No. 151 Abril - Junio 2019 DOI: 10.29236/sistemas ISSN 0120-5919

SISTEMAS

Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2018-186-4-72, vence 31 de Dic. 2019

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS
Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

moodlemoot COLOMBIA

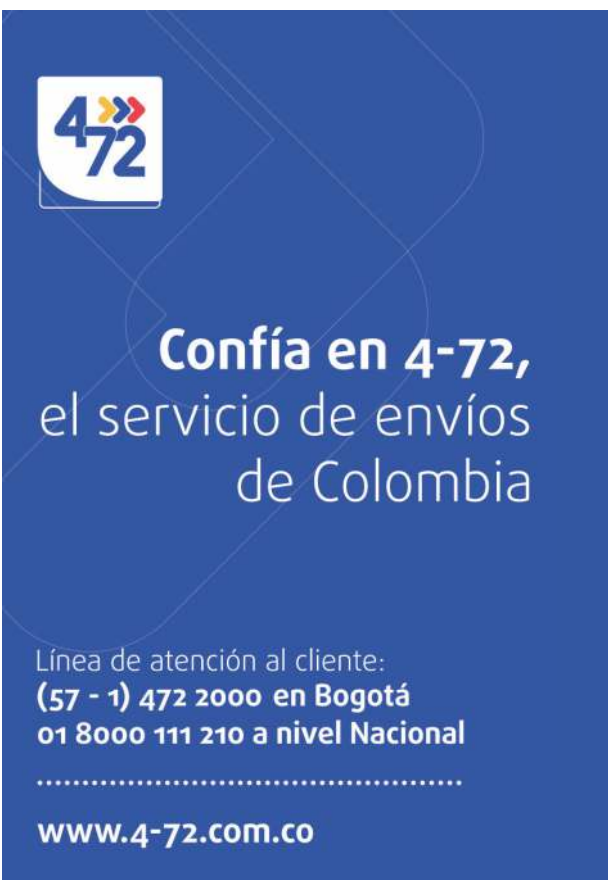
29 - 30 de Agosto de 2019
Bogotá - Colombia

#MootCO19

En esta edición

Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS)
Resolución No. 003983 del Ministerio de Gobierno
Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2015-186 4-72
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Abril - Junio 2019
Calle 93 No.13-32 Of. 102
Teléfonos 616 1407 – 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co



ACIS

ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

La Asociación Colombiana de Ingenieros de Sistemas (ACIS), presente en las redes sociales para servir al sector informático del país y del exterior.

/acis

@acis_co

/aciscolombia

/aciscol

/ACIScolombia

www.acis.org.co

Calle 93 No. 13-32 Oficina 102
Teléfonos: 6161407 / 09 - 3015530540
www.acis.org.co

El ciberriesgo, tensión para los saberes previos

DOI: 10.29236/sistemas.n151a1

Un actor emergente que surge más allá del ambiente de negocios e involucra al ser humano en su dimensión completa.

Jeimy J. Cano M.

La acelerada transformación de las empresas y de la sociedad, acompañada del incremento de la densidad digital de los objetos físicos, establece un nuevo paradigma de comprensión social y económico, que debilita la visión mecanicista del mundo y privilegia una más relacional, en la que ya no son los elementos del sistema los que tienen el protagonismo, sino sus interacciones y conexiones conocidas (y emergentes).

En este contexto, la comprensión actual de los riesgos, asociada con

aquellos conocidos y controlables, le da paso a una nueva lectura que revela, en un escenario hiperconectado, situaciones que pueden ser latentes o desconocidas para las organizaciones y cuyo tratamiento no responde a estándares vigentes a la fecha.

En este sentido, el concepto de ciberriesgo como una realidad sistémica (relacional, dinámica y evolutiva) genera una nueva frontera de reflexiones para los profesionales de seguridad y control, así como, para los ejecutivos de una organización, que los invita a realizar una categorización de los riesgos distinta a la tradicional. Para lograrlo, ahora ellos deben partir de "en relación con" y no "de acuerdo con", retando los estándares vigentes como ISO 31000 e ISO 27005 –para citar algunos−, diseñados para entender entornos conocidos.

Es por esto que la revista "Sistemas", de la Asociación Colombiana de Ingenieros de Sistemas −ACIS−, ha decidido revisar en contexto la comprensión, la gestión y el aseguramiento de los ciberriesgos en las organizaciones actuales. Con ese objetivo, fueron convocados profesionales de distintas disciplinas, quienes desde su área de experiencia proponen reflexiones para seguirle la pista al ejercicio sistémico, en el marco de la convergencia tecnológica, las inestabilidades y las posibilidades de un mundo cada vez más digital y tecnológicamente modificado.

El ingeniero Juan Mario Posada Daza, columnista invitado, establece desde su práctica de consultoría un marco base para reflexionar sobre el ciberriesgo, como el reto de la interdependencia de las empresas en el ciberespacio, que hace de la cooperación un fundamento clave para frenar las situaciones de ataque y responder a los hechos que podrían desestabilizar empresas y naciones. En esa dirección presenta una revisión de documentos de la práctica internacional, en los que fundamenta sus posturas sistémicas y el reconocimiento del ciberriesgo como un elemento estratégico y de negocio en las organizaciones modernas.

Por su parte, el ingeniero Andrés Almanza Junco presenta el análisis de los resultados de la décimo novena encuesta nacional de seguridad de la información, realizada cada año por ACIS, estudio que revela las tendencias más representativas de las empresas colombianas en los temas de protección de la información y la evolución del líder digital de seguridad, así como sus respectivos contrastes con la realidad internacional. Contempla una serie de reflexiones encaminadas al análisis alrededor de la evolución de la seguridad de la información, además del estado actual de la práctica de seguridad y control en el país.

El tradicional foro de la revista contó con la participación de destacados profesionales involucrados con

los retos propios de los ciberriesgos, quienes intercambiaron conceptos y cuestionaron las fronteras actuales de su tratamiento, además de analizar la comprensión de la convergencia tecnológica y sus implicaciones en los negocios. Ellos advierten sobre la necesidad de reinventar la práctica de la gestión de riesgos y amenazas dentro de las organizaciones frente a un escenario cada vez más disruptivo, inestable e hiperconectado, ambiente que demanda una mayor anticipación que prevención.

Así mismo, nuestros lectores dispondrán de dos artículos para reflexionar sobre la conceptualización y gestión del ciberriesgo. Un primer documento de autoría de este servidor se ocupa de los fundamentos del ciberriesgo, con el propósito de ilustrar tres características clave que lo definen como sistémico, emergente y disruptivo. Dicho ejercicio apunta hacia una mirada sistémica y las implicaciones que su materialización puede tener en un escenario hiperconectado. El segundo artículo, escrito por el ingeniero Joshsua González Díaz, aborda el ciberriesgo desde una perspectiva técnica con las implicaciones económicas y sociales. El autor detalla algunos análisis de este riesgo en el sector financiero y plantea varios elementos de cara al concepto de ciberresiliencia.

De manera que, este número de la revista "Sistemas" ofrece un panorama renovado de análisis y consideraciones sobre un nuevo tipo de riesgo, que tensiona los saberes y prácticas existentes. Su contenido invita a todos los profesionales en las diferentes áreas, a mirar de forma convergente las nuevas realidades que revela un mundo digital y tecnológicamente modificado, sin perjuicio de los nuevos desafíos técnicos y administrativos, donde los terceros de confianza, hacen realidad capacidades inexistentes en las organizaciones actuales.

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Profesor Distinguido de la Facultad de Derecho. Universidad de los Andes. Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Es director de la Revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*

¡ESCRÍBANOS!

REVISTA SISTEMAS

Asociación Colombiana de Ingenieros de Sistemas (ACIS)

Diríjase a la editora de la revista:

Sara Gallardo M.

saragallardo@acis.org.co

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

Calle 93 No. 13-32 Of. 102
Bogotá, D.C.
www.acis.org.co

El entorno corre y los ciberriesgos vuelan

DOI: 10.29236/sistemas.n151a2

Los diferentes sectores de la industria afrontan cambios profundos en el entorno de negocios en el marco de un contexto digital que avanza de forma acelerada, a diferencia de los lentos procesos de regulación, adaptación y gestión de los ciberriesgos que en el mediano plazo podrían causar grandes catástrofes.

Juan Mario Posada Daza

Seguimos buscando la manera más efectiva de afrontar los desafíos que trae consigo la Revolución Industrial 4.0 que, en el marco del contexto digital, potencializa el uso de la computación para abordar algunas actividades rutinarias y mecánicas, tradicionalmente ejecutadas por personas e integra el uso de la inteligencia artificial para plantear la solución de problemáticas que eran resueltas también por los trabajadores de las empresas.

Otrora los riesgos asociados al contexto digital se consideraban un problema de pocos, pero en la actualidad es una problemática social, que afecta los diferentes sectores de la industria, que habilita la participación ciudadana en nuevos modelos de negocio, pero que también requiere nuestro mayor cuidado y conciencia.

En medio de esta realidad es fundamental tener presente que en el entorno revolucionario de la Industria 4.0, el objetivo de potencializar la estrategia empresarial y el logro de la visión, no será posible si de la mano de los cambios en curso no

se adoptan estrategias para afrontar los desafíos éticos, sociales y estratégicos planteados, que habilitan la exposición a un ecosistema de riesgos cibernéticos en permanente cambio.

Para enmarcar esta reflexión basta con revisar algunas publicaciones que resaltan los desafíos del entorno de negocios de hoy. Entre ellas, Boston Consulting Group señala 12 fuerzas que cambian la forma de trabajar (Boston Consulting Group, 2017) agrupadas en:

- La productividad digital
- La generación de valor
- La distribución de recursos
- Los cambios de cultura y valores

Dichas fuerzas se observan directamente relacionadas con los cambios que se han originado en la Industria 4.0, especialmente el crecimiento de los dispositivos móviles, la automatización de tareas, la generación exponencial de datos, cuyo análisis aislado podría apresurar la toma de decisiones de la gestión de riesgos estratégicos de las empresas. Esto, teniendo en cuenta que podrían ser considerados como habilitadores para la ampliación de capacidades de cobertura geográfica, ampliación de segmentos de mercado y otros beneficios que solían ser restringidos por las limitaciones de tiempo, recursos y espacio planteados por los modelos tradicionales de hacer negocios.

No ajenos a lo descrito, el Foro Económico Mundial establece que el futuro está girando y está cada vez más orientado hacia una economía digital y una sociedad digital (World Economic Forum, 2019). Esto implica un cambio en el estilo de vida de las personas, generado en buena medida porque las tecnologías, día tras día, cobran más importancia. Las empresas al entender esto, han desarrollado nuevas formas de operación (apoyándose en la tecnología).

En este sentido y por su naturaleza, la tecnología avanza más rápido que nunca (Ley de Moore), por lo que la industria (y la regulación) deben ser rediseñadas para responder efectivamente al rápido ritmo del cambio digital y sus consecuencias.

Por todo lo anterior, estar al tanto de las nuevas tecnologías y formas de operación en diferentes empresas, ya no es sólo una cuestión de innovación, se ha convertido en un tema de supervivencia.

Por su parte, Gartner en su top 10 de las principales tecnologías estratégicas para 2019, muestra que tienen el potencial de impulsar una disrupción significativa y brindar oportunidades en los próximos cinco años (Gartner, 2018). Dentro de las tendencias, resalta la importancia de la ética digital y la privacidad, comprendiendo que, como resultado de la conectividad y el involucramiento de la tecnología en la transmisión y generación de información, la información personal es de

vital importancia para todo tipo de organizaciones.

En tal contexto, el efecto gira alrededor de la necesidad de abordar estos cambios, sin perder de vista el monitoreo constante de los riesgos relacionados con su protección. Además de actualizar las herramientas de seguridad de la información, que con el tiempo deberán contemplar también la toma de medidas asociadas al fortalecimiento de competencias que permitan a las personas mantener un rol relevante dentro de la ejecución de su trabajo, aprovechando de manera eficaz las tecnologías emergentes, potencializando las capacidades de análisis, argumentación y asociación de datos aislados.

Comprender estas diferencias facilitará a las empresas orientar el impacto de la Industria 4.0 en el entorno de ciberriesgos, para que su resultado sea favorecedor a todas las partes interesadas, mediante la articulación de medidas de evaluación, mitigación y cooperación; esta última reconocida como un elemento fundamental para afrontar los ciberriesgos como un riesgo sistémico, que requiere la correlación de eventos e incidentes sucedidos más allá del perímetro de las empresas. La interdependencia que existe en el ciberespacio hace de la cooperación una necesidad básica, para contener y responder ante situaciones de ataque que podrían desestabilizar a un gran número de organizaciones, hecho que daría lugar a un estado catastrófico de interoperabilidad.

El más reciente estudio de EY revela que la ciberseguridad en las organizaciones debe habilitar una ventaja competitiva en la era digital, capitalizando las lecciones aprendidas que, año tras año, dejan las violaciones a gran escala, sufridas por grandes empresas globales. (EY, 2019). Dicha investigación refleja que la mayoría de las organizaciones (77%) ahora están buscando ir más allá de las técnicas básicas de seguridad cibernética, para perfeccionar sus capacidades utilizando tecnologías avanzadas, tales como inteligencia artificial, automatización robótica de procesos y analítica de datos, entre otras.

Pero es allí donde surge la pregunta: ¿es necesario sufrir un ataque para hacer de los riesgos cibernéticos una prioridad? En respuesta a este interrogante, surge una tendencia poco alentadora la cual indica que, entre las organizaciones afectadas por un incidente en el último año, menos de un tercio (31%) señala que su función de seguridad descubrió la situación que los comprometía.

Comprendida tal situación, ¿puede la ciberseguridad ser determinante en el cumplimiento de los planes estratégicos de las organizaciones?

En mi opinión, son muy limitados los pronósticos de éxito de aquellas

empresas que no aborden la gestión de los ciberriesgos como un elemento fundamental en el cumplimiento de sus objetivos de negocio. Me es difícil visualizar empresas viviendo en un contexto digital que no contemplen los ciberriesgos como un elemento estratégico, quedando abiertamente expuestas a los ataques de gran escala que, con los años se hacen más frecuentes, con mayor impacto y en un complejo panorama de interdependencia.

La digitalización de los negocios trae consigo:

- El incremento de ataques cibernéticos y los costos asociados a los mismos.
- El aumento de los requerimientos regulatorios en las diferentes geografías en las que los negocios se habilitan.
- Tecnologías emergentes utilizadas en el cibercrimen.
- La convergencia de entornos de tecnologías de información y tecnologías de operaciones.
- La acelerada adopción de Internet de las Cosas.

