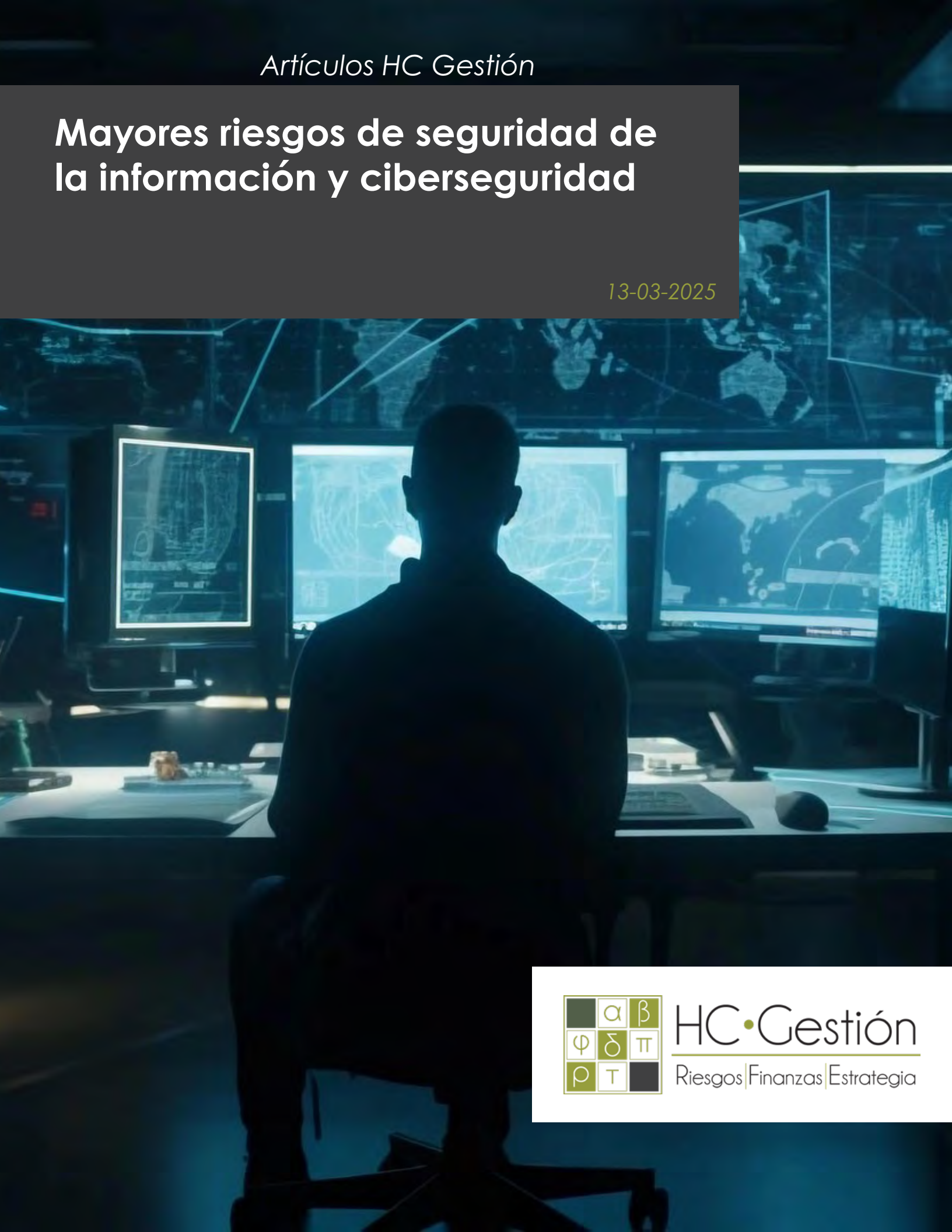
