organizaciones también pueden enfrentar una serie de retos derivados de los siguientes aspectos:

- **Evolución constante de las amenazas**

  Las amenazas cibernéticas están en constante evolución, con técnicas, tácticas y procedimientos altamente sofisticadas. Las organizaciones deben mantenerse actualizadas sobre las últimas tendencias y tácticas de los ciberdelincuentes, lo que puede resultar difícil debido a la rápida evolución del panorama de la ciberseguridad.

- **Complejidad de los sistemas y tecnologías**

  Las organizaciones suelen utilizar una variedad de sistemas, aplicaciones y tecnologías que pueden ser complejas y altamente interconectadas. Gestionar los riesgos en este entorno complejo requiere una comprensión detallada de la infraestructura tecnológica y las interdependencias entre los sistemas. En el sector financiero en particular aún se encuentran muchas organizaciones con sistemas legacy; mientras que, por otro lado, se encuentran empresas que están implementando ambiciosos programas de transformación digital, con tecnologías emergentes, esquemas de Open Banking e incluso entornos multi-cloud, lo cual puede complicar aún más la arquitectura de la organización.

- **Escasez de talento especializado**

  Existe una escasez de profesionales capacitados en ciberseguridad y gestión del riesgo cibernético. La demanda de expertos en ciberseguridad supera la oferta, lo que dificulta a las organizaciones encontrar y retener personal con habilidades y conocimientos adecuados. Este es un problema común que las organizaciones enfrentan a nivel global en la actualidad.

- **Cambios normativos y de cumplimiento**

  Las regulaciones y normativas relacionadas con la ciberseguridad están en constante evolución. Las organizaciones deben mantenerse actualizadas sobre los requisitos legales y de cumplimiento, y asegurarse de que sus prácticas de gestión del riesgo cibernético estén alineadas con dichos requisitos.

- **Gestión del riesgo en la cadena de suministro**

  Las organizaciones suelen depender de terceros en su cadena de suministro, lo que agrega complejidad a la gestión del riesgo cibernético. Asegurarse de que sus terceras e incluso sus cuartas partes cumplan con los estándares de seguridad, y gestionar los riesgos asociados a la cadena de suministro, puede ser un desafío, particularmente en este sector.

- **Falta de conciencia y cultura de seguridad**

  La falta conciencia y de cultura de seguridad dentro de la organización pueden hacer más difícil la gestión efectiva del riesgo cibernético. La educación y la sensibilización sobre las mejores prácticas de seguridad cibernética son fundamentales para involucrar a los empleados y fomentar una cultura de seguridad sólida.

Algunas recomendaciones que pueden ayudar a superar las dificultades identificadas por las empresas encuestadas y los retos mencionados anteriormente son las siguientes:

• Falta de conocimiento de las personas sobre gestión de riesgos

1. **Invertir en capacitación y desarrollo interno**

   Proporcionar oportunidades de capacitación y certificaciones a los empleados existentes para mejorar sus habilidades en ciberseguridad y gestión del riesgo.

• Desconocimiento por parte de los empleados de la metodología de análisis de riesgos de la organización

1. **Entrenamiento en gestión de riesgos**

   Brindar capacitaciones a los empleados para que conozcan sobre la metodología de análisis de riesgos de la organización y estén capacitados para identificar, analizar y evaluar riesgos.

• Desconocimiento de los valores estimados de los activos críticos de la organización

1. **Inventariar los activos de información**

   Mantener un inventario actualizado de los sistemas, aplicaciones, bases de datos y otros activos de información utilizados en la organización para comprender la infraestructura tecnológica y las interdependencias, así como el valor para la empresa y su nivel de criticidad.

2. **Evaluaciones de activos de información**

   Para cada uno de los activos identificados, realizar una evaluación de los controles implementados sobre los activos con el fin de identificar las vulnerabilidades, amenazas y riesgos a los cuales se encuentran expuestos.

• Evolución constante de las amenazas

1. **Mantenerse actualizado**

   Estar al tanto de las últimas tendencias y tácticas de ciberataques a través de fuentes de inteligencia de amenazas, boletines de seguridad y colaboración con entidades de la misma industria.

2. **Implementar soluciones de seguridad y mantenerlas actualizadas**

   Utilizar herramientas de detección y prevención de amenazas actualizadas, como firewalls, sistemas de detección de intrusiones y soluciones de seguridad para endpoints.

• Complejidad de los sistemas y tecnologías

1. **Generar y mantener actualizado un inventario de los activos**

   Mantener un inventario actualizado de los sistemas, aplicaciones y otros activos de información para comprender la infraestructura tecnológica y las interdependencias.

2. **Aplicar prácticas de seguridad en el diseño**

   Incorporar medidas de seguridad desde la etapa de diseño de sistemas y tecnologías, como la segmentación de red, el múltiple factor de autenticación y el cifrado de datos.

Escasez de talento especializado

1. **Invertir en capacitación y desarrollo interno**

   Proporcionar oportunidades de capacitación y certificaciones a los empleados existentes para mejorar sus habilidades en ciberseguridad y gestión del riesgo.

2. **Alianzas con universidades**

   Trabajar con las universidades de forma que se incluyan materias que permitan a los estudiantes tener la formación necesaria para cubrir las brechas de conocimiento y, posteriormente, facilitar las prácticas universitarias en las empresas, que brinden a los estudiantes la oportunidad de aplicar el conocimiento y adquirir experiencia laboral para continuar trabajando en las organizaciones.

3. **Trabajar con proveedores de gestión de riesgos**

   Trabajar con proveedores externos de servicios de seguridad cibernética que puedan brindar experiencia y conocimientos especializados.

Cambios normativos y de cumplimiento

1. **Mantenerse informado sobre las leyes y regulaciones**

   Estar al tanto de los cambios en las regulaciones y normativas relacionadas con la seguridad de la información, la ciberseguridad y la gestión del riesgo.

2. **Establecer un programa de cumplimiento**

   Implementar políticas y controles de seguridad que se alineen con los estándares y regulaciones aplicables, y realizar auditorías periódicas para evaluar el cumplimiento.

Gestión del riesgo en la cadena de suministro

1. **Evaluar proveedores**

   Para cada uno de los activos identificados, realizar una evaluación de los controles implementados sobre los activos con el fin de identificar las vulnerabilidades, amenazas y riesgos a los cuales se encuentran expuestos.

2. **Establecer acuerdos contractuales**

   Incluir cláusulas de seguridad y requisitos de cumplimiento en los acuerdos contractuales con proveedores, y establecer mecanismos de monitoreo y auditoría. En la medida de lo posible, requerir un seguro de riesgo cibernético que pueda cubrir a la organización por una afectación al proveedor.

Falta de conciencia y cultura de seguridad

1. **Programas de capacitación y concientización**

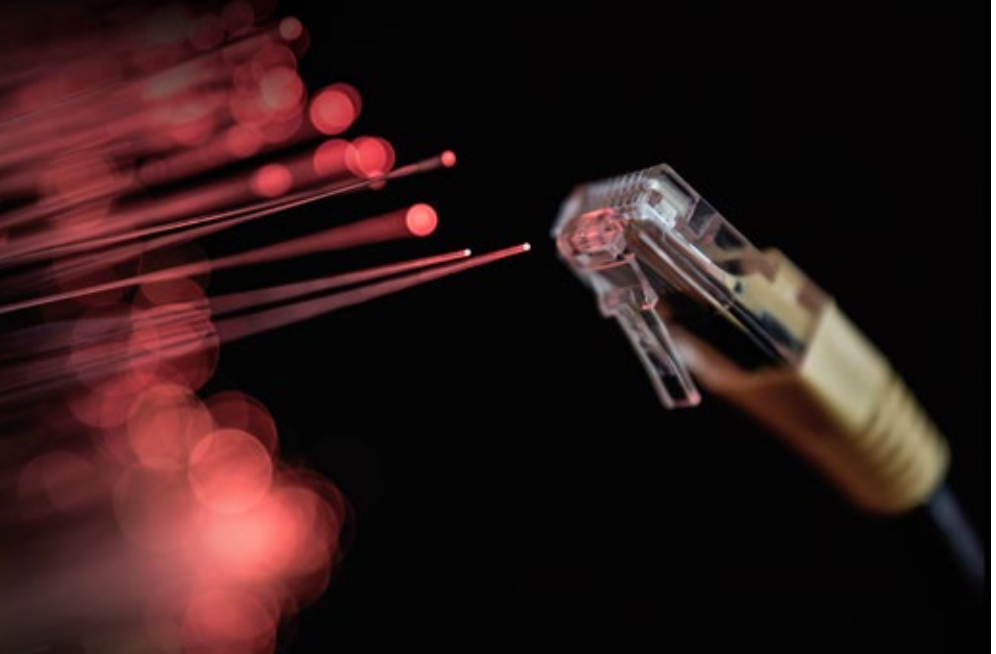
   Implementar programas de capacitación y concientización en seguridad para todos los empleados, enfatizando en las mejores prácticas de seguridad y en los riesgos asociados.