Frente a esta realidad, es clave la intervención de las autoridades para establecer el marco regulatorio que facilitará la convivencia digital segura de las empresas y los ciudadanos, en procura de que la interacción en el contexto digital se lleve a cabo bajo unas normas básicas de transparencia, ética y protección de la privacidad, creando así un entorno de confianza que favorecerá el cumplimiento de los objetivos estratégicos de las diferentes partes interesadas. De lo contrario, seguiremos velando por los intereses particulares y aumentando la exposición de propios y extraños a los ciberriesgos que avanzan a una gran velocidad.

Referencias

Boston Consulting Group. (2017). *Twelve Forces That Will Radically Change How Organizations Work.* BCG. Recuperado de: https://www.bcg.com/publications/2017/people-organization-strategy-twelve-forces-radically-change-organizations-work.aspx

EY. (2019). *Encuesta de seguridad de la información 2018-19 (GISS) ¿Es la ciberseguridad más que protección? .* EY. Recuperado de: https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/$FILE/ey-encuesta-global-seguridad-informacion-2018-19.pdf

Gartner. (2018). *Gartner Top 10 Strategic Technology Trends for 2019*. Recuperado de: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/

World Economic Forum. (2019). *Shaping the Future of Digital Economy and Society*. Recuperado de: https://www.weforum.org/system-initiatives/shaping-the-future-of-digital-economy-and-society

Juan Mario Posada D. *Ingeniero de Sistemas, cursando estudios de postgrado en Gerencia Estratégica. Desde 2005 trabaja como consultor en riesgos tecnológicos y ciberseguridad. Actualmente, se desempeña como gerente de Servicios de Asesoría en EY, liderando los servicios de ciberseguridad.*

XIX Encuesta Nacional de Seguridad Informática

DOI: 10.29236/sistemas.n151a3

Evolución del perfil del profesional de seguridad digital.

Resumen
La encuesta nacional de seguridad informática, capítulo Colombia, soportada por la Asociación Colombiana de Ingenieros de Sistemas (ACIS) y realizada a través de Internet, entre los meses de febrero y abril de 2019, contó con la participación de 299 encuestados, quienes con sus respuestas revelan tendencias particulares para Colombia en los temas de seguridad y control. Este ejercicio fue motivado a través de diferentes redes sociales, comunidades y grupos, y contó con la cooperación de otras asociaciones como ISACA, Capítulo Bogotá, TacticalEdge, y CISOS.CLUB. Los resultados de este estudio muestran un panorama de las organizaciones colombianas, en sus distintos sectores productivos, frente a la seguridad de la información y/o ciberseguridad y su evolución en las diferentes dimensiones incluidas en la encuesta.

Palabras clave
Seguridad de la información, encuesta, líder, perfil profesional, riesgos de información

Introducción

Entender la realidad nacional en materia de seguridad de la información y ciberseguridad permite visualizar los retos a mediano y largo plazo, además de construir mejores posiciones al respecto en las organizaciones. Ese entendimiento, sumado a conocer el contexto internacional, proporciona una proyección al entorno nacional para enfrentar los retos y desafíos en ambientes cada vez más permeados por la realidad digitalmente modificada.

De la misma manera que en otras versiones, la Encuesta Nacional pretende medir las dinámicas y lógicas de las empresas del país, ver otros referentes mundiales en la búsqueda y construcción de los propios.

Año tras año, este estudio ha reflejado cómo ha venido desarrollándose en Colombia la protección de la información en los entornos digitales y cómo en los diferentes sectores (industrial y empresarial), la seguridad y la resiliencia digital se convierten en un valor dentro de las organizaciones.

Con esto en mente y considerando otros estudios internacionales como el realizado por PwC, IBM, Ponemon, Deloitte, EY, CISCO, Verizon, Foro Económico Mundial, Champlain College Online (CCO), Fortinet, IDC y Kaspersky se procederá a analizar los resultados de la Encuesta Nacional de Seguridad Informática ACIS 2019.

Dentro de los estudios referentes consultados y analizados, se encuentran el Global State of Information Security realizado por la firma Pricewaterhousecoopers (PwC, 2018), el Global Information Security Survey 2018-19 consolidado por la empresa Ernst &Young (EY, 2018), el Informe Anual de Seguridad de la compañía Cisco (CISCO, 2019), los resultados del documento State of Cybersecurity Implications elaborado por ISACA (ISACA, 2019), el reporte Measuring & Managing the Cyber Risks to Business Operations (Tenable-Ponemon, 2019), el informe anual denominado Data Breach Investigation Report (Verizon, 2019), el reporte llamado The Cyber Resilient Organization, generado por la empresa Ponemon en asocio con IBM (Ponemon, IBM, 2019), el informe de Deloitte The Future of Cyber Sphere (Deloitte, 2019), The Global Risk Report (WEF, 2019), el reporte Anticipating the Unknowns (CISCOb, 2019), el reporte The State of the Cybersecurity Workforce and Higher Education (CCO, 2018), el reporte Out of the Shadow: CISO is in the spotlight! (PwC Luxemburgo, 2018), el reporte The Ciso Ascends From Technologist To Strategic Business Enabler (Fortinet, 2019), The Modern Connected CISO

(IDC, 2019), el reporte What It Takes to Be a CISO: Success and Leadership in Corporate IT Security (Kaspersky, 2019) y el reporte 22nd Annual Global CEO Survey (PwCb, 2019).

Estructura de la encuesta

El estudio contempla 43 preguntas repartidas en varias secciones sobre diferentes asuntos.

Demografía: describe la información del encuestado, cuáles son las tareas que realiza, la visión de la seguridad, además de los roles que en tal sentido puedan existir dentro de su organización. Datos que permiten ubicar el sector al que pertenece, el tamaño y tipo de empresa.

Presupuestos: relaciona todos los aspectos asociados con los recursos financieros destinados en materia de seguridad y, sobre todo, en qué se concentra la inversión de dichos recursos.

Incidentes de seguridad: muestra los detalles y tipos de incidentes presentados, un barrido por las prácticas más importantes en el manejo y diligencia de la evidencia digital, como herramienta en la persecución de los ciberdelincuentes.

Herramientas y prácticas de seguridad: se refiere a las prácticas comunes en materia de seguridad, ese conjunto de acciones que permite a las organizaciones definir una postura clara en materia de protección.

Políticas de seguridad: busca conocer el estado de las políticas de seguridad, la práctica de la gestión de riesgos y su integración en el contexto organizacional.

Capital intelectual: busca definir cómo son las áreas de seguridad y las características básicas en materia de experiencia, formación y capacitación de los profesionales de seguridad. Muestra también la relación de las instituciones de educación superior frente a una realidad tan cambiante.

Temas emergentes: en esta sección se analizan varios aspectos, entre ellos: la percepción del futuro en materia de ciberseguridad; la vinculación de los directivos de la organización en la ciberseguridad empresarial, además de la responsabilidad y el papel del líder de seguridad en el desarrollo de la dinámica de protección de la empresa.

Hallazgos principales

De la información recogida en este estudio se muestran en la gráfica 1 los aspectos clasificados como importantes por todos los encuestados y reunidos en un grupo denominado top de Hallazgos de las dimensiones de la encuesta.

En la Gráfica 1 se encuentran los datos más relevantes de la encuesta. El 74% de los encuestados reconoce no usar una estrategia de e-discovery o descubrimiento electrónico para soportar los litigios o reclamaciones legales; un 70%

Gráfica 1: Top de Hallazgos

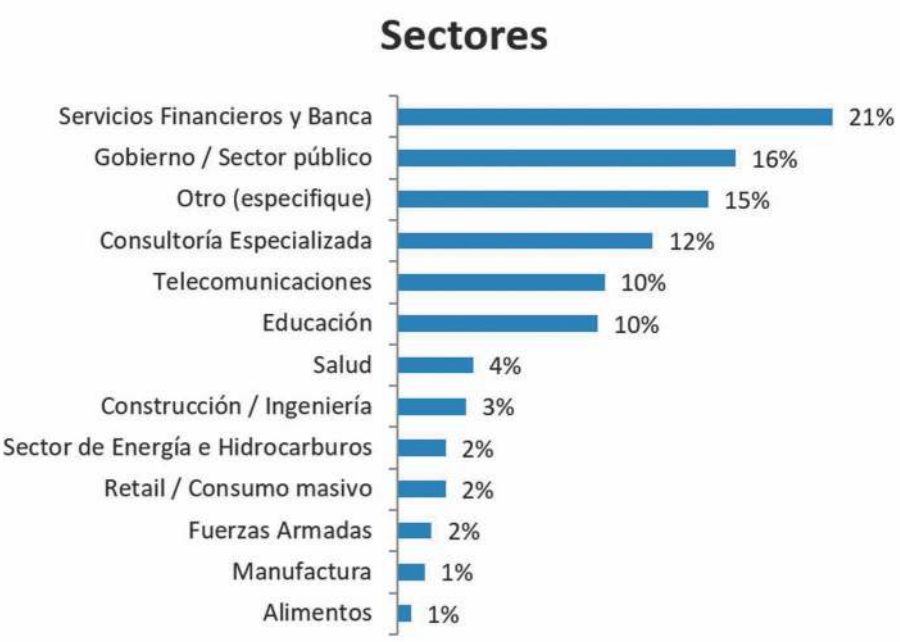
cuenta con un presupuesto para la seguridad de la información en las empresas de la realidad de Colombia. Un 70% indica que la tarea fundamental del responsable de seguridad en Colombia es definir los controles de TI en materia de seguridad de la información. El 70% de los encuestados respondió que en sus empresas se realizan los ejercicios de evaluaciones de riesgos en los que se incluye la seguridad de la información. Las áreas de seguridad en Colombia están conformadas entre 1 y 5 personas como lo resalta el 64% de los participantes. Las amenazas persistentes avanzadas son la preocupación más importante, según el 50% de los encuestados en Colombia. Por último, el 44% manifiesta que la forma como se mantienen actualizados de las fallas de seguridad en Colombia es a través de la lectura de revistas especializadas en materia de seguridad.

Demografía

Sectores participantes

La Gráfica 2 refleja la participación de 13 sectores de la economía colombiana. Los tres segmentos con mayor injerencia están compuestos por el sector financiero, servicios de consultoría especializada y el Gobierno.

La Gráfica 3 muestra el tamaño de las empresas en Colombia, de acuerdo con el número de empleados. El 25% de las empresas está entre los 1001 a 5000 empleados,

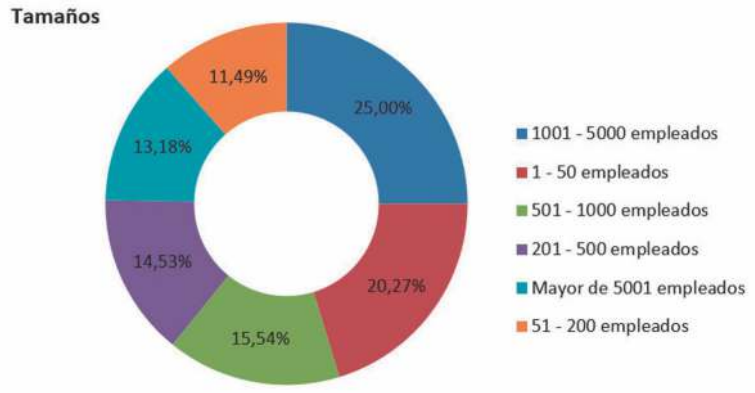


Gráfica 2: Sectores participantes

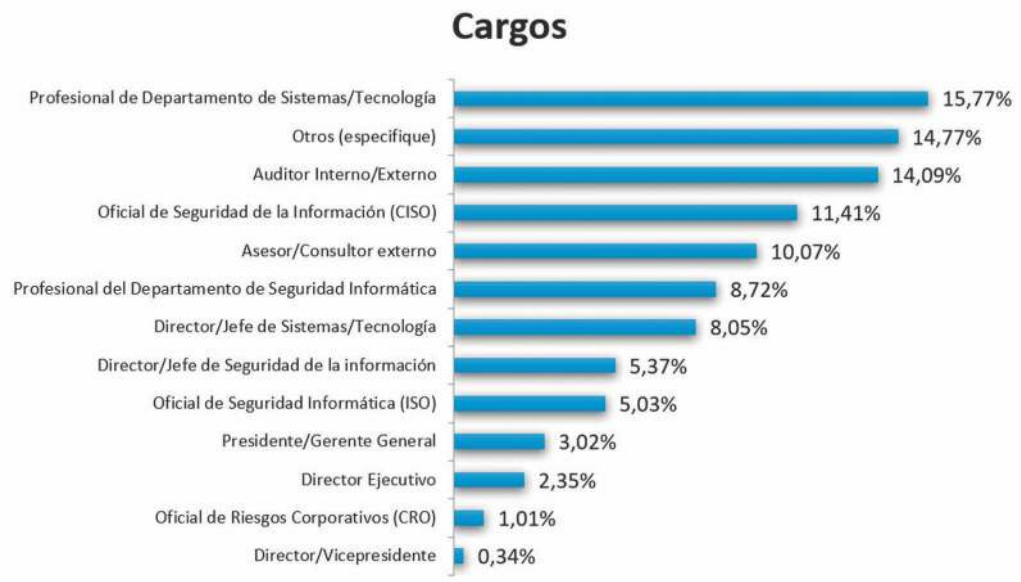
el segundo lugar son las empresas pequeñas (20,27%) que cuentan con 1 a 5 empleados.

La Gráfica 4 muestra los cargos de los encuestados, entre los que se cuentan profesionales de las áreas de TI, auditores internos, oficiales de seguridad, consultores, entre otros. Así mismo, figuran otras clasificaciones para los profesionales de seguridad digital en el país, tales como analistas y profesionales de planta de seguridad, docentes de cátedra y planta de las áreas de seguridad, como los más relevantes.

En la Gráfica 5 se observan las tareas realizadas por los profesionales de seguridad dentro de las orga-



Gráfica 3: Tamaño de las empresas



Gráfica 4: Cargos de los Encuestados

Gráfica 5: Funciones del responsable de seguridad

Gráfica 6: Dependencia del área de Seguridad

nizaciones. El porcentaje más alto está representado en definición de controles de TI en materia de seguridad de la información, velar por la protección de la información empresarial y establecer e implementar un modelo de políticas en materia de seguridad de la información como las principales.

La Gráfica 6 muestra de quién depende el área de seguridad. Los datos indican que el área de seguridad depende de una dirección propia, Director/Jefe de Seguridad de la Información, seguido del Director/Jefe de Seguridad Informática y como tercer lugar la Vicepresidencia/Director Departamento de Tecnologías de la Información.