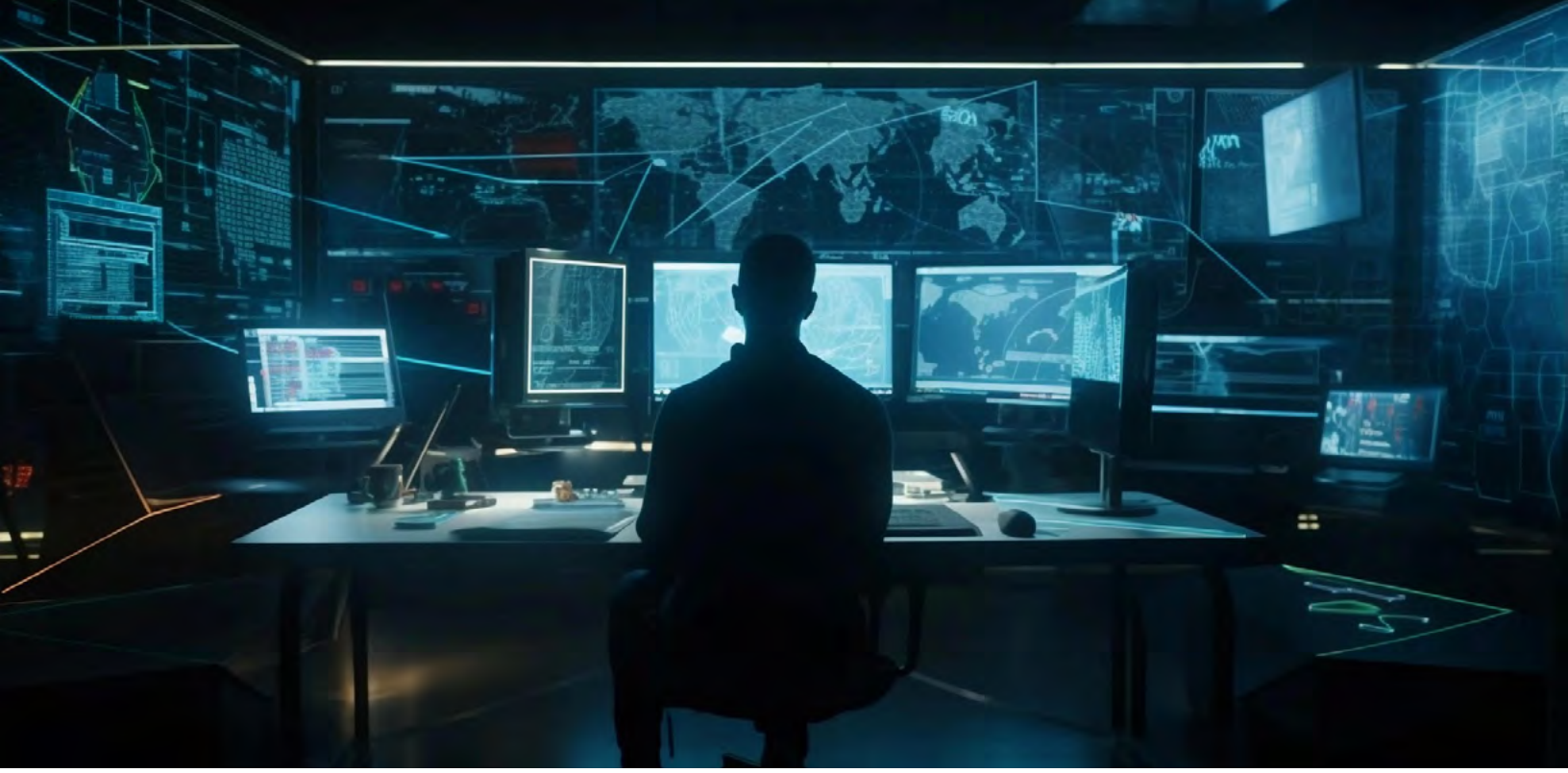
Artículos HC Gestión