2. **Liderazgo y compromiso**

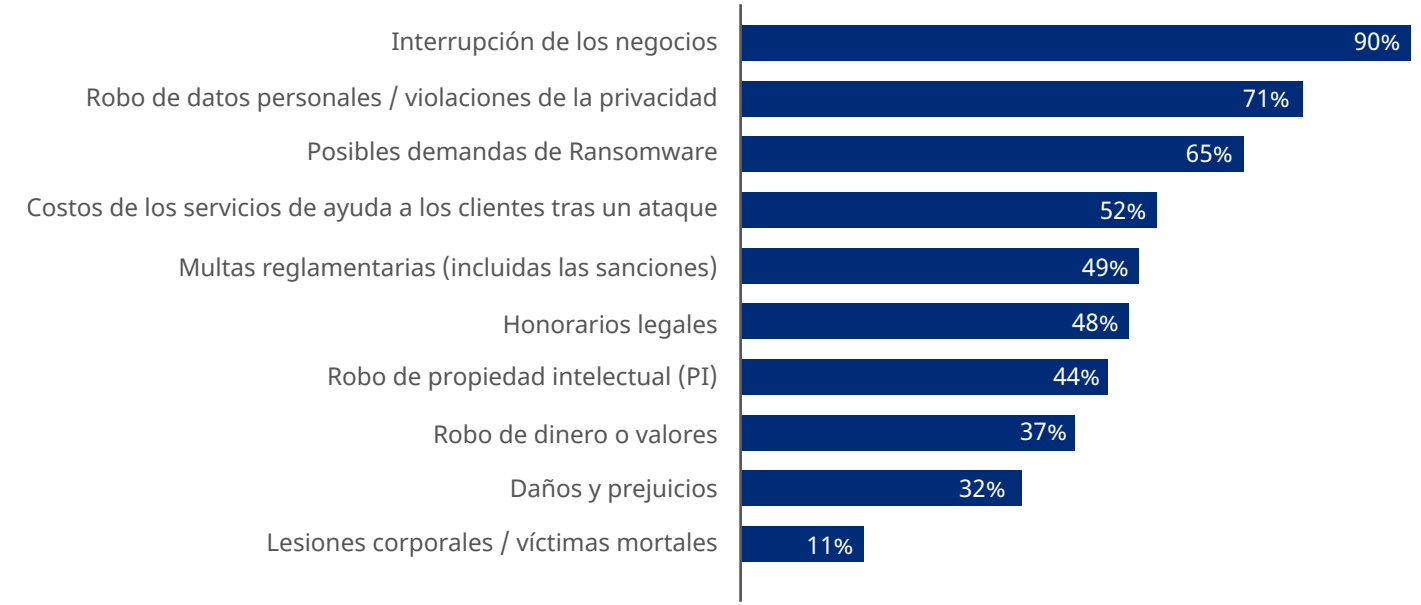
   Asegurar el liderazgo desde la alta dirección y promover una cultura de ciberseguridad en toda la organización.

Impacto de los ciberriesgos

La materialización del riesgo cibernético puede tener un impacto significativo en las organizaciones, el cual va más allá de pérdida de ingresos debido a la interrupción de las operaciones. El estudio realizado por Marsh y Microsoft sobre el Estado de la Resiliencia Cibernética en 2022 mostró que, a nivel global, solamente el 26% de las compañías encuestadas medían el riesgo cibernético en términos financieros. De ese estudio derivó también que los factores más utilizados en los cálculos financieros de estas empresas son: interrupción del negocio (90%), robo de datos personales/violaciones de la privacidad (71%) y posibles demandas de ransomware (65%).



Factores utilizados en los cálculos financieros*



* https://www.marsh.com/mx/services/cyber-risk/insights/the-state-of-cyber-resilience.html

Sin embargo, para estimar el impacto económico que puede tener la materialización de un riesgo de seguridad de la información y ciberseguridad, se recomienda que las organizaciones incluyan un espectro más amplio de áreas de impacto, lo que les permitirá tener un valor más realista del impacto económico de estos riesgos; de este modo podrán tomar decisiones más informadas para definir las estrategias de gestión del riesgo más adecuadas para la organización. Entre algunas de las principales áreas de impacto se encuentran las siguientes:

- **Interrupción del negocio / Lucro cesante**

  Reducción en la capacidad de una organización para generar la propuesta de valor principal, por ejemplo, ingresos, bienes, servicios, etc. Para el cálculo se debe considerar que la recuperación del nivel de ingreso de la organización en caso de un ciberataque puede ser gradual, hasta que finalmente vuelva a sus operaciones a la normalidad.

- **Costos de brechas de datos**

  Gastos asociados con la notificación del incidente a las personas afectadas. Estos costos pueden variar dependiendo del país y de la postura de la organización para la notificación en este tipo de situaciones.

- **Ciberextorsión**

  Valor que se pagaría al grupo cibercriminal detrás de un ataque que incluya el secuestro de los datos de la organización, en caso la empresa lo plantee como parte de un escenario catastrófico. En este punto se podrían incluir los honorarios de organizaciones que se encarguen de ayudar a la empresa afectada con la negociación con los cibercriminales y comisiones adicionales por la compra de criptomonedas.

- **Daño a la reputación**

  La divulgación pública de un ciberataque puede dañar la imagen de la organización y resultar en pérdida de clientes, disminución de las ventas y dificultades para atraer nuevos negocios.

- **Respuesta a ciberincidentes**

  La respuesta a un ciberincidente puede ser costosa, ya que puede incluir la contratación de servicios de análisis forense, número de horas de personas externas u horas extras de personas internas, licencias de herramientas necesarias para agilizar estas actividades, entre otros.

- **Costos de restauración**

  Inversión asociada al reemplazo o restauración de activos perdidos o dañados durante el ciberataque, lo cual podría incluir, por ejemplo, los honorarios de personal adicional para la reinstalación de estaciones de trabajo o servidores, adquisición/alquiler de equipos de reemplazo, etc.

- **Multas y sanciones**

  Las organizaciones suelen depender de terceros en su cadena de suministro, lo que agrega complejidad a la gestión del riesgo cibernético. Asegurarse de que sus terceras e incluso sus cuartas partes cumplan con los estándares de seguridad, y gestionar los riesgos asociados a la cadena de suministro, puede ser un desafío, particularmente en este sector.

- **Costos de litigio**

  Dependiendo del tipo de ciberincidente, la organización puede enfrentar demandas y acciones legales de parte de los afectados, en cuyo caso se recomienda considerar costos asociados a abogado, así como el posible valor a pagar a los afectados.

- **Fraude / Robo de dinero**

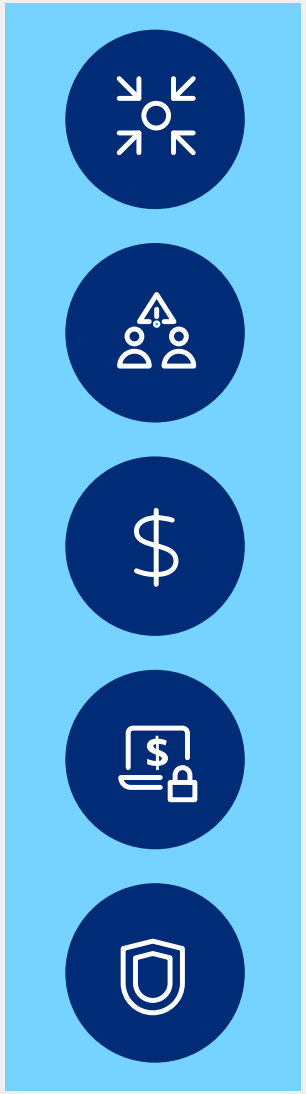
  Según el tipo de escenario que la organización plantee, es posible que se deban incluir aspectos relacionados con la afectación económica estimada en caso de su materialización. Esta podría generarse principalmente por transacciones no autorizadas, ya sea en casos de fraude en canales o directamente el robo de dinero a través de transferencias a través de SWIFT u otros sistemas de pago, así como a través de canales electrónicos como en el caso de ATMs.

- **Mejoras de seguridad**

  Inversión asociada a las mejoras de seguridad que se deben realizar para evitar que se materialice el evento de pérdida por las mismas causas que lo generaron.