En la Gráfica 7 se observan los roles dentro de una organización en materia de seguridad digital. En Colombia figuran los analistas de seguridad (información e informática); le sigue el cargo denominado CISO, al que se suman los ingenieros de pruebas, entre los principales roles.

Consideraciones de los datos

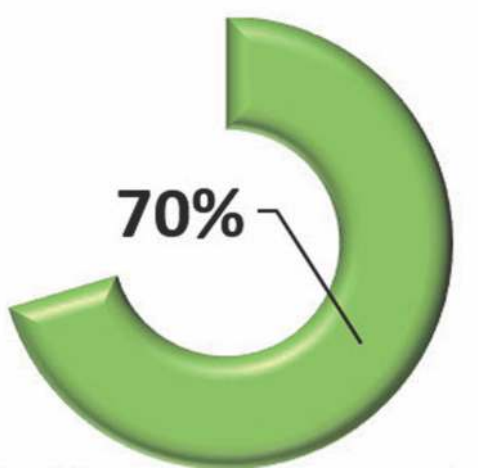
Según el Data Breach Report (2019) de la Firma Verizon, la mayor cantidad de brechas identificadas involucra a negocios pequeños o medianos (43%). Basado en la participación de las empresas que participaron, más del 60% corresponde al rango de pequeñas, medianas empresas y se infiere que, existen altas probabilidades de que las empresas colombianas puedan ser víctimas de un ataque informático. De acuerdo con (CISCOb, 2019), una de las funciones primarias de los responsables de seguridad de las empresas está relacionada en primer lugar con la atención a los riesgos, poner límites a

Gráfica 7: Roles de Seguridad

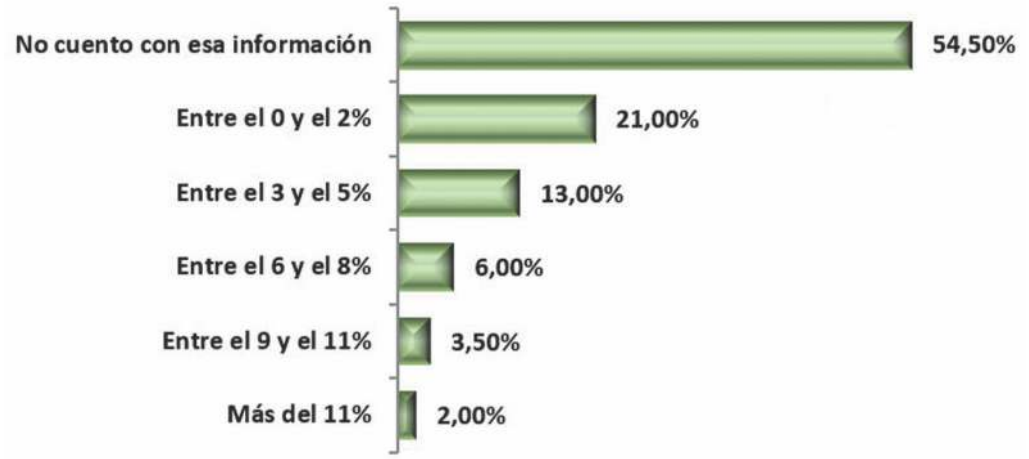
los temas de presupuestos, colaboración con las áreas de la organización, educar y crear cultura, saber cómo se presentan los beneficios de las inversiones en seguridad y ser estratégico en la venta de la implementación de soluciones técnicas de seguridad. En otro informe (Kaspersky, 2019), se resalta que la identificación de riesgos y amenazas son tareas claves de los profesionales de seguridad. Al revisar la tendencia nacional dista completamente. La función principal está relacionada con la implementación de soluciones de TI, basado en 2019.

Presupuestos

En materia de presupuestos, la realidad colombiana es muy interesante en el mundo de la seguridad digital. El 70% de los participantes manifiesta que sí tiene presupuesto asignado a la seguridad digital de sus organizaciones, lo cual se refleja en la Gráfica 8. La Gráfica 9 muestra el monto del presupuesto en relación con el presupuesto global; cerca del 46% de los encuestados lo conoce, mientras que el 54% dice no conocer o no tener la información. La Gráfica 10 refleja la distribución de los presupuestos en dólares. Cerca del 47% tiene un

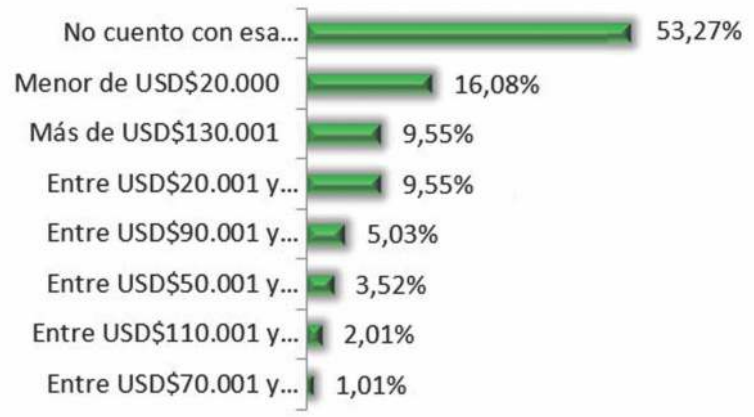


Gráfica 8: Presupuesto de Seguridad

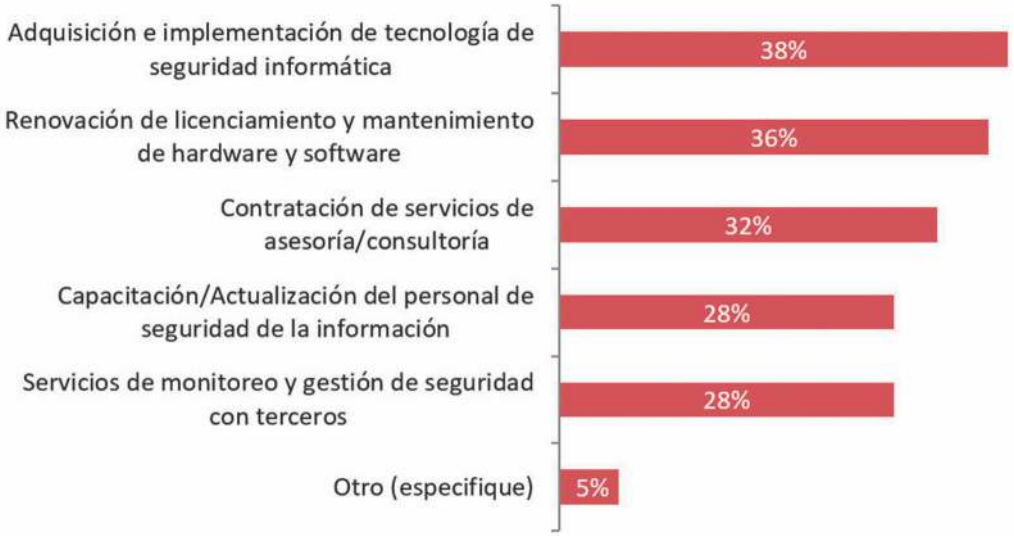


Gráfica 9: Porcentaje del presupuesto Global

monto asignado para la seguridad, el 53% restante manifiesta no conocer dicha información. Esto se puede explicar, toda vez que los cargos de mayor participación están compuestos por auditores y los profesionales de las áreas de tecnologías que pueden no conocer los detalles internos de las áreas de seguridad. La otra gran razón para que se de esta realidad es que muchos de los roles de las organizaciones están asociados con los analistas de seguridad, quienes pueden no conocer estos detalles. La Gráfica 11 muestra cómo se están realizando las inversiones en materia de seguridad. La inversión en tecnologías de seguridad es la parte más importante, seguida de la renovación del licenciamiento de algunas tecnologías en materia de seguridad digital; los servicios de consultoría y asesoría ocupan el tercer lugar; la tercerización de servicios, en materia de seguridad, están en cuarto lugar, y la capacitación y actualización de los profesio-



Gráfica 10: Presupuesto de Seguridad



Gráfica 11: Inversión de Seguridad

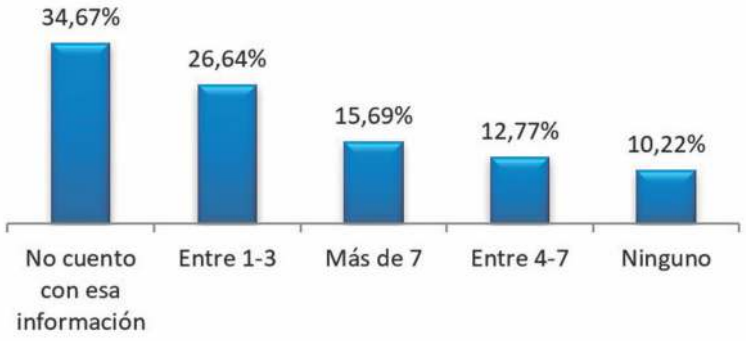
nales de seguridad es el último criterio sobre los presupuestos. La Gráfica 12 representa cuánto dinero se invierte en los criterios identificados. La franja de menos de $US20.000 dólares en Colombia es la que tiene los mayores valores. Sin embargo, la franja de más de $US130.000 dólares es la siguiente, específicamente los servicios gestionados y las relaciones con terceras partes.

Consideraciones de los datos

Los reportes internacionales ratifican la tendencia en Colombia de aumentos pequeños en los presupuestos de seguridad en las organizaciones de todos los tamaños y sectores. No obstante, al revisar el informe (Ponemon, IBM, 2019), se ven grandes diferencias en los valores asignables de presupuestos, según los datos del informe las franjas de los presupuestos están

	Entre US D$110.001 y USD$130.000	Entre US D$20.001 y USD$50.000	Entre US D$50.001 y USD$70.000	Entre US D$70.001 y USD$90.000	Entre US D$90.001 y USD$110.000	Más de USD$130.001	Menor de USD$2
Adquisición e implementación de tecnología de seguridad informática	6%	20%	4%	4%	7%	26%	33%
Capacitación/Actualización del personal de seguridad de la información	4%	22%	9%	2%	7%	22%	33%
Contratación de servicios de asesoría/consultoría	8%	20%	4%	2%	14%	28%	24%
Renovación de licenciamiento y mantenimiento de hardw are y softw are	5%	15%	11%	4%	9%	25%	31%
Servicios de monitoreo y gestión de seguridad con terceros	3%	8%	8%	5%	14%	32%	30%

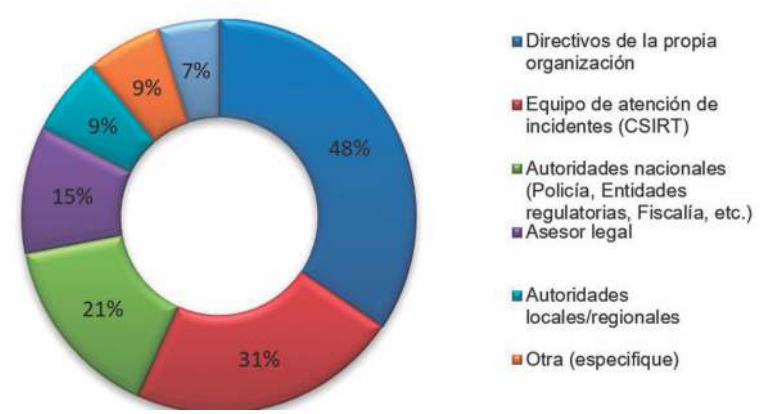
Gráfica 12: Montos en dólares de las inversiones de seguridad. Sectores vs. inversiones



Gráfica 13: Cantidad de Incidentes. Incidentes

entre los $US6 a $US10 millones de dólares como el mejor valor relacionado con el presupuesto sólo asignado a la ciberseguridad. Si bien influyen las realidades económicas y digitales en donde se reali-

Gráfica 14: Tipos de Incidentes de Seguridad



Gráfica 15: A quien se reportan los incidentes

zan los estudios, lo que sí vale resaltar son las tendencias de tener unos presupuestos más dotados para el mundo de la ciberseguridad. En el caso colombiano lo que sí se puede ver es que la franja mayor a los $US130.000 dólares también tiene un porcentaje importante y con tendencia a seguir creciendo en los próximos años.

Incidentes

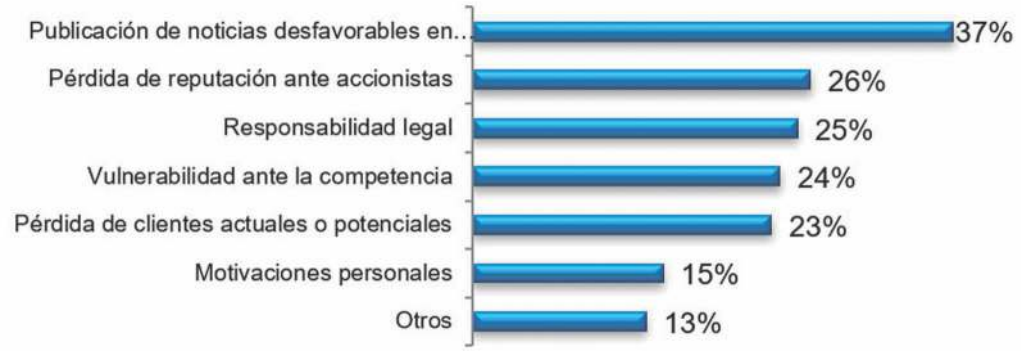
En Colombia se mantiene la tendencia en materia de incidentes de seguridad en concordancia con las tendencias internacionales. Tales desafíos, en términos de preparación y atención, son una exigencia para las organizaciones.

La Gráfica 13 muestra la cantidad de incidentes que se presentan en Colombia, según los participantes. El 56% de ellos manifiesta haber tenido, por lo menos, un incidente de seguridad o ciberseguridad en sus organizaciones. El 35% de los participantes no tiene información al respecto, el 10% de los participantes resalta que no tuvieron un incidente de seguridad.

La Gráfica 14 relaciona los tipos de incidentes que se presentaron en las organizaciones. En ella se relacionan los errores humanos, el *phishing*, la instalación de *software* malicioso y la ingeniería social como los de mayor incidencia.

La Gráfica 15 muestra a quién se reportan los incidentes de seguridad. Los datos reflejan que, ante un incidente y su identificación, el 48% de los participantes lo notifica a la propia organización en cabeza de sus directivos; 31% a los equipos de atención de incidentes CSIRT y 21% a las autoridades de orden nacional como los datos más relevantes.