Mayores riesgos de seguridad de la información y ciberseguridad

13-03-2025



HC·Gestión
Riesgos | Finanzas | Estrategia



Mayores riesgos de seguridad de la información y ciberseguridad

Por Esperanza Hernández Avendaño.

Entre los principales riesgos previstos por HC Gestión para este año de 2025, se encuentran los riesgos de seguridad de la información y de ciberseguridad. En este artículo me refiero a estos dos tipos de riesgos, puesto que ambos presentan características diferentes.

El riesgo de seguridad de la información se materializa en pérdidas ocasionadas por la afectación de la confidencialidad, integridad y disponibilidad de la información relevante para una empresa, bien sea que esta se encuentre de manera digital, física o en forma de ideas y conocimientos, como bien lo señala Hillstone Networks en su artículo "5 diferencias entre ciberseguridad y seguridad de la información". De esta mane-

ra se puede afirmar que el riesgo de seguridad de la información se presenta no solamente en la información digital sino en toda la información de la empresa, independientemente del formato y del estado en que esta se encuentre.

Por su parte, el riesgo de ciberseguridad hace referencia a las posibles pérdidas derivadas de la violación a los activos de información como computadoras, servidores, dispositivos móviles, redes y datos que actúan como sistemas interconectados. Esto significa que en este caso la información debe encontrarse en algún sistema interconectado.

Para mayor claridad y de forma resumida a continuación señalo las 5 diferencias mencionadas por Hillstone Networks en su artículo, así: (i) La seguridad de la información es un concepto mucho más amplio que el de ciberseguridad; (ii) La ciberseguridad solo se aplica a sistemas interconectados; (iii) La seguridad de la información solo tiene que ver con medidas defensivas; (iv) La seguridad de la información puede ser aplicada por un departamento específico de la organización, sin tener que involucrar necesariamente al resto de esta. La ciberseguridad requiere de la colaboración activa de todo el personal; (v) Para la gestión del riesgo de seguridad de la información es útil la norma ISO27001 y otros estándares relacionados. En la gestión del riesgo de ciberseguridad los métodos y herramientas son dinámicos y acordes con la innovación tecnológica.

Una vez aclaradas las características de ambos tipos de riesgos y teniendo en cuenta la fuerte interrelación que existe entre ellos, procedo a describir las razones por los cuales en HC Gestión afirmamos que la probabilidad de ocurrencia y el impacto de ambos riesgos serán mayores en este año de 2025.

En la medida en que la gestión de riesgos es cada vez más una función estratégica generadora de valor para las empresas, el análisis y gestión de datos de tamaño significativo y el uso de tecnologías emergentes como la Inteligencia Artificial (IA) son requeridos en forma creciente por lo tanto, la gestión de los riesgos de seguridad de la información y de ciberseguridad se convierten en funciones fundamentales con el fin de evitar o mitigar de una parte, las posibles amenazas a la confidencialidad, integridad y disponibilidad de la información y de otra, los ciberataques.

La necesidad de gestionar el riesgo de seguridad de la información se acrecienta de acuerdo con el desarrollo y evolución de la estructura de datos, con el objetivo de predecir y responder a eventos disruptivos que puedan afectar la información relevante de la empresa. En esta medida, se requiere una mayor proactividad de parte del gestor de riesgos en los siguientes aspectos: (i) La identificación de los factores o causas de los posibles eventos de riesgo; (ii) La medición y valoración de su impacto en los resultados y la continuidad del negocio; (iii) los tipos de controles a implementar, incluyendo

la valoración de su efectividad; (iv) Los mecanismos de monitoreo y seguimiento a utilizar, requeridos especialmente debido a la dinámica propia de la innovación en tecnología de la información.

En el mismo sentido, teniendo presente la fuerte correlación entre ambos riesgos, las amenazas cibernéticas cada vez serán mayores y más sofisticadas, debido a la evolución de la inteligencia artificial (IA) generativa y a la digitalización cada vez más frecuente de los procesos de la cadena de valor de las empresas, independientemente del tipo de sector económico al que pertenezcan. En la medida en que la IA generativa ha ido en aumento, cada vez es mayor la creatividad e innovación utilizada en los ciberataques. Entre los tipos más conocidos me permito citar los siguientes:

- Deepfakes: Imágenes, videos y audios generados o editados utilizando herramientas de IA que pueden mostrar personas reales o inexistentes.

Lo novedoso de este tipo de ciberataque es la inclusión de algoritmos de reconocimiento facial como Autocodificadores Variacionales (VAE) que consisten en una red neuronal artificial que se entrena para comprimir y luego reconstruir datos de entrada como imágenes o texto y Redes Generativas Adversativas (GANs) que consisten en dos redes neuronales

que pueden generar fotografías que parecen auténticas para los observadores humanos.

- Phishing: Suplantación de identidad que consiste en el envío de correos electrónicos fraudulentos en nombre de otros para poder acceder a los datos en una red personal o empresarial.

La innovación en este tipo de ataque ha sido mayor en los últimos años identificándose diferentes técnicas de phishing como: (i) Vishing que utiliza la voz, es decir consiste en phishing realizado por teléfono; (ii) Smishing ataques mediante mensajes de texto SMS; (iii) Envenenamiento SEO o ataques de phishing que dirigen a los usuarios a sitios web maliciosos manipulando el resultado de las búsquedas habituales; (iv) Clone phishing o phishing de clonación que consiste en enviar a un usuario un correo electrónico de phishing que imita un correo electrónico que éste ha recibido previamente; (v) Business Email Compromise (BEC) que se realiza a través de la suplantación de la identidad del CEO o de otro ejecutivo de alto nivel de la empresa.