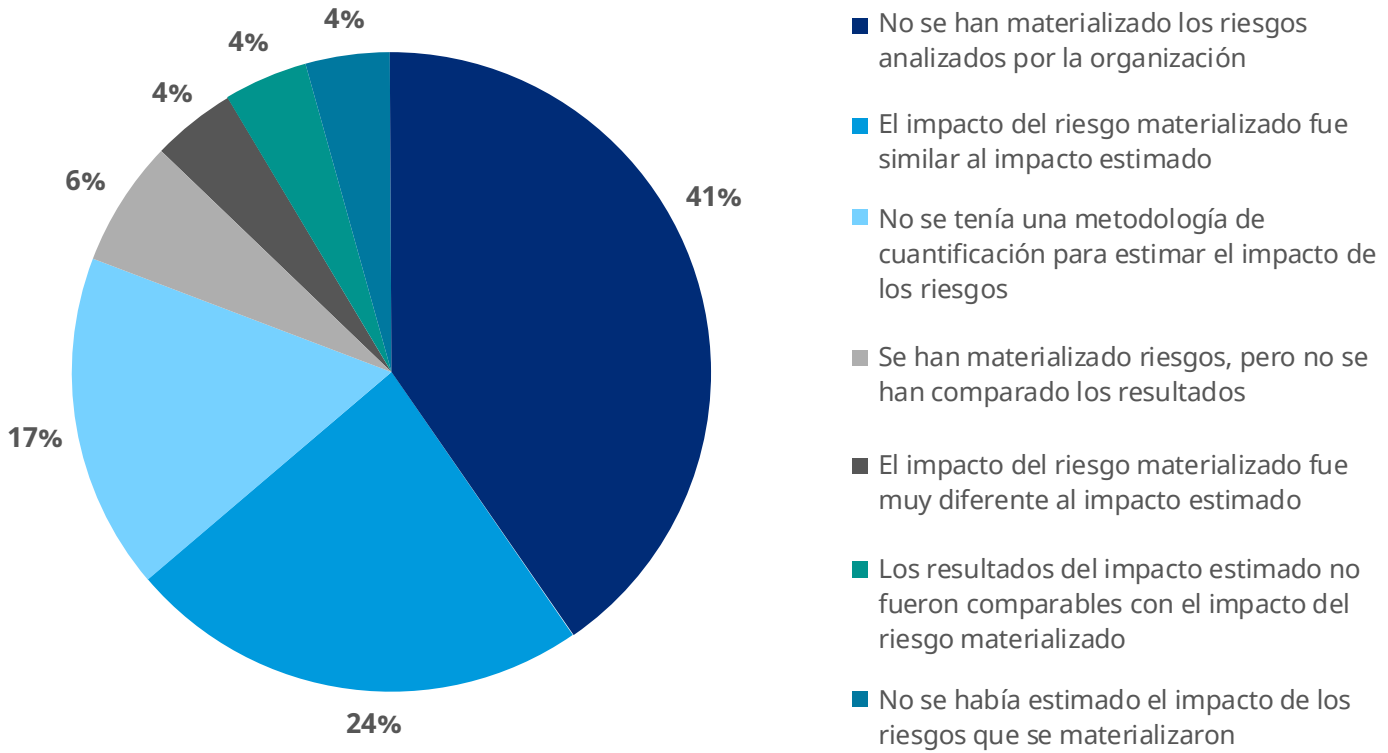
- **Otros gastos**

  La variedad de escenarios de ciberincidentes que pueden afectar a las organizaciones del sector financiero es muy amplia y podría ser necesario incluir algunos factores que no se encuentran considerados en las áreas de impacto mencionadas anteriormente, como bien podría ser el uso no autorizado de recursos de la organización que podría generar una afectación económica o la reducción de ingresos.



Según los factores que se analicen durante los análisis y evaluaciones de riesgos, las estimaciones realizadas por las organizaciones frente a las afectaciones económicas de los riesgos materializados pueden variar significativamente o ser bastantes cercanas. Al respecto, quisimos conocer qué han observado las organizaciones frente al análisis de cifras de un riesgo materializado frente a la estimación del mismo riesgo, para entender que variaciones o similitudes habían identificado. Los resultados fueron los siguientes:

Cuando se han materializado riesgos de seguridad de la información y ciberseguridad en las organizaciones, ¿cuáles fueron los resultados del análisis del impacto del riesgo materializado frente al impacto estimado?



- El **24%** de los encuestados indicaron que el impacto del riesgo materializado fue similar al impacto estimado.

- El **17%** indicó, que no tenían una metodología de cuantificación para estimar el impacto de los riesgos.

- El **41%** de los encuestados indicó que no se les han materializado los riesgos que la organización ha analizado. Sin embargo, cuando a estas organizaciones se les consultó sobre los riesgos que se les habían materializado, mencionaron los siguientes riesgos, los cuales, como hemos indicado durante el desarrollo de este estudio, son riesgos cuya sofisticación y frecuencia ha aumentado en los últimos años, y deberían incluirse en los análisis de riesgos de las entidades del sector financiero:

  1. **Fraude por medios electrónicos**
  2. **Ingeniería social**
  3. **Interrupción de las operaciones**
  4. **Ataque de malware / ransomware**
  5. **Ataque a través de terceros críticos**
  6. **Incumplimiento regulatorio**

- Porcentajes menores al **7%** indican lo siguiente:

  1. **El impacto del riesgo materializado fue muy diferente al impacto estimado**
  2. **Los resultados del impacto estimado no fueron comparables con el impacto del riesgo materializado**
  3. **No se había estimado el impacto de los riesgos que se materializaron**
  4. **Se han materializado riesgos, pero no se han comparado los resultados**

Si bien puede haber diversas razones por las cuales las situaciones anteriores se están presentando, es importante tener en cuenta lo siguiente:

- El análisis detallado de cada uno de los factores mencionados anteriormente es fundamental para llegar a cifras cercanas relacionadas con las afectaciones reales de los riesgos materializados. Adicionalmente, es importante hacer un análisis detallado de los costos por factor para entender dónde se encuentran las mayores diferencias, y entender si se deben hacer cambios o ajustes en la metodología de cuantificación de riesgos.

- Este tipo de modelos pueden requerir múltiples iteraciones para poder ajustarse cada vez mejor a la organización y la participación de equipos multidisciplinarios para reflejar múltiples puntos de vista.

- Es importante alinear las metodologías que se tienen para la cuantificación de los riesgos analizados y de los riesgos materializados, de forma que los resultados puedan ser comparables y permitan tomar acciones de mejora, de ser requerido.

- Una vez se han materializado los riesgos en las organizaciones, se debe asegurar que se cuenten con procesos establecidos y personal encargado de realizar la cuantificación de las pérdidas que ha tenido la organización por la materialización de los riesgos.

¿Cómo damos el siguiente paso?

Si bien el 71% de los encuestados que tienen metodologías cuantitativas no ha considerado cambiarla, a nivel de metodologías cualitativas y semicuantitativas, un porcentaje importante ha considerado cambiarlas debido a:

- Los resultados de estas metodologías no les permiten determinar el valor de la pérdida esperada para los riesgos evaluados.
- Consideran que las escalas utilizadas en estas metodologías de análisis de riesgos son subjetivas (por ejemplo, colores, escalas de 1 a 5 y símbolos).
- Los resultados de los análisis de riesgos son insuficientes para la toma de decisiones.

Adicionalmente, existen razones adicionales por las cuales las organizaciones están adoptando metodologías cuantitativas como son:

Mayor precisión en la evaluación de riesgos

Las metodologías cuantitativas permiten una evaluación más precisa de los riesgos al asignar valores numéricos a los distintos aspectos del riesgo, como probabilidad e impacto. Esto proporciona una visión más detallada y precisa de la magnitud y la probabilidad de los riesgos, lo que ayuda a la toma de decisiones informadas.

1

Apoyo a la toma de decisiones basada en datos

Al utilizar metodologías cuantitativas, las organizaciones pueden basar sus decisiones en datos y análisis objetivos en lugar de estimaciones subjetivas. Esto proporciona una base más sólida para identificar y priorizar los riesgos, así como para seleccionar las estrategias de mitigación más efectivas.

2

Comparación y priorización de riesgos

Las metodologías cuantitativas permiten comparar y priorizar los riesgos de manera más efectiva al utilizar métricas numéricas. Esto ayuda a las organizaciones a asignar recursos y tomar medidas proporcionales según la importancia y el impacto potencial de cada riesgo.

3

Comunicación más clara y efectiva

Las metodologías cuantitativas ofrecen una forma más clara y objetiva de comunicar los riesgos a las partes interesadas, como la alta dirección y los inversionistas. Los resultados numéricos y las métricas facilitan la comprensión y la comunicación del riesgo, lo que a su vez mejora la gestión del riesgo en toda la organización.

4

Integración con otros procesos de gestión

Las metodologías cuantitativas de riesgos se integran mejor con otros procesos de gestión como la planificación estratégica, la asignación de recursos y la gestión del desempeño. Esto permite una gestión más eficiente y coherente de los riesgos en toda la organización.

5

Cumplimiento regulatorio y exigencias del mercado

Algunas regulaciones y normativas requieren un enfoque más cuantitativo en la gestión del riesgo, especialmente en sectores altamente regulados como el financiero.

6

Adicional a lo anterior, y según lo indicado en el reporte "Cost of a Data Breach Report 2022"*, se estima que las organizaciones que utilizan técnicas de cuantificación de riesgos ahorran US$2.1M frente a aquellas que no.

* https://www.ibm.com/reports/data-breach

Cuantificación avanzada de ciberriesgos

Cuando las organizaciones han tomado la decisión de implementar metodologías de cuantificación de riesgos pueden enfrentar varios retos y desafíos como son:

Disponibilidad y calidad de los datos

La cuantificación de riesgos requiere datos relevantes cercanos a la realidad de la organización. Una de las dificultades es asegurar la disponibilidad y la calidad de los datos necesarios para realizar análisis cuantitativos. El 57% de los encuestados confirmaron que carecen de información histórica, ya sea porque los riesgos analizados no han ocurrido en la empresa o hay muy pocos datos de los incidentes que se analizan a nivel global; el 36% indicó que hay ausencia de datos para definir los rangos de cuantificación.

Capacidad y experiencia en análisis cuantitativo

La implementación de metodologías de cuantificación de riesgos puede requerir habilidades y conocimientos especializados en análisis cuantitativo, estadísticas y modelado. Las organizaciones pueden enfrentar desafíos para adquirir y desarrollar estas capacidades internamente. Adicional a esto, el 36% de los encuestados indicaron que presentan dificultades al momento de definir adecuadamente el escenario de evento de pérdida para hacer un análisis cuantitativo del mismo.