La Gráfica 16 las razones por las que no se denuncian los incidentes. Se destacan fundamentalmente la imagen 37%, la reputación 26%, y la responsabilidad legal 25%, como las razones que aducen los en-



Gráfica 16: Razones para no denunciar los incidentes

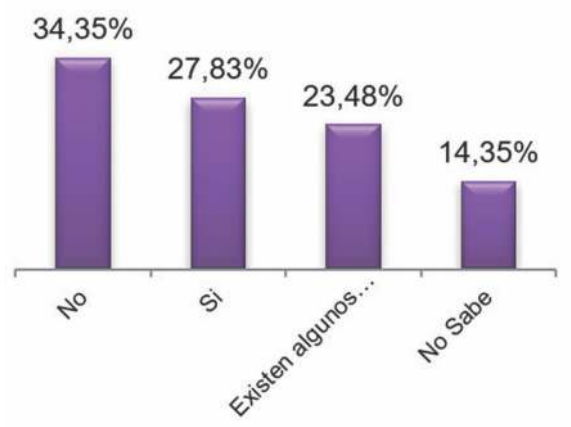
Gráfica 17 Mecanismos para denunciar/compartir

cuestados sobre el porqué no se denuncian los incidentes. La Gráfica 17 muestra la forma los mecanismos que se podrían utilizar para compartir información o denunciar información. En primer lugar, usar canales privados y cifrados como el mecanismo más idóneo, 56%.

La evidencia digital y su uso dentro del proceso de gestión de incidentes es pieza fundamental para un adecuado mejoramiento. La Gráfica 18, resalta la importancia y consciencia en relación con el adecuado manejo de la evidencia digital. El 74% resalta que es consciente de

Gráfica 18: Consciencia de la Evidencia Digital

ello. Sin embargo, la Gráfica 19 muestra que el 34% no posee un



Gráfica 19: Procedimiento de Gestión de Evidencia Digital

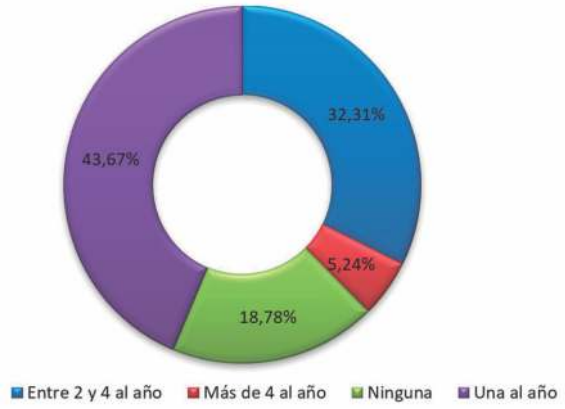
Gráfica 20: Contactos con autoridades locales/regionales

procedimiento para hacer la gestión de la evidencia digital. La Gráfica 20 resalta que el 62% mantiene algún tipo de contacto con autoridades del orden local o regional. La Gráfica 21 señala que el 74% de los participantes no posee una estrategia para el descubrimiento electrónico, que les permita soportar litigios o reclamaciones legales.

Consideraciones de los datos

Los reportes internacionales como (Tenable-Ponemon, 2019) y (CISCO, 2019), indican que los incidentes que interrumpen los procesos (54%) son la preocupación más grande para las empresas. Esto ratifica lo encontrado para la realidad de Colombia, sobre los incidentes en Colombia como *Malware, Phishing* y Acceso no autorizado, los cuales son incidentes que van en la misma línea de interrumpir las operaciones de las empresas. De igual manera, la presencia de los incidentes en Colombia se puede ratificar con el informe (Ponemon, IBM,

Gráfica 21: e-discovery



Gráfica 22: Evaluaciones de Seguridad

2019) según el cual cerca del 79% de las compañías tienen más de un incidente de seguridad. El mismo informe resalta la importancia de intercambiar y compartir la información, 58%; dicho estudio resalta que se han visto beneficiados con compartir información, toda vez que sus procesos de aprendizaje y contención frente a los incidentes de seguridad han mejorado. En Colombia aún no se piensa del todo en ello y por tanto se evidencia lejanía de esta práctica. La práctica de la gestión de incidentes que en Colombia según los datos se resalta como una práctica no desarrollada, se ratifica a través del informe (EY, 2018) el cual describe que las inversiones en seguridad están orientadas a fortalecer la gestión de incidentes, toda vez que se considera una práctica con muy poca madurez en las organizaciones, cerca del 10% de los participantes hace esta consideración. El informe (Deloitte, 2019), resalta que los impactos mayores a la hora de un incidente se expresan en términos de pérdidas de utilidades (21%), pérdida de confianza (21%), pérdida de reputación (16%), multas y sanciones (14%). Estos datos ratifican las preocupaciones de los responsables de seguridad al no denunciar los incidentes, toda vez que la pérdida de la reputación, confianza, sanciones y/o multas son las razones que se aducen para no hacerlos.

Herramientas

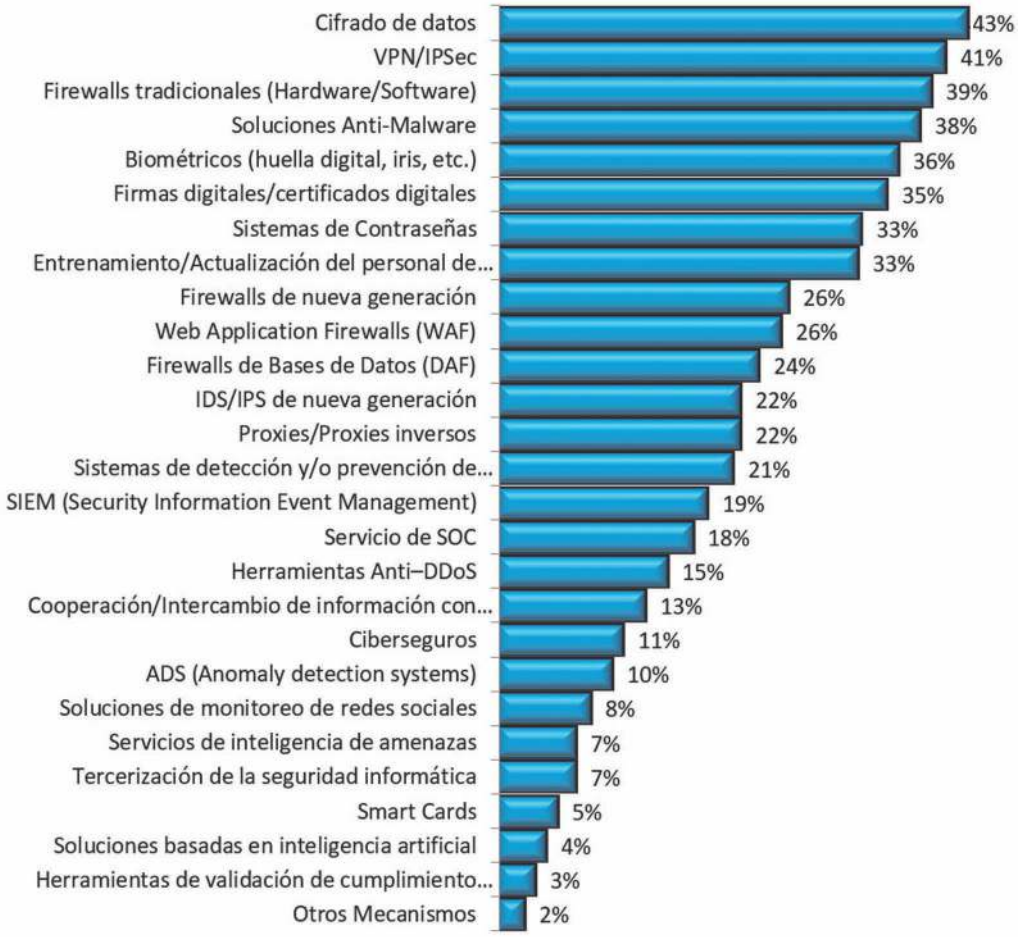
La Gráfica 22 muestra el uso de las evaluaciones de seguridad como una de las prácticas más usadas. Un 82% de los participantes manifiesta hacer uso de esta práctica como instrumento clave para validar el estado de la seguridad digital de la organización. El 44% de los participantes usa esta práctica una vez al mes; el 32% entre dos y 4 veces al año; el 19% usa más de 4 veces al año y el 5% dice no usarla.

La Gráfica 23 indica cuáles son los mecanismos de seguridad comúnmente usados en las organizaciones. El cifrado de datos 43%, VPNs 41% y Firewalls tradicionales 39% son los tres mecanismos más usados basados en las respuestas de los participantes.

La gráfica 24, enfatiza en las herramientas que más se usan para notificarse de las fallas de seguridad los profesionales. El 44% usa la lectura de sitios especializados, como la práctica más común.

Consideraciones de los datos

La tendencia en Colombia se mantiene comparada con los años anteriores. Así mismo lo ratifican los datos internacionales, el informe de (Deloitte, 2019) muestra que las organizaciones interactúan con sus unidades de negocios a través de las evaluaciones de seguridad o auditorías, en un 29% El informe de (Tenable-Ponemon, 2019) señala que la frecuencia de realizar las evaluaciones de seguridad muestra la madurez y la madurez tiende a mostrar priorización para realizar



Gráfica 23: Mecanismos de Seguridad

estos ejercicios. Así las cosas, en Colombia los datos muestran una evolución significativa de esta práctica y basado en ello es posible afirmar que hay una tendencia a la madurez de la misma.

Políticas

La Gráfica 25 refleja el estado de las políticas de seguridad en las organizaciones colombianas; el 61% de los encuestados manifiesta tener formalizada sus políticas de se-

Gráfica 24: Mecanismos de notificación

Gráfica 25: Estado de las Políticas

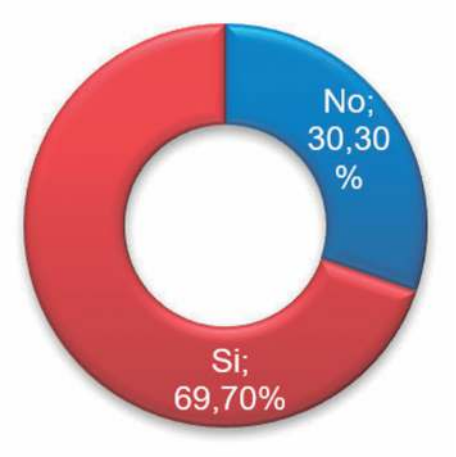
guridad, el 28% actualmente en desarrollo y, sólo el 11%, dice no tener políticas de seguridad de la información.

La Gráfica 26, muestra lo que manifiestan los participantes al indagar por los obstáculos por los cuales no hay una postura adecuada de seguridad en sus empresas.

La gestión de riesgos como parte estructural de las funciones y tareas de los responsables de seguridad y sus organizaciones es otro de los componentes clave. En la Gráfica 27, el 69% de los participantes hace una evaluación de riesgos de seguridad digital y la incluyen en sus ejercicios globales de gestión de riesgos. En la Gráfica 28, el 69% realiza ejercicios de evaluación de riesgos una vez al año, el 22% dos al año y el 9% más de dos al año.

La gráfica 29, muestra las razones de por qué no es realizada la ges-

Gráfica 26: Obstáculos de la Seguridad



Gráfica 27: Gestión de Riesgos de Seguridad

tión de riesgos. El primer motivo que señalan los participantes está relacionado con no disponer de un proceso formal de gestión de riesgos (35%).

La Gráfica 30 muestra el tipo de metodologías usadas al realizar los ejercicios de gestión de riesgos de seguridad; la ISO 31000, con un 27%, es la metodología más usada. La Gráfica 31, indica que los incidentes de seguridad son asociados a algún tipo de riesgos. El 55% de los incidentes se asocia como cate-

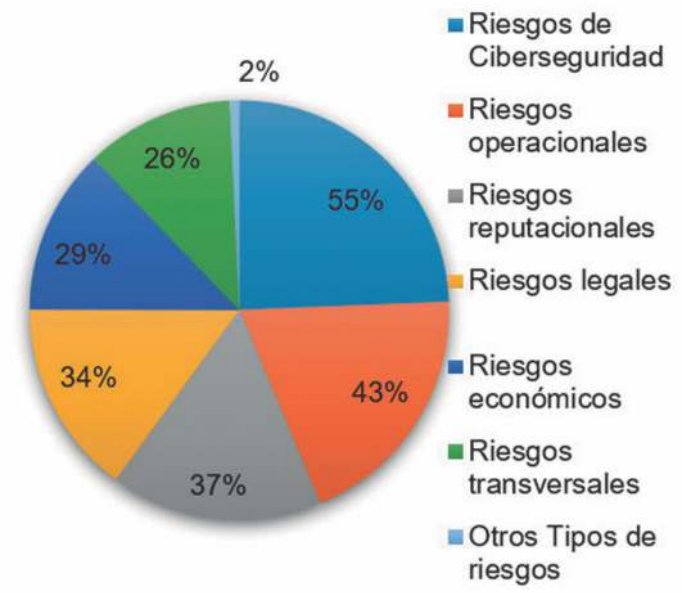
Gráfica 28: Cantidad de Gestión de Riesgos en Seguridad

Gráfica 29: Razones para no realizar la gestión de riesgos

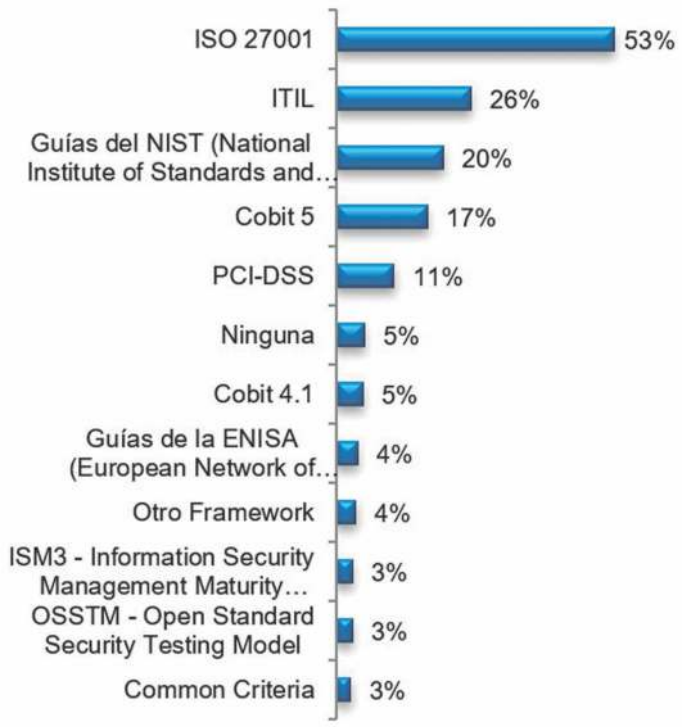
Gráfica 30: Tipos de Metodología

goría en los procesos de identificación de riesgos, a los riesgos de ciberseguridad; el 43% lo asocia a riesgos de operación, el 37% los relaciona con riesgos reputacionales.