Seguramente cada vez aparecerán otros tipos de phishing que se constituirán en nuevos retos para el gestor del riesgo de ciberseguridad.

- Amenazas internas: Por parte de personas que trabajan para la empresa y se pueden manifestar en robo de datos,

uso indebido de estos, sabotaje, espionaje y fraude. Es muy común en este tipo de amenazas el uso de "bombas lógicas" o códigos maliciosos ocultos dentro de un script que se activan cuando se cumple una condición particular, como una fecha, hora o inicio específico de una aplicación.

- Malware: Código malicioso preinstalado en dispositivos como teléfonos, unidades de bus serial universal (USB), cámaras y otros dispositivos móviles que se activa cuando se conecta con el sistema o la red. Los códigos maliciosos igualmente se pueden incluir en el firmware el cual ayuda a la interacción entre usuarios y sistemas en el hardware digital, obteniéndose así acceso a un sistema o a una red.

- Ingeniería social: Manipulación para obtener datos personales o información financiera, con el propósito de llevar a cabo robo de identidad o plantar ransomware en los sistemas y acceder a redes digitales, dispositivos y cuentas.

La probabilidad de la frecuencia de los eventos de riesgos de seguridad de la información y de ciberseguridad irá en aumento acompañada además de mayor sofisticación e impacto, lo cual definitivamente seguirá siendo un desafío para los gestores de estos riesgos. La mayor capacidad de su identificación y oportuna gestión dependerá entonces del grado de preparación que sobre el tema hayan desarrollado

las empresas, así como de la evolución de la regulación a nivel local, regional y global.

En 2024 y de acuerdo con la publicación de Welivesecurity ESET de diciembre 12 de ese año, los "7 incidentes de ciberseguridad que marcaron el 2024 en América Latina", fueron:

1. Banco Do Brasil: Robo de datos personales y financieros de más de 2 millones de clientes, que fueron usados para cometer delitos financieros por un total de 40 millones de reales, contando con la participación de personal del Banco mediante la inserción de scripts maliciosos en los sistemas.
2. Interbank, Perú: Filtración de datos personales de más de 3 millones de usuarios con el objetivo de extorsionarlos, llevada a cabo por un tercero sin autorización del Banco.
3. Coppel, México: Ciberataque que afectó a 1.800 tiendas en todo el país causado, de acuerdo por algunos medios de comunicación, por ransomware Lockbit 3.0.
4. Air-e, Colombia: Ataque de ransomware afectando la distribución y comercialización de energía eléctrica en varias regiones o departamentos del país.
5. Consejería Jurídica del Poder Ejecutivo Federal, México: Ataque de ransomhub con el secuestro de más de 300GB

de información, entre contratos, presupuestos e información de sus funcionarios.

6. Registro Nacional de las Personas, Argentina: Robo de más de 100 mil fotografías de ciudadanos para la emisión de documentos de identidad y pasaportes en 2021, pero con consecuencias aún en 2024 manifestadas en casos de phishing, ingeniería social y suplantación de identidad.
7. Bimbo, México: Ataque de ransomware Medusa, conocido por su capacidad de cifrar datos de los usuarios y añadir la extensión "MEDUSA" a los archivos comprometidos.

Todos estos casos validan la importancia de llevar a cabo una mayor gestión de los riesgos de seguridad de la información y de ciberseguridad en América Latina para mitigar el impacto no solamente económico, sino también, de pérdida de confianza por parte de los clientes y usuarios.

Los resultados de la encuesta Global Digital Trust Insights de 2024 realizada por la firma de auditoría Price Waterhouse Cooper (PwC) a 3.876 ejecutivos comerciales y tecnológicos de las empresas globales más grandes (el 30% de los encuestados presentaban ingresos de 10 mil millones de dólares o más), evidenció un margen considerable de mejora en materia de ciberseguridad, señalando además, tres riesgos prioritarios para 2025: (i) Riesgos digitales y tecnológicos (51%); debido a

la innovación tecnológica y a la incapacidad para ejecutar iniciativas de transformación digital; (ii) Riesgos cibernéticos (43%) como piratería, ransomware y aquellos asociados al control y vigilancia de los sistemas; (iii) Volatilidad macroeconómica (41%), ante los choques de demanda y oferta en la economía con impacto negativo, crisis de deuda y estallido de burbujas de activos.