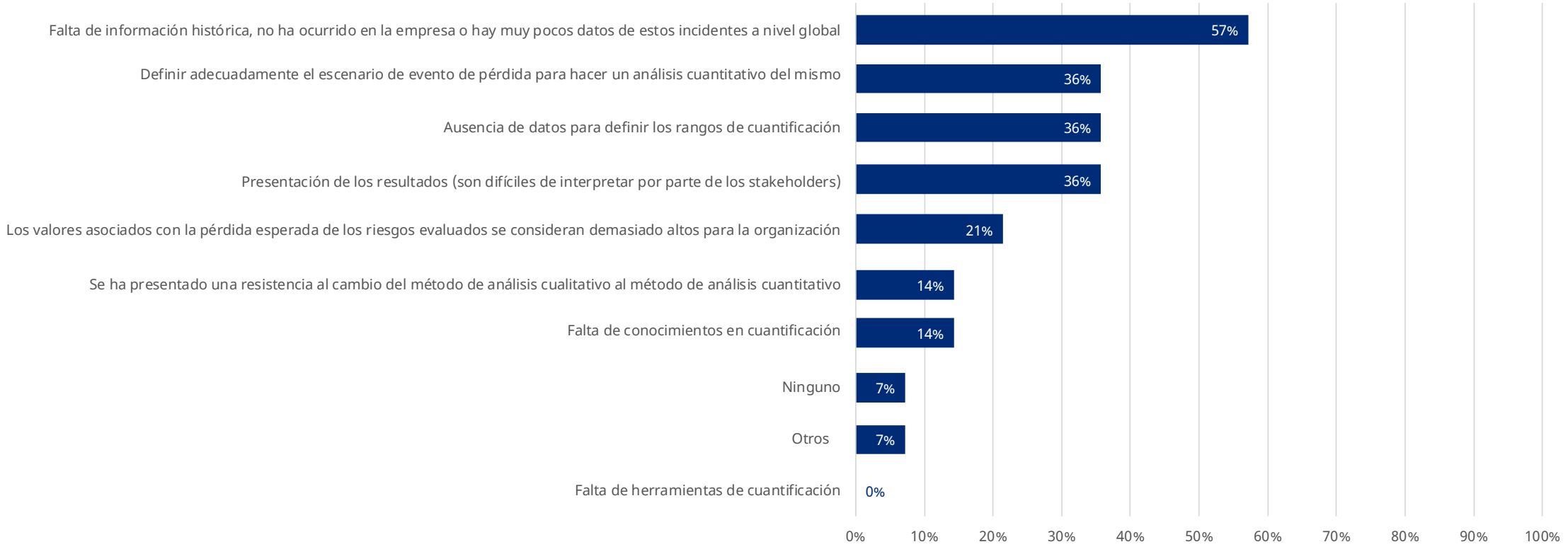
Interpretación y comunicación de resultados

La cuantificación de riesgos requiere datos relevantes cercanos a la realidad de la organización. Una de las dificultades es asegurar la disponibilidad y la calidad de los datos necesarios para realizar análisis cuantitativos. El 57% de los encuestados confirmaron que carecen de información histórica, ya sea porque los riesgos analizados no han ocurrido en la empresa o hay muy pocos datos de los incidentes que se analizan a nivel global; el 36% indicó que hay ausencia de datos para definir los rangos de cuantificación.

Costos y recursos

La adopción de metodologías de cuantificación de riesgos puede requerir inversiones en términos de recursos financieros, tecnológicos y humanos. Las organizaciones deben evaluar y asignar adecuadamente los recursos necesarios para implementar y mantener estas metodologías, lo que puede ser un desafío en términos de presupuesto y gestión de recursos.

Retos al usar un método cuantitativo de análisis de riesgos



Las organizaciones deben estar preparadas para superar estos retos y aprovechar los beneficios que ofrece la cuantificación de riesgos. A continuación mencionamos algunas recomendaciones que se pueden tomar en cuenta:

Disponibilidad y calidad de los datos

1. Identificar los datos necesarios para el análisis cuantitativo de riesgos.
2. Identificar las fuentes de datos internas con las que cuenta la organización, como son: reportes de incidentes, resultados de auditorías, resultados de escaneos de vulnerabilidades, registros de accesos a los sistemas, análisis de pérdidas financieras, reclamos de seguros, entre otros.
3. Identificar las fuentes de datos externas disponibles que incluyan información sobre los riesgos que se quieran evaluar. En estos casos, Marsh puede proveer información valiosa de estadísticas o benchmarks que pueden ser utilizados en los ejercicios de cuantificación.

Capacidad y experiencia en análisis cuantitativo

1. Evaluar las habilidades y conocimientos actuales dentro de la organización relacionadas con la cuantificación de riesgos, y determinar las brechas de competencias.
2. Proporcionar capacitación y desarrollo profesional a los empleados existentes.
3. Considerar la contratación de personal con experiencia en análisis cuantitativo o la asesoría con consultores externos.

Interpretación y comunicación de resultados:

1. Desarrollar informes y visualizaciones claras y comprensibles para presentar los resultados del análisis cuantitativo.
2. Asegurar que los resultados estén alineados con los objetivos y las necesidades de los responsables de la toma de decisiones.
3. Establecer canales de comunicación efectivos para transmitir los resultados de manera clara y oportuna.

Costos y recursos

1. Realizar un análisis de costo-beneficio para justificar la inversión en la implementación de metodologías cuantitativas.
2. Asignar presupuesto adecuado para recursos tecnológicos, herramientas de análisis y personal capacitado.

Beneficios de la cuantificación de riesgos

Para comprender la exposición que tienen las organizaciones frente al riesgo, es necesario identificar primero los riesgos a los cuales se enfrentan y luego cuantificar el impacto económico que tendría la materialización de dichos riesgos. Para esto, es importante definir procesos de gestión de riesgos que incluyan análisis cuantitativos y les brinde a las organizaciones resultados objetivos, significativos y relevantes para una adecuada toma de decisiones que los lleve a realizar una buena gestión del riesgo.

Las metodologías de análisis cualitativo y los mapas de calor que se generan como resultado de los análisis de riesgos, generalmente no permiten a las empresas responder preguntas de los stakeholders asociadas con el retorno de una inversión en ciberseguridad o cuánto dinero podrían perder frente a un escenario de riesgo específico.

Por el contrario, realizar un análisis cuantitativo de riesgos les traerá los siguientes beneficios a las organizaciones:

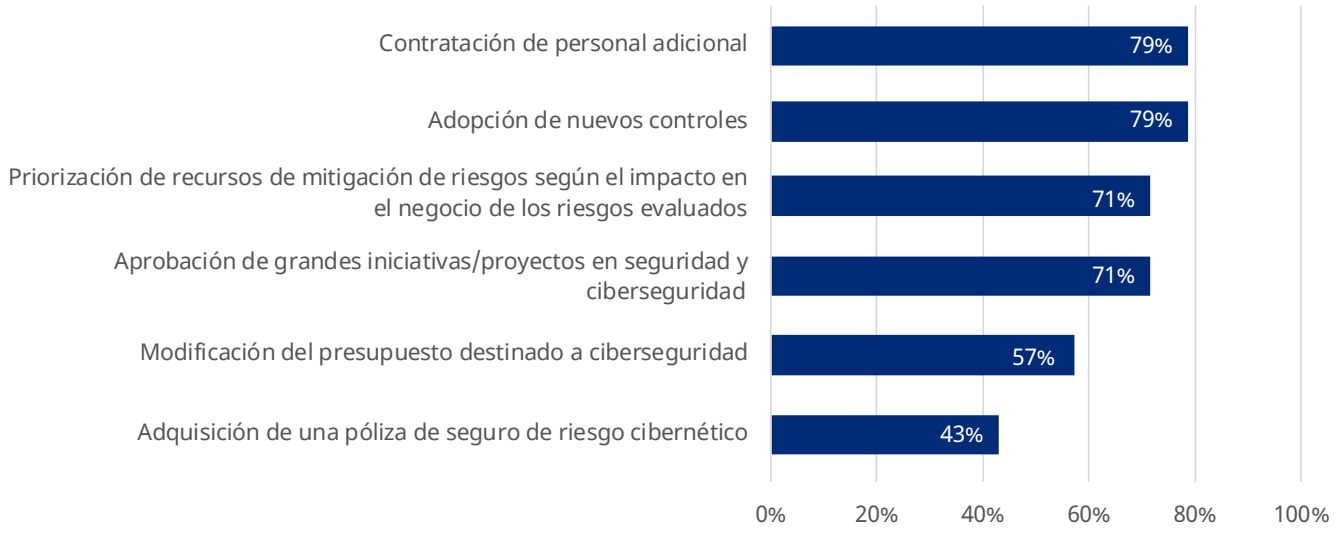
- Identificar los riesgos a los cuales se encuentra expuesta la organización y enfocarse en las cosas que más le interesan a la misma.
- Identificar cuál es el retorno a la inversión en seguridad de la información y ciberseguridad (ROSI), y ver en dónde se invierten dichos recursos, lo cual es de alta importancia teniendo en cuenta que son limitados en todas las organizaciones, así como cuáles son las inversiones que reducen en mayor manera el riesgo residual.
- Permite hablar a los stakeholders en un lenguaje que para ellos sea entendible y puedan estar en una posición para tomar mejores decisiones desde su perspectiva.

Para conocer cómo estos beneficios se han presentado en las organizaciones que actualmente cuentan con metodologías de cuantificación de riesgos, les preguntamos a los encuestados cómo habían utilizado los resultados arrojados. Con las respuestas identificamos que más del 70% de los encuestados han podido realizar las siguientes actividades:

- Adopción de nuevos controles
- Contratación de personal adicional
- Aprobación de grandes iniciativas/proyectos en seguridad y ciberseguridad
- Priorización de recursos de mitigación de riesgos según el impacto en el negocio de los riesgos

Adicionalmente, el 57% indicó que se ha modificado el presupuesto destinado a ciberseguridad, y el 43% ha realizado la adquisición de una póliza de seguro de riesgo cibernético con base en los resultados arrojados por la ejecución de la metodología.