La Gráfica 32 ilustra el uso de los distintos marcos de trabajo (*frameworks*) usados en las organizaciones colombianas: ISO/IEC 2700, ITIL, NIST y Cobit 5 son los más usados. La Gráfica 33 refleja las regulaciones a las que las organizaciones están sometidas; en el caso colombiano, el 66% de los participantes manifiesta que sí existen re-



Gráfica 31: Tipos de Riesgos



Gráfica 32: Marcos de trabajo usados

gulaciones a las que sus organizaciones se ven sometidas. La tendencia internacional se orienta a que, cada vez más, existirán regulaciones más globales. La regulación GDPR (General Data Protection Regulation) nace como una necesidad de la Comunidad Europea

Gráfica 33: Regulaciones o normativas

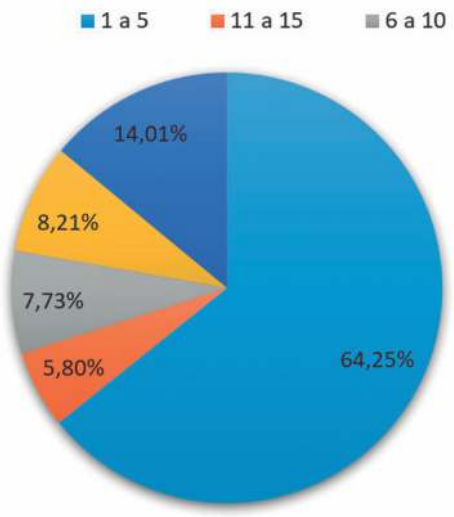
(EU), de gran impacto a nivel global.

Consideraciones de los datos

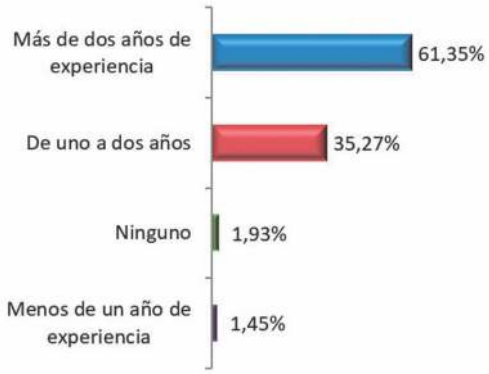
En definitiva, los riesgos de seguridad de la información y ciberseguridad son una realidad como lo ratifica el informe del Foro Económico Mundial (WEF, 2019), el cual manifiesta que la prioridad de estos tipos de ataques es alta en las organizaciones del mundo. Esto ratifica la tendencia de los resultados de Colombia que ven en la práctica de gestión de riesgos una herramienta vital para la construcción de capacidades frente a la atención de los ciberataques, así se ve ratificado en el informe de (PwC, 2018), en el que el 39% está muy confiado en sus capacidades de gestionar ciberataques basados en la práctica de gestionar los riesgos. Así mismo, el informe de (Deloitte, 2019) indica que el 50% de los participantes usan metodologías de riesgos y la cuantificación de los mismos como instrumentos y prácticas sólidas para la atención de los ciberataques de seguridad en las empresas. Con relación a las políticas y su adopción la tendencia de Colombia apunta a tener un modelo fortalecido en relación con las políticas, ratificado con el informe de (CISCO, 2019), el cual señala que más del 85% conoce muy bien las políticas y su efecto dentro de las organizaciones.

Capital intelectual

La Gráfica 34 muestra el grupo de organizaciones que cuenta con un recurso dedicado a la seguridad; en ellas, cerca del (86%) manifiesta tener recursos dedicados a la seguridad. La Gráfica 35 muestra que el tiempo de experiencia promedio para que los profesionales de seguridad sean contratados en Colombia es superior a dos (2) años (62%).

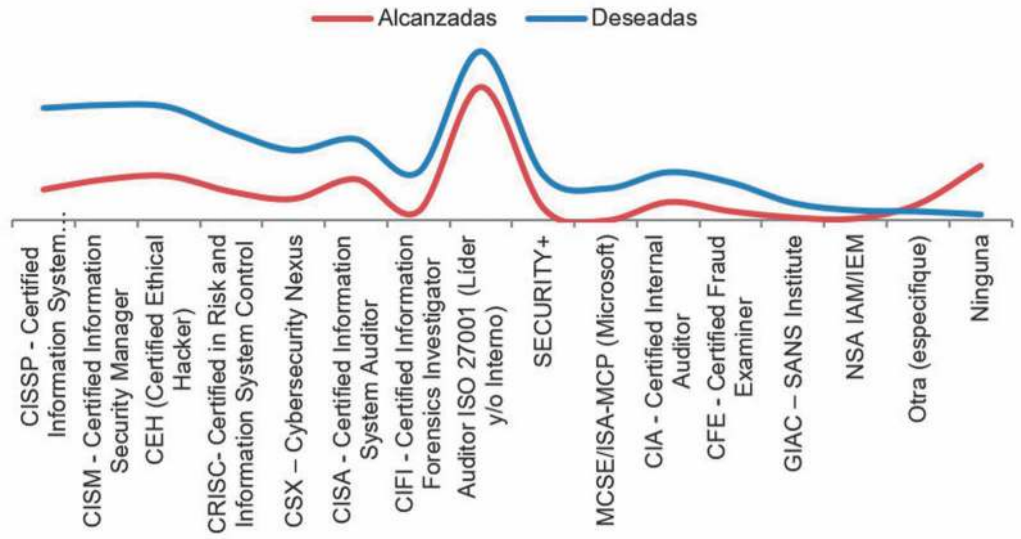


Gráfica 34: Recursos dedicados a la Seguridad



Gráfica 35: Experiencia del profesional

La Gráfica 36, representa la comparación de las certificaciones que



Gráfica 36: Certificaciones alcanzadas vs deseadas

los profesionales de seguridad poseen en la actualidad y que desean alcanzar en el tiempo. CISSP, CISM, CEH, CRISC son las certificaciones que mayor variación tienen de lo poseído actualmente y lo deseado en el futuro no muy lejano.

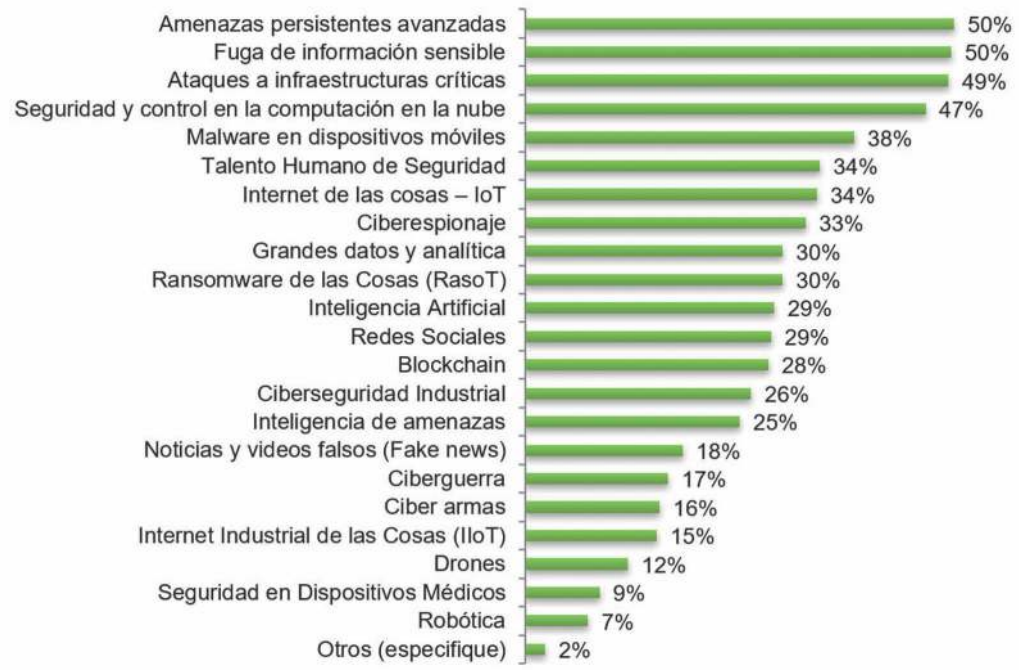
La Gráfica 37, indaga sobre la forma en que la educación ha participado en la formación de los profesionales de seguridad. El 31% manifiesta que los niveles de investigación son escasos; el 28% manifiesta que existen limitados labora-

Gráfica 37: Papel de la educación

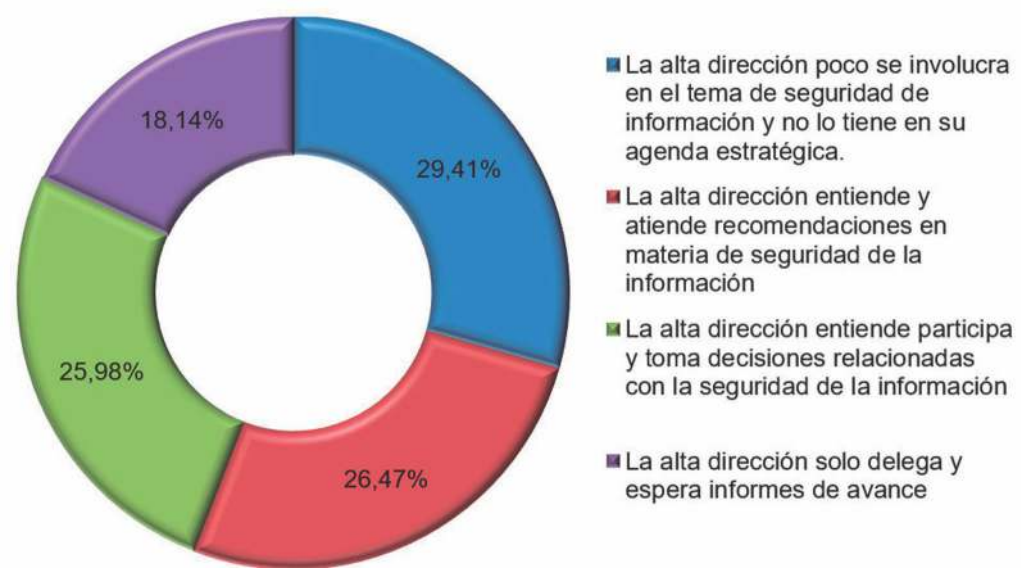
torios e infraestructuras para soportar los cursos especializadas 28%.

Consideraciones de los datos

La experiencia del profesional de seguridad de las organizaciones en Colombia es clave, así como su formación. Las tendencias internacionales ratifican los resultados de Colombia. En su informe (Kaspersky, 2019), lo resalta diciendo que muchos de los perfiles de seguridad (CISO), fundamentalmente, tienen más de 5 años de experiencia en el cargo (52) %; sólo un 12% tiene entre uno y dos años de experiencia en el cargo. Desde el punto de vista académico, el mismo informe señala que el (68%) de los CISOs tienen una maestría. En cuanto a las certificaciones se observa que sólo el 46% de la población estudiada posee una certificación. No obstante, el informe (Kaspersky, 2019) ratifica la tendencia de Colombia en términos de certificaciones, con ISO 27001, CISSP, CISM como las certificaciones más apetecidas por los profesionales de seguridad a nivel global; hecho confirmado en el informe (PwC Luxemburgo, 2018). Por el lado de la educación superior, el informe (CCO, 2019) resalta que 72% de las personas en este estudio seguiría una carrera en ciberseguridad, si ésta fuera financiada por su empleador. El mismo informe indaga sobre cómo las universidades pueden trabajar y ayudar en la creación tanto de formación como de soluciones para enfrentar los desafíos en materia de ciberseguridad y



Gráfica 38: Desafíos del 2019

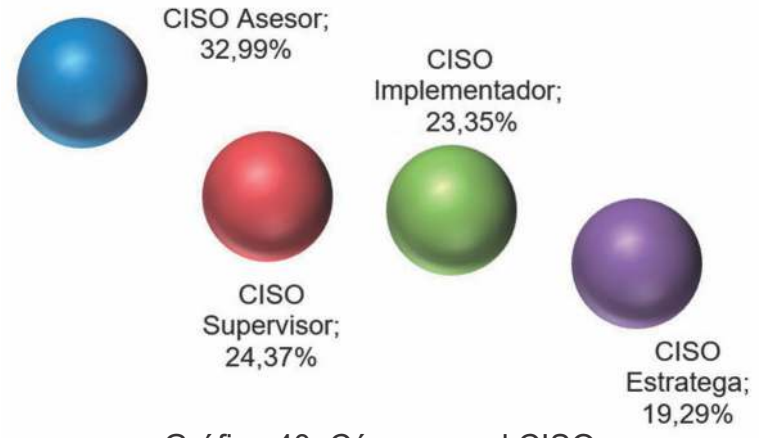


Gráfica 39: Involucramiento de los Directivos

concluye que el sector de la educación juega un papel fundamental en ambos sentidos; el 91% considera que se pueden crear más programas de formación, así como ayudar a desarrollar mejores capacidades para desempeñar los diferentes cargos de la ciberseguridad (90%). Al revisar los datos nacionales se ratifica el potencial de la universidad en la formación de capacidades acordes con los roles; sin embargo, no se observa que en Colombia exista esta potencial formación de los profesionales de seguridad.

Temas emergentes

La Gráfica 38 muestra los temas relevantes y emergentes que tienen en la mira los profesionales de seguridad. El más relevante, las amenazas persistentes avanzadas, fuga de información sensible, los ata-



Gráfica 40: Cómo ven al CISO

Gráfica 41: Entrega de información del profesional de seguridad

ques de infraestructuras críticas y la seguridad de la computación en la nube son los de más alto valor.

La gráfica 39, relaciona la forma en cómo las juntas directivas, o comités ejecutivos se relacionan con la seguridad. El 57% están atendiendo y participando activamente, mientras que el 47% restante delega o poco se involucra en los temas de seguridad en Colombia.