De los resultados de la encuesta me parece importante resaltar además lo siguiente:

- La principal amenaza identificada fue la seguridad de la información en la nube, que a la vez ha sido la que más inversión ha recibido de parte de los encuestados, pero que, de acuerdo con ellos mismos, ha sido mal gestionada.

- El costo medio de las infracciones de ciberseguridad en millones de dólares y el porcentaje de las infracciones más perjudiciales que cuestan 1 millón de dólares o más, es liderado por el sector salud, seguido de los sectores de tecnología, medios y telecomunicaciones, servicios financieros, energía, industrial y en último lugar retail.

- Casi siete de cada diez encuestados afirmaron que su organización utilizará inteligencia artificial generativa (GenAI) para la ciberdefensa de sus sistemas.

- El 44% de los encuestados informaron utilizar un conjunto integrado de soluciones de tecnología cibernética, mientras el 39% manifestó planes para cambiarse a una de estas soluciones en los próximos dos años. El 19% manifestó tener demasiadas soluciones cibernéticas y necesitar su consolidación. Al respecto me parece importante destacar que la integración tecnológica es fundamental en la gestión del riesgo cibernético para lograr una visión global y actuar con mayor oportunidad y efectividad.

- De acuerdo con la mayoría de los encuestados, las nuevas normas y regulaciones sobre ciberseguridad obstaculizan los ingresos, pero al menos un tercio de ellos opina que las barreras que imponen los reguladores pueden dar a las empresas una mayor confianza para explorar, experimentar, inventar y competir, de forma tal que el cumplir con los requisitos regulatorios puede convertirse en una ventaja competitiva para las empresas líderes en el tema.

De lo observado en la práctica, considero importante señalar que, para determinar el mayor o menor grado de desarrollo de la gestión de estos riesgos, se debe tener en cuenta el sector económico en el cual la empresa lleva a cabo sus operaciones, así como el marco regulatorio expedido por las entidades encargadas en cada región y para cada actividad económica.

Según la encuesta realizada por PwC, el sector financiero se encuentra en cuarto lugar entre los sectores con costo medio y porcentaje de infracciones más perjudiciales por eventos de ciberseguridad. Es de resaltar que en razón a la importancia de este sector en el manejo de los ahorros del público y el sistema de pagos de la economía, la regulación y supervisión de la gestión de estos riesgos ha evolucionado desde hace ya varios años. De hecho, en 2018 uno de los resultados de la investigación llevada a cabo por la Organización de Estados Americanos (OEA) denominada "Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe", señalaba que: "(…) Respecto al apoyo a la gestión del riesgo de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) por parte de la alta dirección de la entidad bancaria, se destaca que más del 60% del total de las entidades bancarias en la región lo demuestran i) exigiendo la adopción de buenas prácticas de seguridad (65%), ii) fomentando la capacitación y sensibilización en seguridad digital (63%) y iii) impulsando planes de seguridad digital (60%).".

A partir de 2020 la preferencia de los usuarios por canales digitales para realizar operaciones financieras ha ido en aumento, al mismo tiempo que la IA evolucionó incrementado la vulnerabilidad de la información y de los sistemas ante riesgos más complejos, entre los que se encuentran aquellos derivados de la computación cuántica, la cual hace

vulnerable a las instituciones, en la medida que este tipo de computadores pueden traducir fácilmente los algoritmos de cifrado que utiliza la banca actualmente y por lo tanto pone en riesgo la confidencialidad de la información de los clientes, las comunicaciones entre pares, los procesos de autenticación y la confianza en las firmas digitales. Por otro lado, la velocidad de procesamiento es enorme. De hecho, una computadora cuántica utilizada por Google en 2019 llevó a cabo un cálculo en 200 segundos que hubiera requerido, según esta empresa, 10.000 años a una supercomputadora digital.