Acciones que se han realizado con base en los resultados de los análisis cuantitativos de riesgos de seguridad de la información y ciberseguridad



La cuantificación de riesgos permitirá a las organizaciones conocer cuál es el valor que se obtiene de las inversiones realizadas en seguridad al momento de mitigar o transferir los riesgos. Esto será un insumo fundamental durante los procesos de toma de decisiones para la gestión efectiva de los mismos.

Mediante los análisis cuantitativos de riesgos se podrán identificar las situaciones bajo las cuales una inversión en seguridad permitirá reducir el riesgo o, por el contrario, identificar dónde los costos pueden ser reducidos mientras que no impacte el nivel del riesgo.

Para realizar esto, es necesario durante los análisis de riesgos identificar cómo la inversión propuesta impactaría a cada escenario de riesgo. y luego medir el estado actual del riesgo con los controles actuales. En este punto, y con el apoyo del personal experto dentro de la organización, se debe hacer un análisis cuantitativo del impacto financiero futuro de cada uno de los riesgos evaluados en su estado actual y con la inversión propuesta, de forma que se comparen los resultados y se identifique como la inversión impacta las pérdidas pronosticadas.

Es importante que, para estos procesos de análisis y cuantificación de riesgos, las compañías cuenten con las capacidades, recursos y conocimiento que les permita realizar ejercicios que les arrojen resultados valiosos para la organización. Para esto, es necesario definir e implementar metodologías cuantitativas de riesgos y capacitar continuamente al personal que hará parte de su ejecución, de forma que puedan expresar su conocimiento en términos cuantitativos y estimar de forma adecuada el impacto financiero de las pérdidas. También es importante complementar los análisis realizados con herramientas analíticas que permitan realizar estimaciones de las pérdidas financieras para poder contrastar contra los resultados arrojados por las metodologías definidas.

Comunicación a los stakeholders

Como mencionamos anteriormente, la cuantificación de riesgos permitirá, adicionalmente, tener una comunicación con los stakeholders en un lenguaje que para ellos sea entendible y puedan estar en una posición para tomar mejores decisiones desde su perspectiva. Para esto, es importante entender cuáles son los beneficios que esta comunicación traerá a cada uno de los líderes en las organizaciones.

- ## CEO (Chief Executive Officer):

1. **Visión general de los riesgos:**

   Brinda una visión general de los riesgos cibernéticos a los que se enfrenta la organización, incluyendo una comprensión clara de los impactos potenciales y las implicaciones para el negocio en términos financieros y reputacionales.

2. **Priorización de recursos e inversiones:**

   Ayuda a tomar decisiones informadas sobre las inversiones para la implementación de las estrategias de ciberseguridad y supervisar su progreso y cumplimiento de objetivos.

- ## CRO (Chief Risk Officer):

1. **Análisis de riesgos:**

   Ayuda a identificar y cuantificar los riesgos cibernéticos que pueden tener un impacto significativo en el logro de los objetivos de la empresa. Identifica aquellos que superan los niveles de tolerancia y asegura que se definan planes de tratamiento apropiados y oportunos.

2. **Monitoreo y seguimiento de riesgos:**

   Facilita el monitoreo continuo y el seguimiento de los riesgos cibernéticos a través de indicadores clave de desempeño (KPI) y métricas cuantitativas, permitiendo una gestión proactiva de los riesgos y la implementación de medidas correctivas.

• CISO (Chief Information Security Officer):

1. **Gestión estratégica:**

   Brinda un enfoque más estratégico a su gestión. Prepara casos de negocio sustentados en la posible pérdida ante la materialización de ciberriesgos.

2. **Priorización de medidas de seguridad:**

   Estructura estrategias de seguridad de la información y ciberseguridad basadas en riesgos, y en el impacto financiero de la organización.

3. **Análisis costo-beneficio:**

   Permite realizar análisis de costo-beneficio más precisos al evaluar las inversiones en tecnología y medidas de seguridad, identificando aquellas que brinden el mayor valor y retorno económico o mayor reducción de pérdidas potenciales.

• CIO (Chief Information Officer):

1. **Priorización de medidas de seguridad:**

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

• CFO (Chief Financial Officer):

1. **Retorno a la inversión:**

   Entender el retorno de la inversión en ciberseguridad y la posible afectación para la organización en caso de su materialización.

2. **Presupuesto en seguridad:**

   Evaluar el presupuesto de ciberseguridad en línea con el posible impacto económico de la falta de implementación de proyectos significativos.

3. **Seguro cibernético:**

   Definir los límites del seguro de riesgo cibernético a contratar adecuados para la organización, según su apetito de riesgo.

4. **Análisis de riesgo financiero:**

   Ayuda a evaluar el impacto financiero de los riesgos cibernéticos y determinar las implicaciones para el flujo de efectivo, el balance general y la planificación financiera de la organización.

¿Cómo utilizar un seguro como herramienta de transferencia del ciberriesgo?

Hay cuatro opciones de tratamiento del riesgo: la prevención, la mitigación, la transferencia y la aceptación. En el caso del riesgo cibernético, este resulta inevitable debido a diversos factores. Uno de ellos es la transformación digital que ocasiona que, por un lado, los ciberdelincuentes encuentren permanentemente nuevas formas de explotar vulnerabilidades y traspasar controles de ciberseguridad. Por otro lado, la digitalización provoca una creciente dependencia a las tecnologías emergentes como la inteligencia artificial, el internet de las cosas (IoT) o la nube, las cuales amplían aún más la superficie de ataque. Además, el factor humano es un elemento que amenaza constantemente la ciberseguridad, ya que los errores, negligencia o actos maliciosos de personas internas pueden comprometer en cualquier momento los sistemas o datos de una organización.

Es por ello que, para la adecuada gestión del riesgo cibernético, es indispensable un complemento entre mitigación, transferencia y aceptación del riesgo. La mitigación ayuda a reducir la probabilidad de un ciberataque con controles adecuados que contribuyan a identificar una amenaza, protegerse ante ella y responder adecuadamente. Sin embargo, como el riesgo cibernético es inevitable, la mitigación puede resultar insuficiente al momento de un ciberataque. Es entonces cuando la transferencia del riesgo la complementa al disminuir la severidad del impacto financiero y reputacional que puede padecer la compañía atacada. El seguro de riesgo cibernético es un mecanismo de transferencia del riesgo que ayuda a proteger a las organizaciones de las pérdidas y gastos de mitigación de crisis derivados de ataques cibernéticos y filtraciones de datos.

A causa del continuo aumento en la frecuencia y severidad de los siniestros de este seguro en los últimos años, las aseguradoras incrementaron la cantidad de información de ciberseguridad que solicitan a las empresas que buscan ser aseguradas, y también disminuyeron su flexibilidad para suscribir el riesgo. Es decir que, para poder conseguir un seguro de riesgo cibernético, el asegurado debe contar con un mínimo de controles de ciberseguridad debido a que las aseguradoras que ofrecen este producto le están dando una mayor importancia al desarrollo de capacidades internas de ciberresiliencia para que las compañías estén protegidas frente a ciberamenazas.

Los controles que las compañías de seguros solicitan como mínimo están directamente relacionados con las causas que estadísticamente han ocasionado más siniestros. De modo que, el seguro de riesgo cibernético apoya a impulsar la madurez de los controles más relevantes para la gestión del riesgo, y genera que contar con él demuestre una debida diligencia del mismo. Además, la póliza del seguro de riesgo cibernético puede ayudar a minimizar los efectos adversos que se producen como resultado de un ciberataque, reembolsar los costos financieros del manejo y la respuesta a la crisis, y ayudar a la organización a recuperarse rápidamente de la interrupción del negocio.

El mercado de seguros de riesgo cibernético cuenta con un diverso portafolio de opciones. La complejidad del riesgo ha derivado en una falta de uniformidad en los clausulados utilizados por cada mercado, lo cual hace desafiante el proceso de entendimiento de las coberturas y exclusiones del seguro, y hace necesario un análisis detallado para seleccionar la opción de seguro que se adapte adecuadamente a las necesidades de cada compañía.

A pesar de esta falta de estandarización, de manera general, se puede afirmar que a través de los seguros de riesgo cibernético se transfiere el impacto financiero que una compañía puede sufrir como consecuencia de un evento malicioso o accidental que comprometa la confidencialidad, disponibilidad y/o la integridad de su información, de sus sistemas de tecnología de la información (IT) y de sus sistemas de tecnología operacional (OT).

Las principales coberturas del seguro de riesgos cibernéticos normalmente se dividen en coberturas de responsabilidad civil y coberturas de pérdidas propias. Entre las coberturas de responsabilidad civil que indemnizan la mayoría de los productos en el mercado, están la de responsabilidad por privacidad o confidencialidad, responsabilidad por seguridad de la red y responsabilidad por publicación de contenido.

La cobertura de responsabilidad por privacidad o confidencial indemniza los perjuicios causados a terceros por la divulgación de información personal o de información confidencial por parte del asegurado en caso de que una organización no haya sido capaz de evitar el acceso, la divulgación o la recopilación no autorizados de información que les haya sido confiada.