Las Gráficas 40, 41 y 42 reflejan la forma como el CISO se ve, se desenvuelve y cómo puede evolucionar en el contexto de las organizaciones nacionales. La Gráfica 40 muestra la forma como es visto el profesional de seguridad. En este año, el 33% resalta que en Colombia es visto como un asesor, luego como supervisor, implementador y en último lugar como estratega.

La Gráfica 41 muestra la forma como el líder de seguridad se comunica con la organización y se observa que la información comunicada hoy por parte del líder de seguridad está relacionada con la gestión de la seguridad para la toma de decisiones (31%), seguido de la información relacionada con las brechas de seguridad (29%) y, en tercer lugar, la información relacionada con los riesgos (29%).

La Gráfica 42 muestra las oportunidades de crecimiento y mejora en las que los profesionales de seguridad pueden trabajar, como parte del cierre de brechas existentes. En primer lugar, las habilidades técnicas y/o experiencia en lo que puede enfocarse el líder de seguridad por mejorar (41%), seguido de las habilidades gerenciales (37%) y, en tercer lugar, la formación académica y técnica (32%).

Consideraciones de los datos

Los diferentes informes como (EY, 2018), (CISCO, 2019), (CISCOb,

2019), (Deloitte, 2019), e (IDC, 2019), ratifican las observaciones de los datos de Colombia en relación con los temas más relevantes del presente y futuro cercano, observados por los responsables de seguridad digital del país. La nube es la tendencia en todos los informes y confirma lo que sucede en Colombia; la movilidad y sus ataques, aunque no está en el top de preocupaciones, sí está en la agenda; los ataques complejos como APT (Amenazas Persistentes Avanzadas) y los ataques a infraestructuras críticas son otros de los elementos que dichos informes muestran como temas claves para ser observados por los profesionales de seguridad. En cuanto a los mismos se ratifica que las habilidades gerenciales, el liderazgo y la comunicación son piezas fundamentales de los nuevos líderes de seguridad, así lo manifiesta el reporte (Fortinet, 2019). En consecuencia, se ratifica lo observado para la realidad colombiana. En Colombia se ve al CISO como un asesor y supervisor de la seguridad; al contrastar los informes internacionales como (IDC, 2019), (Kaspersky, 2019), (PwC Luxemburgo, 2018), los cuatro informes confirman que el CISO es visto como un elemento que cada vez más tiene una visión de negocios; sin embargo (PwC Luxemburgo, 2018) y (IDC, 2019), resalta que el líder de seguridad debe trabajar bastante en su imagen conocida como el "doctor No". En Colombia, la posición del CISO ha evolucionado y se confirma su ascenso en la organización, pasando de labores técnicas a labores de nivel ejecutivo; di-

Gráfica 42: Camino de crecimiento de un profesional de seguridad

cha tendencia se confirma con el informe (PwC Luxemburgo, 2018) en el que se observa que el 34% de los participantes ven al líder de seguridad en un nivel 2 dentro de las estructuras organizacionales. No obstante, como indica el mismo informe y confirmando la tendencia de Colombia, es necesario que se trabaje en fortalecer muchas de sus capacidades. Las altas direcciones tienen en sus mentes las amenazas digitales, así lo muestran los datos en Colombia y de la misma manera lo resaltan las tendencias internacionales (PwCb, 2019), las cuales indican que el 40% de los CEO de las compañías observadas, tienen en el top de sus agendas estos temas y le dan la importancia necesaria.

Reflexiones finales

Cada vez más las organizaciones se enfrentan a una realidad digitalmente modificada, en la que las nuevas tecnologías permean cada uno de los ambientes organizacionales y personales. Esta realidad crea nuevos y desafiantes escenarios que se transforman en riesgos para las organizaciones; sin embargo, invitan a desarrollar nuevos, continuos y creativos esfuerzos en procura de proteger y crear valor como la confianza y confiabilidad, permitiendo lograr posturas digitales más confiables en un mercado competitivo y exigente.

Año tras año, el estudio muestra un afianzamiento de la seguridad digital como un instrumento corporativo en las empresas colombianas. En este contexto, cada vez más incierto, son necesarios los pensamientos amplios que involucren a los actores y los lleven a pensar en un replanteamiento de la protección de la información, sin perder de vista lo ya alcanzado, para enfrentar la realidad del mundo en que se desenvuelven.

Por lo tanto, los ejecutivos de seguridad de esta nueva era se enfrentan de una manera más directa a otros escenarios dinámicos que demandan reacciones rápidas; pero, sobre todo, se trata de espacios que exigen anticiparse a observar los entornos cambiantes y superpuestos, en procura de la protección de la información.

En la realidad colombiana, los datos muestran que los esfuerzos se vienen haciendo, que año tras año las demandas de la realidad digitalmente modificada transforman la visión de la seguridad. El contexto internacional indica la misma tendencia.

En la realidad nacional se pueden concluir los siguientes aspectos:

1. La realidad digital hace que a todos los sectores e industrias les importe el tema de ciberseguridad. A sectores como el financiero, la consultoría especializada y el Gobierno, les interesa participar y conocer la realidad de la seguridad, tendencia observada en diferentes informes

publicados sobre seguridad y ciberseguridad. Sin embargo, sectores como el de la salud y retail vienen observando y dando pasos pequeños en procura de atender la realidad en materia de confianza digital.

2. En las organizaciones colombianas, las áreas de seguridad y ciberseguridad tienen dos posiciones marcadas. Algunas cuentan con una dirección propia y definida, mientras otras dependen formalmente de las áreas de tecnología. Las compañías de gran tamaño, con más de 1000 empleados, son las que tienen mayor claridad en torno a un área independiente y a un director de seguridad. En tales empresas grandes, el área de seguridad depende de las direcciones como la de gestión de riesgos. Es interesante observar entre las organizaciones de todos los tamaños, el bajo porcentaje que no tiene un cargo o responsabilidades definidas.

3. La posición del profesional de seguridad continúa su proceso de afianzamiento dentro de las organizaciones, en una realidad digitalmente modificada. Hoy vemos que el responsable de seguridad ha evolucionado un poco más de su *back* técnico que aún debe ser fortalecido como lo ratifican los datos; ha ido creando capacidades en otras dimensiones que se convierten en claves para el desempeño de su función. Los datos de Colombia muestran la importancia del profesional de seguridad, su relevancia para mantener un negocio con los niveles de confianza digital adecuados pensando en las dinámicas digitales. Así mismo, se invita al profesional a seguir expandiendo y ampliando tanto sus saberes como sus haceres. Hay muchos desafíos y se requiere del crecimiento del profesional de una manera rápida, oportuna y con altos niveles de adaptabilidad para afrontar los desafíos actuales y futuros como líder de seguridad.

4. A nivel nacional, se mantiene la sólida tendencia de usar mecanismos tecnológicos como las principales herramientas de protección; si bien las tendencias internacionales ya dan esto por sentado, sí se debe hacer un llamado tanto a los responsables de seguridad como a las organizaciones, para que vean la seguridad como un tema un poco más amplio. Las tendencias internacionales precisamente ratifican que es necesario extender la visión de la seguridad como una fuente de aporte al valor de la organización y de los objetivos de su negocio.

5. El poder de las anomalías digitales, de los adversarios y de la realidad digital se entiende cada vez más en el marco de las

organizaciones colombianas. Más allá de lo técnico, se registran los errores humanos y, en tal sentido, es necesario pasar de procesos de sensibilización al cambio de comportamientos, liderado por los responsables de la seguridad, con el ánimo de crear una nueva cultura alrededor de entornos digitalmente modificados. Así mismo, es necesario gestionar unos programas de seguridad que permeen todos los niveles organizacionales, sobre prácticas centradas en los diferentes grupos de interés, dirigidas a construir posturas de seguridad diferentes, basadas en los desafíos que debe asumir el talento humano.

6. Las nuevas tecnologías como *Cloud, IoT*, *IA*, *Machine Learning,* entre otras, están cambiando la concepción del mundo, la forma de interactuar y los retos a los que se enfrentan las organizaciones a nivel nacional e internacional. De ahí que los profesionales de seguridad deban tener claridad para profundizar en estas nuevas tendencias y su uso. En ambientes internacionales es limitado el uso de la nube, producto del desconocimiento y los riesgos que ésta implica.

7. Los resultados de la encuesta reflejan que, a la hora de implementar modelos de seguridad, las organizaciones usan algún estándar, hecho motivado más por las regulaciones que por una intención de proteger, lo que genera el debate nacional e internacional alrededor de tales asuntos. La meta de la protección organizacional no debe estar sujeta al cumplimiento.

En resumen, el panorama general de la seguridad en Colombia muestra cambios importantes y se mueve en la misma línea de las tendencias internacionales en los aspectos revisados. Se registran nuevos desafíos y una gran oportunidad para potenciar a las organizaciones, en procura de construir posturas de seguridad digital más confiables y resilientes, encaminadas a mejorar e impulsar su competitividad actual y futura.

Referencias

PwC, 2018. Global Information Security Survey. Recuperado de: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

EY, 2018. Global Information Security Survey 2018-19. Recuperado de: https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf

CISCO, 2019. Informe Anual de Seguridad. Recuperado de: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/cybersecurity-series-threat.pdf

ISACA, 2019. State of Cybersecurity Implications. Recuperado de: https://cybersecurity.isaca.org/state-of-cybersecurity

Verizon 2019. Data Breach Investigation Report. Recuperado de: https://enterprise.verizon.com/resources/reports/2019/2019-data-breach-investigations-report.pdf

Ponemon, IBM, 2019. The Cyber Resilient Organization. Recuperado de: https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them

Deloitte, 2019. The Future of Cyber Sphere 2019. Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-sphere.pdf

WEF, 2019 (World Economic Forum). The Global Risk Report 2019. Recuperado de: https://www.weforum.org/reports/the-global-risks-report-2019

CISCOb, 2019. Anticipating the Unknowns. Recuperado de: http://ebooks.cisco.com/story/anticipating-unknowns

CCO, 2018 (Champlain College Online). The State of the Cybersecurity Workforce and Higher Education. Recuperado de: https://www.champlain.edu/champlain-college-online/about-us/in-the-news/cybersecurity-survey-2018

PwC Luxemburgo, 2018. Out of the Shadow: CISO is in the spotlight!. Recuperado de: https://www.pwc.lu/en/digital-services/cyber-security/docs/pwc-ciso-survey-2018.pdf

Fortinet, 2019. The Ciso Ascends From Technologist To Strategic Business Enabler. Recuperado de: https://hub.fortinet.com/hiring-guides/the-ciso-ascends-from-technologist-to-strategic-business-enabler

IDC, 2019. The Modern Connected CISO. Recuperado de: https://www.capgemini.com/wp-content/uploads/2019/01/The-Modern-Connected-CISO.pdf

Kaspersky, 2019. What It Takes to Be a CISO: Success and Leadership in Corporate IT Security. Recuperado de: https://kas.pr/4sw6

PwCb, 2019. 22nd Annual Global CEO Survey. Recuperado de: https://www.pwc.com/gx/en/ceo-survey/2019/report/pwc-22nd-annual-global-ceo-survey.pdf

Tenable-Ponemon, 2019. Measuring & Managing the Cyber Risks to Business Operations. Recuperado de: https://www.tenable.com/cyber-exposure/ponemon-cyber-risk-report

Andrés R. Almanza J., Ms.C, CISM. *Coach Ejecutivo y Chief Growth Officer en CISOS.CLUB. Ingeniero de Sistemas y Computación de la Universidad Católica de Colombia. Especialista en Seguridad en Redes de la Universidad Católica de Colombia. Máster en Seguridad Informática, Ms.C, de la Universidad Oberta de Cataluña, España. Profesional certificado como Coach Ejecutivo y de Vida, por la International Coaching Leadership and Future Achivement. Profesional certificado como Information Security Manager (CISM), por ISACA. Docente de Cátedra de la Universidad Externado de Colombia. Miembro del Comité Editorial de la Revista "Sistemas" de la Asociación Colombiana de Ingenieros de Sistemas (ACIS).*

Ciberriesgo: visión convergente y reto sistémico

DOI: 10.29236/sistemas.n151a4

La revolución digital, Internet y las redes sociales han transformado la sociedad en su esencia y en dicho cambio está latente un espacio todavía desconocido, generador de incertidumbre y grandes retos.

Sara Gallardo M.

Hasta hace poco tiempo el riesgo presente en todos los sectores de la economía, se relacionaba con el impacto sufrido por la información, propiedad de los usuarios de servicios y de los empresarios proveedores. Se trataba de amenazas conocidas, a las que se podía aplicar una serie de controles para enfrentarlas y evitar implicaciones de gran envergadura.

Hoy en día, el denominado ciberriesgo, un riesgo categorizado como sistémico, producto de la conectividad del ser humano hasta en sus espacios más íntimos, ha precipitado en ellos temores y ambigüedades, porque se trata de un factor desconocido, incierto, entrelazado en una red de situaciones sin aparente control, que involucra lo tangible e intangible, las necesidades básicas de la humanidad y el entorno físico e inmaterial.

Es por eso que muchos profesionales de diferentes disciplinas es-

tán uniendo esfuerzos para hacer un frente común ante lo que varios expertos advierten como un nuevo desafío que reclama desde ya un ojo avizor y acciones tendientes a estar preparados para afrontarlo.

Por tales razones la tecnología no brilla sola ni independiente entre los bits y los bytes, ese ciberriesgo trascendió la combinación de los unos y los ceros para tocar lo humano en combinación con lo social, el exterior y el interior de las personas. Se trata de un hecho generador de caos, de incertidumbres y en el peor de los casos, extinción, cuando de negocios se trata.

De ahí que fuera escogido como tema central de esta edición de la revista que convocó distintas voces para conversar al respecto. A la cita acudieron: María Conchita Jaimes Gómez, partner Advisory Services en Ernst & Young S.A.S.; Jaime Eduardo Santos Mera, miembro de la Junta Directiva de Olimpia Management IT; Alberto León Lozano, coordinador en la Gerencia de Ciberseguridad y Ciberdefensa, área adscrita a la Vicepresidencia Digital de Ecopetrol; Gustavo Lozano Caballero, Corporate Sales Manager de O4IT y Diego Zuluaga Urrea, responsable de Seguridad de la Información en Isagen.

"Continuando en la línea de abordar temas de impacto para nuestros lectores, en esta oportunidad trataremos de entender el ciber-


María Conchita Jaimes G.


Jaime Eduardo Santos M.


Alberto León L.


Gustavo Lozano C.

riesgo y sus implicaciones, como una realidad sistémica, en busca de mejores argumentos y como un reto emergente para todo tipo de negocio", manifestó Jeimy J. Cano Martínez, director de la revista y moderador de la reunión, quien procedió a formular la primera pregunta.