La innovación tecnológica definitivamente exige medidas de mitigación igualmente novedosas que ya se empiezan a desarrollar en el sector bancario, tales como el uso de la misma IA generativa para la defensa de los ciberataques. Es así como En el sector y los supervisores, entre estos últimos la Superintendencia Financiera de Colombia (SFC), son conscientes de la necesidad de preparar el camino para enfrentar los riesgos provenientes de la computación cuántica en el mediano y largo plazo. Al respecto es importante mencionar el artículo "Las posibilidades y los riesgos de la información cuántica" de la revista Finanzas y Desarrollo que se soporta en el documento de trabajo 21/71 del FMI "Quantum Computing and the Financial System Spooky Action at a Distance?", en el que se señala como desde 2021 "En Estados Unidos, el Instituto Nacional de Normas y Tecnología está llevando a cabo un

concurso para desarrollar algoritmos de encriptación que puedan hacer frente a las computadoras cuánticas".

Toda esta innovación exige cada vez más la necesidad de implementar el concepto de "confianza cero" o "zero trust", el cual, como lo señaló la SFC en el 17° Congreso de Seguridad, Amenazas Cibernéticas, Fraude y Experiencia, celebrado en octubre de 2024, consiste en "(…) un conjunto de principios y estrategias que buscan reducir al mínimo la incertidumbre, al implementar decisiones de acceso estrictas basadas en solicitudes con privilegios mínimos.". Sin embargo, es importante tener en cuenta que resolver los retos de la implementación de este concepto tomará tiempo de manera que los avances de su adopción se podrán medir mediante el desarrollo de un modelo de madurez que implica la aplicación de principios de gobernanza, automatización, visibilidad y analítica en los pilares de identidad, dispositivos, redes, aplicaciones y cargas de trabajo y muy importante en los datos.

Los desafíos en la gestión de estos riesgos son grandes, pero no se puede desconocer el desarrollo logrado en aspectos como: uso de la IA defensiva, configuraciones predeterminadas más inteligentes, disrupción de redes de ciberdelincuentes, mayor seguridad en las identidades digitales, autenticación resistente al phishing, mayores inversiones estatales y esfuerzos para reducir los ciberataques, al mismo tiempo que como lo señala National Cibersecurity Alliance de Estados Unidos en su

artículo "Predicciones de ciberseguridad para 2025: desafíos y oportunidades": "(…) se abordan las amenazas inmediatas y se construye resiliencia a largo plazo."

Para quienes la gestión de riesgos es una pasión, estos desafíos y los avances logrados son motivación para seguir identificando los factores o causas de estos riesgos y continuar desarrollando e implementando mejoras a su gestión, al mismo tiempo que se procede a su integración con los demás riesgos a los que se encuentra expuesta la empresa para conocer el impacto global en la rentabilidad.

Los riesgos de seguridad de la información y de ciberseguridad seguirán incrementándose al ritmo de la evolución de la innovación tecnológica y por lo tanto es importante aprender a gestionarlos para seguir estando vigente en el mercado.

***Para mayor detalle y apoyo en la gestión de estos dos riesgos y los demás riesgos financieros, no financieros y emergentes puede acceder a nuestra página web* https://hcgestion.com *y contactarnos a nuestro correo* redeshcgestion@gmail.com.**

Fuentes:

1. Hillstone Networks en su artículo "5 diferencias entre ciberseguridad y seguridad de la información".
2. Foqum, Plataforma IA, Glosario.
3. Wikipedia, Red generativa adversativa.
4. Microsoft, ¿Qué es un ciberatque?.
5. Check Point, Tipos de técnicas de phishing.
6. IBM, ¿Qué es la ingeniería social?
7. Data Security Plus, 10 mejores prácticas para neutralizar las amenazas internas.
8. Fortinet, ¿Qué es un ataque a la cadena de suministro?
9. Welivesecurity, Christian Ali Bravo, Cibercrimen.
10. PWC, The C-suite playbook: Putting security at the epicenter of innovation, Findings from the 2024 Global Digital Trust Insights.
11. OEA, Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe.
12. Superintendencia Financiera de Colombia (SFC), Retos importantes en seguridad y disponibilidad en el sector financiero.
13. Finanzas y Desarrollo, Las posibilidades y los riesgos de la información cuántica.
14. National Cibersecurity Alliance, Predicciones de ciberseguridad para 2025: desafíos y oportunidades.

Esperanza Hernández Avendaño.

Socia fundadora y Representante Legal de HC Gestión

Consultora con conocimiento técnico, amplia experiencia y resultados concretos en gestión y supervisión de riesgos, estrategia corporativa y función financiera, en los secortes privado y público.

Más de 30 años como docente universitaria en programas de pregrado y posgrado.

HC·Gestión

Riesgos | Finanzas | Estrategia