La cobertura de responsabilidad por seguridad de la red indemniza los perjuicios causados a terceros por la infección de sus sistemas informáticos. Algunos productos se extienden a cubrir los perjuicios causados a terceros por la falta de disponibilidad de sistemas, por ejemplo, apps y páginas web, pero no es una cobertura estándar.

Finalmente, la cobertura de responsabilidad por publicación de contenido indemniza los perjuicios causados a terceros por la infracción de derechos de autor, difamación, calumnia, entre otros, incurridos por el asegurado en la publicación de contenido digital; algunos productos se extienden a cubrir publicaciones físicas también.

Por otro lado, dentro de las coberturas de pérdidas propias se encuentran las coberturas de pérdida de ingresos y las de gastos de mitigación de crisis. Entre las coberturas de pérdidas propias que indemnizan la mayoría de los productos en el mercado, están la de pérdida de beneficios por interrupción del negocio, recuperación de activos digitales, extorsión cibernética, protección a la reputación, gastos forenses, gastos de respuesta a fuga de datos, gastos de defensa y multas y sanciones.

La cobertura de pérdida de beneficios por interrupción del negocio cubre la indemnización del lucro cesante y los gastos adicionales incurridos por el asegurado como consecuencia de la interrupción de las operaciones por la afectación de la información o sistemas informáticos del asegurado. Esta cobertura puede incluso extenderse a indemnizar la interrupción del negocio contingente, que cubre el lucro cesante y gastos adicionales incurridos por el asegurado como consecuencia de la interrupción de sus operaciones por la afectación de los sistemas informáticos de proveedores de tecnología de la información (servicios de nube, hosting, datacenter, entre otros) o proveedores de procesos de negocios (servicios de pago de nómina, facturación, entre otros).

En cuanto a la cobertura de recuperación de activos digitales, esta indemniza los costos necesarios para recuperar o reconstruir los activos digitales afectados. Mientras que, la cobertura de extorsión cibernética indemniza el pago de la suma de dinero exigida como consecuencia de una amenaza a la información o sistemas informáticos del asegurado y otros costos relacionados, como la contratación de negociadores especialistas o el pago de recompensas.

La cobertura de protección a la reputación indemniza los costos de contratación de expertos en relaciones públicas que ayuden a mitigar o prevenir los efectos adversos a la reputación del asegurado por alguno de los eventos cubiertos. Incluso, en algunos productos se llega a extender la cobertura a indemnizar a el ingreso dejado de percibir como consecuencia de la afectación de la reputación del asegurado derivado de un evento cubierto por el seguro.

En el caso de la cobertura de gastos forenses, se indemnizan los costos para la contratación de firmas de informática forense que investiguen la fuente o causa del incidente cibernético. Asimismo, la cobertura de gastos de respuesta a fuga de datos indemniza los gastos para notificar a los titulares de los datos personales afectados por la divulgación y costos para monitoreo del crédito.

Finalmente, la cobertura de gastos de defensa indemniza los honorarios de abogados para la defensa ante reclamaciones presentadas por terceros al asegurado o para la defensa ante procesos administrativos por fallas en el tratamiento de datos personales. En cuanto a la cobertura de multas y sanciones, esta indemniza las multas impuestas por entidades administrativas como consecuencia de una divulgación de datos personales.

Las coberturas antes mencionadas hacen parte de las principales coberturas de un seguro de riesgo cibernético tradicional. Sin embargo, en el mercado existen otras coberturas diseñadas para industrias específicas, por lo cual es fundamental entender las necesidades de la organización de acuerdo al sector al que pertenece. En el caso de las Instituciones Financieras, una de las coberturas adicionales a tener en cuenta es la de incumplimiento de estándares PCI (Payment Card Industry) que indemniza las multas que esta entidad puede imponer por el incumplimiento de los estándares, los costos relacionados con la re-certificación, contratación de auditores, re-expedición de tarjetas, entre otros.

Este seguro también tiene algunas limitaciones que son estándar en la mayoría de los productos, tales como las siguientes exclusiones: todo evento conocido por el asegurado antes del inicio de vigencia, la implementación de mejoras o actualizaciones al sistema informático a un nivel superior al estado existente, lesiones corporales y daños materiales. Además, están excluidos comúnmente también los fallos o interrupciones eléctricas, mecánicas, de software, de telecomunicaciones, de satélite o internet, incluyendo, entre otros, sobretensión, corriente, caída de tensión o apagón, cortes de gas, agua, teléfono, cable, etc. Igualmente, excluye toda responsabilidad profesional por incumplimiento contractual o por errores u omisiones cometidas por el asegurado.

Otra limitación del seguro de riesgo cibernético que es especialmente importante para las Instituciones Financieras, es que excluye la pérdida, robo o transferencia fraudulenta de dinero o títulos valores desde las cuentas del asegurado a las de un tercero. Las transacciones fraudulentas, inclusive las que son consecuencia de un fraude cibernético de ingeniería social, están excluidas de la póliza de seguro de riesgo cibernético debido a que la cobertura anexa a la BBB de Crimen por Computador, en algunas ocasiones ya las indemniza.

Es común que se confundan la cobertura de Crimen por Computador con la póliza de seguro de riesgo cibernético. Sin embargo, en el caso de la cobertura de Crimen por Computador, esta requiere dolo por parte de un tercero, debe resultar en una pérdida de dinero o títulos valores, debe haber una manipulación del sistema computacional del asegurado y, a diferencia del seguro de riesgo cibernético, no cubre errores, ni gastos de respuesta, o la responsabilidad civil por pérdida de información.

En resumen, el seguro de riesgo cibernético es un mecanismo de transferencia del riesgo que cubre la pérdida de ingresos, los gastos de mitigación de crisis y la responsabilidad civil por un acto malicioso o accidental que afecte su información y/o sus sistemas de IT y OT. Las organizaciones que cuentan con él denotan una adecuada gestión del riesgo porque acompañan la transferencia del mismo con capacidades de respuesta ante incidentes cibernéticos. Además, lo recomendable es que las Instituciones Financieras complementen la póliza BBB con la de riesgo cibernético para estar protegidos y evitar áreas grises en sus coberturas ante un ciberataque.

¿Conoces las capacidades de cuantificación de ciberriesgos de Marsh?

Desde la práctica de consultoría en Riesgo Cibernético de Marsh Advisory, contamos con un portafolio de integral de servicios que incluyen la cuantificación de ciberriesgos, que permite ayudar a nuestros clientes a que conozcan la exposición financiera que tienen frente al riesgo cibernético, y definir estrategias adecuadas de gestión. A continuación, detallamos nuestros principales servicios relacionados con la cuantificación de ciberriesgos:

Definición de la metodología de cuantificación de riesgos de seguridad de la información y ciberseguridad

1

Con base en el conocimiento y experiencia que nuestros consultores tienen sobre gestión de riesgos y modelos propietarios de Marsh, este servicio consiste en definir una metodología cuantitativa de gestión de riesgos de seguridad de la información y ciberseguridad, o ajustar la metodología actual del cliente, de forma que le permita realizar evaluaciones cuantitativas. Como parte de este servicio, apoyamos adicionalmente a nuestros clientes a identificar los activos de información de los procesos de negocio y sobre estos hacer una identificación, valoración y evaluación de riesgos, con el fin de definir estrategias de mitigación de los riesgos acorde con el apetito al riesgo de la organización.

Cyber Exposure Quantification (Cyber XQ)