¿Qué es el ciberriesgo?

María Conchita Jaimes Gómez
Partner Advisory Services
Ernst & Young S.A.S.

El ciberriesgo es aquel que se presenta en un espacio distinto al tradicional de trabajo, es decir, el ciberespacio producto de la conectividad digital soportada por Internet, transformadora del riesgo y que lo convierte en exponencial, considerando que asocia diferentes tecnologías digitales, redes sociales y distintos actores dentro de una conectividad globalizada. En tal sentido, el ciberriesgo requiere un manejo completamente diferente al tradicional. En este contexto, se habla de un concepto básico; la fórmula mágica de antes dejó de existir en términos de la probabilidad por impacto. Hoy en día, no sabemos cuál es la probabilidad del riesgo y se constituye en una diferencia muy importante.

Jaime Eduardo Santos Mera
Miembro Junta Directiva
Olimpia Management IT

Es como todo riesgo. Se trata de un factor de miedo que está de moda y todos los seres humanos tenemos miedo de perder el bienestar físico y emocional. Existe el temor de perder la identidad, de perder los datos, entre otros hechos generadores de miedo, lo que lleva a asumir un comportamiento de defensa. Pero, cuando nos ubicamos más en el entorno tecnológico, el ciberriesgo tiene otras implicaciones, toda vez que es un hecho sin historia, sin data para poder aplicar toda la estadística probabilística, lo que genera todavía más miedo y, más aún, cuando en muchos de estos hechos convergen, lo analógico y lo digital. Dichos riesgos generan más temor a los seres humanos y a las empresas, porque no se tiene

certeza sobre su manejo. Antes el riesgo se manejaba con un SAR (Sistema de Administración de Riesgos) y se le ponía un apellido, de crédito, de liquidez, de lavado de activos, entre otras posibilidades. Pero, el ciberriesgo no lo vamos a poder bautizar de la misma manera y va a implicar una creatividad e innovación para analizarlos.

Gustavo Lozano Caballero
Corporate Sales Manager
O4IT
El ciberriesgo es básicamente una amenaza que afecta aquellos sistemas de información con los que interactuamos; lo que no podemos manipular como la interacción automática entre los mismos sistemas. Es un hecho que toca el aspecto humano, no sólo lo tecnológico, sino cómo el usuario interactúa con la tecnología y cómo accede a la información. Por tal razón, no afecta solamente a las empresas, sino al usuario tradicional que tiene simplemente un teléfono inteligente. El ciberriesgo es entonces esa interacción entre lo humano y lo tecnológico. Amenazas presentes, en el marco de nuevas tecnologías emergentes, expuestas en ese entorno.

Alberto León Lozano
Coordinador en la Gerencia
Ciberseguridad y Ciberdefensa
Vicepresidencia Digital
Ecopetrol
El ciberriesgo es una sumatoria de muchos riesgos. Es un tipo de riesgo que involucra diferentes aspectos, tecnologías y realidades, además de todos los elementos de la sociedad actual, orientados por su convergencia. Esto conduce a un complejo de riesgos difíciles de comprender. Se integra una variedad de amenazas y vectores de riesgo que están en evolución: el ciberriesgo de hace cinco años no es el mismo que tenemos hoy y éste es seguramente diferente al que tendremos en tres años, debido a la amalgama de condiciones en la transformación que se está dando. Desde el punto de vista empresarial, el ciberriesgo es un riesgo estratégico

Diego Zuluaga Urrea
Responsable Seguridad de la Información
Isagen
(Envió sus opiniones)
Como se ha visto en los últimos tiempos, el ciberriesgo corresponde a los riesgos a los que nos vemos enfrentados cuando aceptamos ser parte de este nuevo entorno digital, en el que se ha desarrollado una sociedad completa, en donde existe una ciudadanía digital que, como la ciudadanía física, tiene tanto buenos como malos ciudadanos, con buenas y malas intenciones, quienes en algunas ocasiones buscan aprovecharse de los demás y obtener beneficios para sí mismos o sus grupos sociales, sin importarles las regulaciones ni las conductas éticas y moralmente aceptables por la sociedad. En ese sentido, los ciberataques, el fraude por medio informático, los delitos

informáticos, la ciberguerra, el ciberterrorismo se han circunscrito dentro de esta palabra que puede incluir además los riesgos de la pérdida de privacidad y de identidad digital en muchos escenarios.

Jeimy J. Cano M.
Moderador

En la discusión de la primera pregunta se observa inmerso el concepto de la complejidad, como esa capacidad para distinguir nuevas propuestas en el contexto volátil, incierto, complejo y ambiguo que tenemos en la actualidad. Otro aspecto relevante, es la convergencia entre lo humano, lo técnico y lo social, como una amalgama de situaciones y conocimientos que abren nuevas posibilidades. Es decir, no se habla de un asunto tecnológico únicamente, sino de una confluencia de dinámicas y realidades que evolucionan y se materializan de forma distinta. Si eso es así, este riesgo tiene una característica necesariamente sistémica, está conectado con todo y todo está conectado con él. ¿Por qué es un riesgo con tales características?

Alberto León L.
Precisamente, porque confluyen muchos componentes y de alguna manera la tecnología de la información y las comunicaciones; también por ser transversal a todas las actividades de la humanidad y a todos los procesos de las organizaciones. Las tecnologías de la información y las comunicaciones (TIC), sí son un factor generador para que exista afectación en todos los ámbitos relacionados con este riesgo. La forma en que ha ingresado en este ambiente, de manera convergente con otras tecnologías, determina su complejidad. Y eso lo hace sistémico, porque toca todos los diversos componentes. En diferentes reportes emitidos por entidades tales como el Foro Económico Mundial y el Instituto de Riesgos existenciales de la Universidad de Cambridge, aproximan el riesgo de ciberseguridad como riesgo empresarial, sistémico, cibernético. Claramente, si el riesgo es sistémico, las soluciones para tratarlo deben integrar y relacionar sus componentes, de igual forma sistémica.

Gustavo Lozano C.

El ciberriesgo es sistémico y esto no significa que en las organizaciones exista un área responsable o doliente de este tipo de riesgo; se trata de algo que nos toca a todos, que no tiene dueño. Todas las áreas deben aportarle a la mitigación o al control, a la calificación, categorización, probabilidad, a todos los números que se le puedan extraer para disminuir esa exposición presente en las empresas de hoy. Si existe un área de seguridad de la información, ésta debe ser transversal, de apoyo a todas las áreas. El ciberriesgo debe ser sistémico y divulgado en todos los niveles de la empresa. Se trata de un asunto que involucra desde la gerencia hasta los niveles más bajos de una organización, dentro de un mapa de decisiones enfocadas, basadas en datos, información, experiencias, visibilidad de lo que sucede en el exterior. La exposición es permanente.

Jaime Eduardo Santos M.

En la actualidad hablamos de riesgos sistémicos porque llevamos siglos en que la academia, las empresas, los Estados premiamos a los especialistas y en consecuencia el conocimiento se fraccionó. Por ejemplo, ir al médico se convirtió en que para una consulta son necesarias como mínimo tres citas con diferentes galenos, debido a las subespecialidades. De manera que los humanos con la limitación del cráneo para tener la caja de información, esta caja nos obligó a fraccionar el conocimiento por pedacitos para entender el problema. Cabe la comparación metafórica entre un elefante y una vaca que ambos se comen a mordiscos, para describir hoy el conocimiento. Esto obedece al etiquetamiento, en el sentido de que un abogado no puede hablar de tecnología, que un ingeniero no sabe escribir. De manera que, a través de los siglos, la educación ha venido convirtiéndose en método de castración para romper las interfases naturales o quizás de sentido común. La universidad se enfrenta a las necesidades de profesionales de acuerdo con el cargo que ofrecen las em-

presas. De ahí el problema tan grave al que se enfrenta la sociedad colombiana, existen seis mil vacantes para ingenieros de sistemas. En nuestra compañía tenemos experiencias de enfermeras que hacen excelentes trabajos en inteligencia artificial, toda vez que ésta está funcionando con las mismas limitaciones de los humanos. Uno escucha Watson cocina, Watson cáncer, entre otras posibilidades. Desde la misma conceptualización cuando vamos a atacar el tema sistémico, nos estamos olvidando que no podemos ver el problema si seguimos observándolo con dos ojos, dos orejas, una nariz y una boca. El asunto sistémico implica que todos nos podamos conectar; es decir, hacer una revolución conceptual del conocimiento, es una complejidad para mirarlo de otra manera y no bajo un lente particular de una especialidad.

María Conchita Jaimes G.

Desde mi perspectiva observo dos conceptos alrededor del tema. Uno desde la complejidad del ecosistema, en que la conectividad ha llevado a ampliar el escenario de riesgos. Hoy tenemos varios usuarios con distintas alternativas tecnológicas, utilizando una diversidad de dispositivos y canales para acceder a la información; a su vez, los procesos de negocio están interconectados con otros tipos de negocio y distintos actores en ese ambiente. Esto hace que el riesgo se vuelva sistémico; no estamos hablando de un riesgo estático, sino dinámico. Cuando nos referimos a estos temas, utilizo un ejemplo tan sencillo en el que un atacante entra a un computador A, va a uno B, obtiene información de éste y lo lleva al C; esta información es utilizada y enviada a otro, lo que quiere decir un riesgo dinámico, considerando la dimensión del ecosistema y es imposible determinar el movimiento del riesgo. Lo otro es que se hablaba de que los procesos de negocio de una compañía de consumo son distintos a los de una financiera. Pero, si se mira un poco más allá, los límites y fronteras de los sectores de negocio y de la industria se están rompiendo. Hoy hablamos, por ejemplo, de compañías de retail soportadas en lo digital, lo que ha producido cambios en la forma de hacer los negocios y por ende en las competencias de los seres humanos. En esa medida el entorno es distinto y los riesgos también. Pero no solamente lo digital hace que el riesgo sea exponencial; la diversificación del portafolio de productos y servicios está llevando a una complejidad mayor con impacto directo en la gestión de la ciberseguridad.

Diego Zuluaga U.

En mi concepto este riesgo es totalmente sistémico, porque al enmarcar todo el comportamiento digital, comprende los aspectos de este entorno hacia el cual ha migrado la vida de los ciudadanos, con comportamientos económicos, de interacción social, política y religiosa, entre otros; y cuando se mezcla

con sistemas ciberfísicos puede afectar la vida y los bienes de las personas. Cuando se piensa en este tipo de riesgos, las personas se ven afectadas en su vida cotidiana, las empresas en su reputación y economía, en la interacción con las comunidades y sus entornos o incluso en su producción y en los medios utilizados por los empleados para lograrla. Hoy el flujo de información en las empresas es como el sistema circulatorio de los humanos, cuando se interrumpe, modifica o se expone de maneras inadecuadas, sufren todos sus procesos, departamentos y áreas; lo mismo puede decirse incluso del funcionamiento de los Estados y de sus relaciones con los ciudadanos, así como de la prestación de los servicios esenciales, entre ellos las telecomunicaciones y de energía, que también pueden ser impactados por riesgos cibernéticos causando fallas sistémicas en todos los demás sectores económicos, afectando la gobernabilidad y el estado normal de la sociedad.

Jeimy J. Cano M.

Esta ronda fue interesante por dos razones: hemos sido entrenados en islas disciplinares en las cuales fueron cortadas las interfases con otras vistas del conocer y ahora el mundo advierte, que estas islas deben estar conectadas y cualquier hecho que se registre deberá ser tratado de esta forma. De manera que la exigencia del saber ahora es transdisciplinar. El ciberriesgo rompe fronteras, reta al ser humano, genera una ruptura que da lugar a la generación de aprendizaje. Un tercer elemento mencionado tiene que ver sobre cómo los riesgos tocan diferentes esferas para entender la dinámica del mundo de otra forma. Fuimos educados para hablar en islas y ahora éstas ya no existen. Cabe la frase de Edgar Morin "navegamos en un mar de incertidumbres, para encontrar algunos archipiélagos de certezas"[1]. Entonces, la siguiente pregunta es: ¿debe tener el ciberriesgo un tratamiento distinto a los riesgos tradicionales? ¿Por qué? ¿Cuáles son las razones? ¿Eso requiere otro tipo de formación?

Gustavo Lozano C.

Sobre las áreas de tecnología surge un área de gasto que los dueños solían considerar desde los permanentes pedidos que hacía. Hoy en día la opinión es diferente y la consideran un área de apoyo para tener en cuenta. Por ejemplo, existen nuevos bancos cien por ciento digitales, sin oficinas y sin papel, de manera que esto cambia el negocio. El nuevo contexto contempla un nuevo y desconocido riesgo, sin posibilidad de conocerlo para cuantificarlo. El riesgo es que mi competencia conocerá mis clientes, mis estados financieros y voy a quedar expuesto. En muchas organizaciones miran el riesgo desde la pérdida de dinero, pero hoy el riesgo hay

1 Morin, E. (2001) *Los siete saberes necesarios para la educación del futuro*. Barcelona, España: Paidós.

que mirarlo más allá del dinero, relacionado con la reputación, como un hecho no tradicional, al que se le debe tener mucho más en cuenta. De tal manera que se genera la necesidad de identificar nuevos riesgos asociados con la conexión hacia el mundo: las redes sociales, la comunicación e interacción de los empleados en torno a la información que se extrapola. Al integrar esos nuevos riesgos frente a la conectividad, sin importar la metodología, lo importante es saber que existen. No hay peor enemigo que lo que no se logra ver. La invisibilidad del riesgo es como la ceguera. Así que es necesario asumir otras posturas al respecto, además de crear conciencia del nuevo ambiente, la prevención que se debe asumir, para lo cual debe haber un entrenamiento, de manera de provocar la reacción ante el riesgo.

Alberto León L.

Desde el punto de vista sistémico y teniendo en cuenta que hemos sido educados hacia una gestión profesional por silos, el diseño de las organizaciones funciona bajo este mismo concepto. Es posible intentar el cambio de las personas, pero es muy difícil modificar las estructuras de las organizaciones. Muchos estudios se refieren a la dificultad que existe para romper los silos en las empresas. Independientemente del modelo de gestión de riesgos que se tenga, es vital asumirlos bajo la realidad actual, para integrar los procesos. En un riesgo sistémico, si la organización no lo gestiona desde esa óptica, será muy difícil poner en marcha cualquier metodología, tradicional o nueva. Así mismo, el riesgo hoy es exponencial, la industria 4.0 nos ha llevado a ser testigos del desarrollo exponencial de las últimas décadas y todo indica que se mantendrá esa tendencia en los años venideros, lo que producirá seguramente que la gestión del riesgo supere el pensamiento lineal. La visibilidad es otro aspecto a tener en cuenta. En resumen, asumir la gestión del riesgo implica proyectarnos hacia el entorno de años adelante, ni siquiera para actualizar los modelos, sino para permanecer un paso adelante, porque se trata de una batalla en la que

el atacante es distinto, invisible, impredecible y tiene mayor movilidad. La aproximación al ciberriesgo debe llevarnos necesariamente hacia la resiliencia.