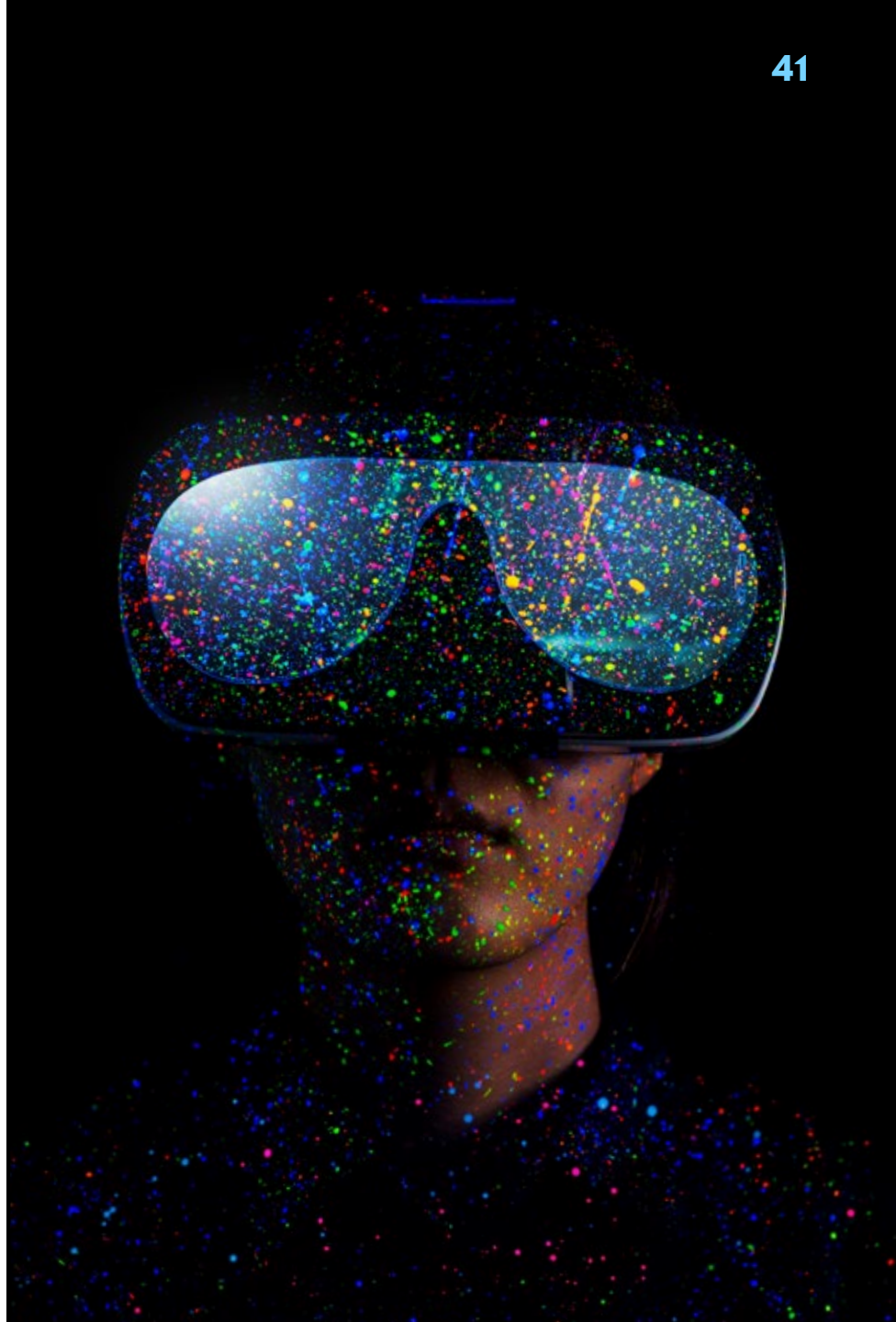
2

Modelo propietario de Marsh mediante el cual se realizan evaluaciones detalladas de las posibles pérdidas económicas que una organización puede sufrir ante la materialización de diferentes escenarios de riesgo de ciberseguridad. Para lograr esto se realiza un análisis de diferentes factores asociados a áreas de impacto como pérdidas de ingresos, costos de brechas de datos, costos de recuperación, multas y sanciones, fraude, entre otros. Si la organización cuenta con un modelo matemático base para la cuantificación de los impactos generados por escenarios de riesgo, los resultados de este ejercicio pueden servir de insumo.

Marsh Blue[i] Cyber

3

Herramienta de analítica propietaria de Marsh mediante la cual se realiza una estimación de las pérdidas económicas que puede sufrir una organización frente a la materialización de 3 escenarios de riesgo de ciberseguridad clave, utilizando datos de incidentes reales. Esta herramienta también permite evaluar la reducción del riesgo cuando las organizaciones mejoran sus controles de ciberseguridad. Si la organización cuenta con un modelo matemático base para la cuantificación de los impactos generados por escenarios de riesgo, los resultados de este ejercicio pueden servir de



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

Realizar una identificación y clasificación de los activos de información más críticos de la organización, de forma que se conozca la criticidad que tienen para la empresa. Posteriormente, realizar una evaluación de los controles implementados sobre estos activos, con el fin de identificar las vulnerabilidades, amenazas y riesgos a los cuales se cuáles se encuentran expuestos.

Implementar metodologías de análisis cuantitativo de riesgos

Considerar la implementación de metodologías cuantitativas para la gestión del riesgo cibernético, que les permita a las organizaciones una comprensión más precisa y basada en datos de la exposición al riesgo, lo que facilitará la toma de decisiones informadas y la asignación de recursos adecuados.

Establecer estrategias de gestión del riesgo

De acuerdo con el apetito al riesgo de la organización, y con base en los resultados de los análisis cuantitativos de riesgos, definir estrategias adecuadas de gestión del riesgo, en donde se prioricen y planifiquen las iniciativas, proyectos y controles a implementar, comenzando por aquellas que mitiguen los riesgos más críticos o de alto impacto.

Gestión del riesgo en la cadena de suministro

Realizar una debida diligencia exhaustiva al evaluar y seleccionar proveedores de la cadena de suministro, incluyendo evaluaciones de seguridad y controles de cumplimiento. Así mismo, incluir cláusulas de seguridad y requisitos de cumplimiento en los acuerdos contractuales con proveedores y terceros, y establecer mecanismos de monitoreo y auditoría.

Recopilación y análisis de datos para la cuantificación de riesgos

Asegurarse de contar con datos relevantes y actualizados sobre las amenazas, vulnerabilidades e impactos potenciales a los que puede estar expuesta la organización, a través de la consulta en fuentes de información tanto internas como externas y que involucren la opinión de expertos tanto de las diferentes áreas de la organización como de consultores externos.

Comunicación estratégica del riesgo cibernético

Teniendo en cuenta que el resultado de la cuantificación de riesgos permitirá tener una comunicación con los stakeholders en un lenguaje que para ellos es entendible, asegurar una comunicación continua y estratégica, de forma que cada uno de ellos, tome las mejores decisiones en gestión de riesgo, desde su perspectiva. Esta comunicación incluye la presentación de informes periódicos sobre el estado de los riesgos cibernéticos, los avances en la gestión de riesgos y los resultados obtenidos mediante la metodología cuantitativa.

Análisis del impacto de los riesgos

Una vez se han materializado los riesgos en las organizaciones, se debe asegurar que se cuente con procesos establecidos y personal encargado de realizar la cuantificación de las pérdidas que ha tenido la organización por la materialización de los riesgos. Adicionalmente, es importante alinear las metodologías que se tienen para la cuantificación de riesgos y para cuantificar las pérdidas generadas por los riesgos materializados, de forma que los resultados puedan ser comparables y permitan tomar acciones de mejora, de ser requerido.

Definición de los escenarios de riesgos

Es importante entrenar al personal involucrado en la gestión de riesgos y dedicar tiempo suficiente para definir adecuadamente los escenarios de riesgos, con el fin de obtener mejores resultados durante el análisis y cuantificación de estos. Esto permitirá disminuir las suposiciones que se hagan alrededor de cada escenario de riesgo analizado y obtener resultados más precisos.

Factores de cuantificación de riesgos

Para estimar el impacto económico que puede tener la materialización de un riesgo de seguridad de la información y ciberseguridad, las organizaciones deberían analizar y tener en cuenta por lo menos los siguientes factores que les permitirán tener un valor aproximado del impacto económico de estos riesgos:

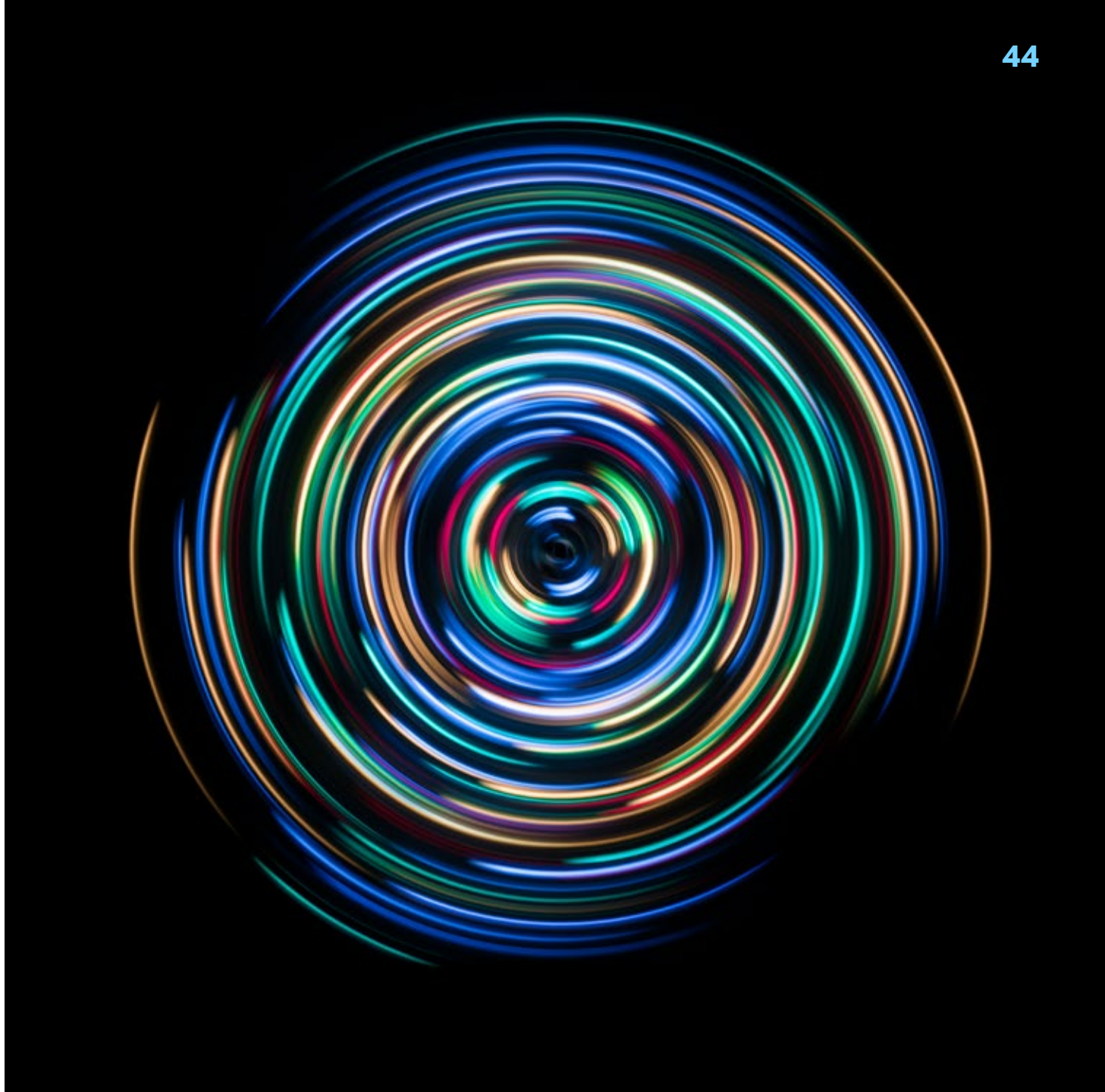
- Interrupción del negocio / Lucro cesante
- Costos de brechas de datos
- Ciberextorsión
- Daño a la reputación
- Respuesta a ciberincidentes
- Costos de restauración
- Multas y sanciones
- Costos de litigios
- Fraude o robo de dinero
- Mejoras de seguridad

Mantenerse actualizado

Estar al tanto de las últimas tendencias y tácticas de ciberataques a través de fuentes de inteligencia de amenazas, boletines de seguridad y colaboración con entidades de la misma industria. Adicionalmente, implementar soluciones de seguridad actualizadas y utilizar herramientas de detección y prevención de amenazas actualizadas, como firewalls, sistemas de detección de intrusiones y soluciones de seguridad endpoint.

Capacitación y entrenamiento

Proporcionar capacitación y entrenamiento continuo a los empleados sobre gestión de riesgos de ciberseguridad, metodologías de cuantificación de riesgos, nuevas tecnologías, panorama de riesgos, entre otros aspectos claves para que ayuden a la organización a identificar y gestionar los riesgos adecuadamente.



Conclusiones

1. Los riesgos cibernéticos en el sector financiero han aumentado en los últimos años, siendo los más destacados los ataques de ingeniería social, los ataques de ransomware, fraude por medios electrónicos, y ataques a través de proveedores y terceros.

2. Las organizaciones enfrentan retos durante los procesos de gestión del riesgo cibernético, como la falta de datos confiables para determinar el impacto y la probabilidad de ocurrencia de un riesgo que enfrente la organización, la complejidad de las amenazas y la falta de conocimiento, conciencia y cultura de seguridad y gestión de riesgos en toda la organización.

3. La adopción de metodologías cuantitativas de riesgos ofrece múltiples beneficios a las organizaciones, como tener un lenguaje común con los líderes de la empresa, una evaluación más precisa de las medidas de seguridad, asignación de recursos adecuados, evaluación de costos y beneficios, toma de decisiones estratégicas informadas, y evaluación de riesgos en el contexto general de riesgos de la empresa.

4. Las organizaciones enfrentan dificultades para cuantificar las pérdidas de un riesgo cibernético materializado debido a la falta de datos históricos, la complejidad de los impactos indirectos y la falta de análisis de los factores involucrados en la materialización de los riesgos.

5. Es importante consultar opiniones de expertos y fuentes de datos externas e internas para la recopilación y análisis de datos, invertir en capacitación y desarrollo de habilidades, establecer una comunicación efectiva entre los equipos de gestión de riesgos, fomentar una cultura organizacional centrada en la gestión de riesgos, y realizar evaluaciones periódicas de la metodología de gestión de riesgos.

6. Según los factores que se analicen durante los análisis y evaluaciones de riesgos, las estimaciones realizadas por las organizaciones frente a las afectaciones económicas de los riesgos materializados pueden variar significativamente o ser bastantes cercanas.

7. Se presentan retos en las organizaciones en el momento de la definición de los escenarios de riesgos, por lo cual, no se identifican claramente las consecuencias de la materialización de estos. Es importante capacitar al personal encargado de la gestión de riesgos y, a su vez, a los empleados, para que puedan dar su opinión del impacto y la probabilidad de ocurrencia del riesgo en los términos requeridos.

¿Cómo puede ayudar Marsh?

La práctica de consultoría en Riesgo Cibernético de Marsh Advisory, cuenta con un amplio portafolio de servicios con los que buscamos dar un enfoque estratégico a la gestión del riesgo cibernético en nuestros clientes. Al unir las capacidades de una amplia red de profesionales a nivel global y la potencia de Marsh, hemos logrado diseñar servicios únicos en el mercado que permitirán ayudar a nuestros clientes a enfrentar sus riesgos cibernéticos de punta a punta. A continuación, se pueden observar algunos de nuestros principales servicios:

Principales Servicios de Consultoría en Riesgo Cibernético.

Herramientas especializadas

Estrategia y gobierno

- Diagnóstico de seguridad y ciberseguridad
- Desarrollo de la estrategia de ciberseguridad
- Diagnóstico de ciberseguridad ICS / SCADA
- Diagnóstico de ciberseguridad Cloud
- Diagnóstico de prevención del fraude digital
- Definición de políticas y procedimientos de seguridad de la información y ciberseguridad
- Definición del dashboard ejecutivo de ciberseguridad
- Tercerización de la Oficina de Seguridad
- Diagnóstico frente a Ransomware

Cumplimiento

- Auditoria de Controles Generales de TI
- Evaluación de cumplimiento regulatorio
- Implementación de requerimientos regulatorios
- Diagnóstico de PCI DSS
- Desarrollo del diagrama de flujo de datos de la tarjeta habiente (PCI DSS)
- Diagnóstico de Protección de Datos Personales
- Implementación del programa de privacidad

Cyber Risk Analytics

Cultura de ciberseguridad

- Cyber Chemistry – Evaluacion de cultura de ciberseguridad
- Desarrollo del programa de concientización en ciberseguridad
- Capacitaciones especializadas en ciberseguridad
- Evaluación de las capacidades del equipo de Seguridad de la Información y Ciberseguridad*

Herramientas especializadas

Cyber Risk Analytics

Gestión y cuantificación de riesgos

- Identificación y clasificación de activos de información
- Definición de la metodología cualitativa y cuantitativa de gestión de riesgos de seguridad de la información y ciberseguridad
- Evaluación de riesgos de seguridad de la información y ciberseguridad
- Cuantificacion de la exposición al riesgos cibernético (CyberXQ, Cyber RFO, Marsh Blue(i) Cyber)

Gestion de riesgos con terceros

- Definición del marco de gestión de ciber-riesgos con terceros (TPRM – Cyber)
- Evaluación de riesgos de seguridad de la información y ciberseguridad con terceros
- Due-diligence de ciberseguridad para fusiones y adquisiciones (M&A)

Seguro de riesgo cibernético

- Autoevaluación de madurez de ciberseguridad para el seguro de riesgo cibernético*
- Cyber IDEAL – Estimación de perdidas para el seguro (brecha de privacidad, ransomware y lucro cesante de un ciberataque) *
- Cybersegurity Rating (BitSight y SegurityScorecard) *
- Evaluación de riesgos para el seguro cyber
- Contratación del seguro de riesgo cibernético*
- Cyber Claims & Crisis Orchestration (soporte en el reclamo de siniestros cyber)Información y Ciberseguridad*

Desarrollo seguro de software

- Desarrollo de la metodología de desarrollo seguro de software
- Capacitación de desarrollo seguro
- Revisión de seguridad en código fuente
- Web & Mobile Application Hacking

Seguridad defensiva y ofensiva

- Ciberinteligencia (búsqueda de información fugada en internet)
- Gestión de vulnerabilidades
- Revisión de la configuración de ciberseguridad (hardening)
- Pruebas controladas de intrusión (ethical hacking)
- Web & Mobile Application Hacking
- Pruebas de ingeniería social
- Pruebas de red team

Gestión de Incidentes

- Respuesta ante ciberincidentes
- Desarrollo del plan de respuesta ante ciberincidentes y playbooks
- Desarrollo del protocolo organizacional frente a casos de ransomware
- Ejercicios de escritorio de ciber-crisis y del plan de respuesta ante ciberincidentes
- Desarrollo del plan de mejoras post-incidente

Contactos

Para conocer cómo podemos apoyar a su organización en la gestión del riesgo cibernético, póngase en contacto con nuestros profesionales:

- **Gerardo Herrera Perdomo**
  Director General de Consultoría en Riesgos para Latinoamérica
  Marsh Advisory
  gerardo.herrera@marsh.com

- **Edson Villar Da Silva**
  Líder de Consultoría en Riesgo Cibernético para Latinoamérica
  Marsh Advisory
  edson.villar@marsh.com

- **Angela Cubillos Martín**
  Líder de Consultoría en Riesgo Cibernético para Colombia
  Marsh Advisory
  angela.cubillos@marsh.com

- **Hugo Preciado García**
  Senior de Riesgo Cibernético
  Marsh Advisory
  hugo.preciado@marsh.com

- **Paula Ordóñez Vasco**
  Líder de Productos Financieros (FINPRO) para Latinoamérica
  Marsh
  paula.ordonez@marsh.com

- **Paulina Vélez Gómez**
  Líder del Seguro de Riesgo Cibernético para Latinoamérica
  Marsh
  paulina.velez@marsh.com

- **Susana Muñoz Acosta**
  Analista Senior del Seguro de Riesgo Cibernético para Latinoamérica
  Marsh
  susana.munoz@marsh.com

A business of Marsh McLennan