María Conchita Jaimes G.
El tratamiento del riesgo está directamente relacionado con el control, pero el inventario que existía al respecto, no puede ser el mismo. Es necesario archivarlo para pensar en forma diferente. Si el tema es exponencial los controles tradicionales desaparecen, no funcionan. Antes se establecía un control central, pero hoy cuando se tienen dos y mil y más personas conectadas desde un celular y éste con acceso a los sistemas de información, la situación es otra. De manera que el concepto de control cambia. Se debe dar un tratamiento preventivo a través de los dispositivos de acceso y un enfoque fuerte alrededor de la cultura de las personas. Esto en lo que se refiere al tratamiento. Sobre las competencias existe un asunto que cada vez toma más fuerza de cara a los riesgos, las cuales también se modifican y tienen que ver con la analítica. Quienes trabajamos en el entendimiento de los riesgos, tenemos que entender los datos generados en todos los sistemas y automatizar la gestión del riesgo. Otro asunto también muy importante está relacionado con las regulaciones en el manejo de la información, de las leyes que la cobijan. Es necesario que los profesionales de la seguridad estén capacitados al respecto.

Jeimy J. Cano M.
¿Estamos entrando entonces a un nuevo analfabetismo de los datos? ¿Se trata de un nuevo insumo que debe contemplar el perfil del profesional de la seguridad?

María Conchita Jaimes G.
Exactamente, de eso se trata, es necesario saber cómo interpretar la serie de eventos generados alrededor de los dispositivos digitales. Hoy en día una compañía con dispositivos digitales y todo tipo de información circulante ¿con qué capacidad cuenta para su manejo? ¿cómo controla ese mundo tan dinámico? Es necesario tener en cuenta cómo se van a integrar los distintos sistemas. Y esto, por supuesto, está relacionado con los riesgos, si no se conocen no se sabe cómo tratarlos. Es necesario interpretarlos y una alternativa para ello es la analítica. En resumen, las competencias hay que aumentarlas porque el nuevo entorno así lo exige.

Jaime Eduardo Santos M.
Los riesgos emergentes entre los que está el ciberriesgo deben ser tratados con las mismas armas del atacante y ese es el problema actual, no las tenemos o no las usamos. Seguimos con controles de frecuencia e impacto, líneas de defensa, anillos de seguridad para los riesgos probabilísticos, pero no para los emergentes. Eso no funciona. El tratamiento debe ser completamente distinto. En el caso, por ejemplo, de *blockchain*, es nece-

sario ubicar los controles, en igualdad de armas. Y para ello, el conocimiento de las personas debe ser también distinto. En ese sentido, para mí llegó el momento de los científicos puros, de los doctores, porque el mundo viene siendo de los especialistas. Ahora con aspecto exponencial, vamos a tener que hablar es del informe del cambio climático de Naciones Unidas que produjo el análisis de todos los aspectos relacionados con el tema, de donde sale la idea de que nos vamos a volver inmortales. De manera que, al trabajar en una compañía de seguros, por ejemplo, no se trata de identificar un riesgo ni nada por ese estilo, sino de mirar el momento en que los seres humanos seamos inmortales. Es el momento de las ciencias puras para escuchar a quienes no escuchamos, personajes que infortunadamente no hay muchos en nuestro país. Estamos escasos de doctores y de grupos de investigación. Es necesario que encontremos herramientas para que abogados, filósofos y biólogos sepan de qué están hablando. No pueden seguir funcionando los metalenguajes de cada profesión. Es el momento de las ciencias y en ellas de la lingüística y ésta dentro del mundo computacional ya existía y ellos encontraron la manera de comunicarse, a través de lenguajes universales. Uno de estos utilizado en la industria computacional es la lectura distante que solamente la puede hacer una máquina y no un humano. Si a través de ésta podemos entrenar un robot que puede hacer lectura de todos los libros escritos por la humanidad y nos indica, por ejemplo, en cuáles se ha escrito la palabra 'amor', y la va a correlacionar y ponderar, pues es el momento de apreciar a los lingüistas, a los filósofos, antropólogos, a los biólogos, astrónomos, y físicos y a todos los profesionales con esas miradas, para abrirles espacio en las organizaciones. Por ejemplo, un astrofísico tiene mayor entendimiento de la data, porque maneja millares de datos en su computador y en su cabeza. Un profesional puede ser muy experto en riesgo en el entorno de un banco, pero se queda corto frente a un astrofísico. Mi invitación también es a abrir los espacios para las ciencias puras que nos ayuden a recuperar las interfases que nos quitaron, en procura de un lenguaje común para advertir con anticipación los problemas venideros en la humanidad digital.

Diego Zuluaga U.

Cada vez más, el riesgo cibernético es considerado dentro de los riesgos más importantes para las empresas y las naciones; el Foro Económico Mundial, lleva más de cinco años mostrándolo dentro de los cinco riesgos más importantes del mundo. El año pasado, temas como el fraude digital y los ciberataques ocuparon los primeros lugares, sólo superados por los desastres que pueden causar la naturaleza y el cambio climático. En mi concepto es un riesgo que se debe tratar de manera similar a los demás

riesgos, asumiéndolos, tratándolos o transfiriéndolos, pero entendiendo en forma adecuada sus particularidades y que las vulnerabilidades –en muchos casos intrínsecas- se pueden administrar, pero en las amenazas hay que tener en cuenta que provienen de fuentes antes no analizadas, porque se veían muy lejos de la realidad y con las nuevas tecnologías están más cerca de lo que la misma geografía permite. Esto es muy importante en el cibercrimen organizado internacionalmente y en las guerras cibernéticas que no se dan con los vecinos inmediatos, sino con cualquiera en el globo, debido a que en la actualidad estamos a menos de 100 milisegundos de cualquier parte del mundo. Las medidas de control sí son altamente especializadas y requieren medidas preventivas, detectivas y correctivas, para considerar el entorno actual integrando capacidades de prevención atención, respuesta y resiliencia ante eventos cibernéticos, desde la cultura de las personas, los procesos y la tecnología que los soporta.

Jeimy J. Cano M.

Es muy interesante ver que la reflexión aquí muestra la entrada en una era de analfabetismo de datos, que ya no es un asunto informático, sino de los datos y su interpretación, de ahí que valga la pena citar la siguiente definición : "Es el producto que resulta de la evaluación, la integración, el análisis y la interpretación de la información"[2], disciplina que se llama inteligencia. Y cuando se habla de ciberriesgos se trata de producir no prácticas, sino capacidades. Aspecto muy importante para tener en cuenta, como producto de las reflexiones hasta el momento expuestas.

Jaime Eduardo Santos M.

En el curso sobre la Cuarta Revolución Industrial en la universidad Nacional tenemos un psicólogo, un ingeniero, un abogado y casi que la mitad de la clase la dedicamos a

2 Jiménez, F. (2019) *Manual de inteligencia y contrainteligencia*. Tercera Edición. Campus Internacional para la Seguridad y la Defensa. Sevilla, España: CISDE Editorial

analizar la forma sobre cómo aprendemos los humanos para después empezar a hablar sobre tecnología.

Jeimy J. Cano M.
¿Qué hacer con ISO 31000? ¿Responde a lo que estamos hablando sobre el ciberriesgo? ¿Qué opinan al respecto?

Alberto León L.
Mi respuesta es que sí. El ciclo básico que propone ISO 31000 está replicado en todas las nuevas prácticas: establecer un contexto y desarrollar la identificación, valoración, tratamiento, monitoreo y en el corazón de este ciclo, gestionar la comunicación con las partes interesadas. Considero que exige transformación en la profundidad en cada una de estas fases. Primero, es necesario disponer de un contexto con claros niveles de apetito y tolerancia al riesgo, establecidos y ampliados. Se debe hacer conciencia sobre el riesgo sistémico y asegurar la elasticidad y agilidad en los ciclos de gestión del riesgo, dado que las velocidades y complejidad en el entorno del riesgo se han incrementado. A raíz de la pregunta es necesario reflexionar sobre los cambios que se deben introducir a estos modelos.

María Conchita Jaimes G.
En torno a las buenas prácticas ¿cuáles se pueden asumir frente al ciberriesgo? El punto es el enfoque en el riesgo residual, no se pueden omitir los controles asociados a cada tecnología, esto debe ser una práctica generalizada que no puede pasar por alto. Entendido esto, el riesgo remanente es el foco, aquél que debe ser gestionado y en el que permanecen vigentes las buenas prácticas de tratamiento de los ciberriesgos. Las buenas prácticas siempre aportarán a la gestión del riesgo, entre éstas la ISO 31000.

Jeimy J. Cano M.
¿Esto quiere decir que el tratamiento de un riesgo sistémico se hace a través de una herramienta sistemática construida desde saberes disciplinares? Entonces ¿siento que forzamos algo que es por definición sistemático para tratar un asunto sistémico?

María Conchita Jaimes G.
Amplío la explicación mediante el ejemplo anterior, con mil personas utilizando otro tanto de servicios, redes, etc., hay una parte de control a través de los mecanismos tecnológicos para tratar el riesgo de manera acorde con los dispositivos. Se debe examinar la forma de hacerlo con cultura, hasta ahí no hay cambio. Pero, queda un riesgo remanente que se genera en tantos dispositivos, redes y fuentes y es muy difícil de tratar por ser exponencial y entra en juego la analítica. Se trata de un riesgo diferente. En otras palabras, consiste en determinar cómo interpreto la información asociada a los riesgos residuales para poder tratarlos de forma complementaria.

Jaime Eduardo Santos M.
Mi camino es otro. La ISO 31000 en mi opinión ya no sirve, ni ninguna de las ISO, porque así me lo ha mostrado el mundo real, muchas formas, códigos, políticas que el día del problema no soportan las decisiones hacia adelante. Desde hace 20 años gestiono crisis y lo residual se convirtió fue en eso, en crisis. Cuando tengo el problema a resolver el equipo interdisciplinario debe ser capaz de gestionar ese entorno con casi ninguna información. Es necesario tener en las corporaciones expertos en gestión de crisis, con diversas competencias neurofisiológicas, basales y frontales. Y para ir hacia adelante me cambié a manejar el concepto de riesgos emergentes de la humanidad; para lo cual me introduzco en un mapa más grande alrededor de las correlaciones con la tecnología, observo ese posible ambiente de cara a la humanidad. A manera de ejemplo, cambio climático, indignación social y activismo judicial. De manera que cuando entro en ese marco más grande, los ciberriesgos se convierten en una rama de ese árbol y empiezo a utilizar herramientas para su tratamiento, con científicos, con nuevas herramientas tecnológicas. Es claro que, así como la humanidad destruye el planeta, también puede repararlo. Es necesario aceptar la necesidad de aprender de otros y colaborar con otros. Insisto en que mi camino está orientado al poder de la gestión de crisis en colaboración con el ecosistema empresarial porque los riesgos son exponenciales. La palabra ya ni siquiera es controlar.

Gustavo Lozano C.
No existe un estándar, una norma o unas mejores prácticas que logren cubrir todo el concepto del riesgo. Lo que deben hacer las empresas es primero entender su negocio para determinar cuál de todas esas tecnologías emergentes deben aplicar. Y otras entidades como las financieras obligadas a implementar ISOS, pues deben estar en actitud de alerta, porque se van a archivar procesos, documentos y una cantidad de papel, sólo por cumplir, por exigencia de la ley y eso no es así. Si no se cambia la manera de entender el nuevo ambiente, las empresas quedarán estáticas. La tecnología avanza mucho más rápido que los estándares a imponer en las organizaciones.

Jeimy J. Cano M.
El ciberriesgo lo que plantea es una tensión en sí mismo en la gestión de los riesgos. Hay unos trasfondos muy interesantes, no sólo de la práctica, sino de capacidades. En ese sentido ¿se conocen a la fecha buenas prácticas en el tratamiento de los ciberriesgos? Si existen, ¿qué temáticas y retos contemplan? Si no, ¿cómo asumir los retos de su tratamiento?

María Conchita Jaimes G.
Tenemos que trabajar con compañías de tecnología, con abogados y otros profesionales para no quedarnos cortos, en aras de prestar

un servicio de calidad. Para entender todo lo que sucede alrededor del ciberriesgo es necesario comprender que no es posible atenderlos con la metodología tradicional, sino es necesario romper fronteras. Hoy en día no se trata de una sola tecnología, sino de varias. Por ejemplo, la presencia de un robot. De manera que no es posible pensar en auditorías ni procedimientos tradicionales. El tratamiento requiere de nuevas competencias y como éstas en su totalidad no están en todas las profesiones, es necesario crear un ecosistema propio para el servicio proporcionado. Es decir, cómo se rompe la caja en que nos movemos con el aporte de las distintas profesiones en la prestación de un servicio.

Jaime Eduardo Santos M.

Claramente no existen mejores prácticas porque no es posible. Entonces esa posibilidad tampoco funciona. Surge un concepto denominado de las cinco hélices de la sostenibilidad, en procura de que la humanidad sea sostenible, porque el reto que estamos viviendo contempla los límites de lo humano y lo tecnológico, lo tecnológico-humano y estos dos conjuntos se están juntando y en el momento en que tal hecho se presente, surge la singularidad. Y si esto es una realidad, sea una posición ética o política, hasta dónde vamos a permitir que un punto quede completamente interceptado con el otro. Los que creemos en la humanidad y que la tecnología es una herramienta para mejorarla y no para sustituirla, tenemos que poner elementos para la sostenibilidad de la humanidad, que sólo se logra combinando muchas fuerzas. Así que la teoría de las cinco hélices es muy importante: Estados, empresas, academia, comunidad y el medio ambiente. Entre esos cinco elementos que nos permiten comportarnos como humanos, tenemos que promover el movimiento de esa hélice.

Gustavo Lozano C.

No existen soluciones genéricas que las organizaciones puedan poner en marcha. Así como el ciberriesgo es un universo, cada empresa también lo es, todas manejan tecnologías distintas y organizan su información y datos también en forma diferente. Existen buenas prácticas vigentes, pero lo más importante es que debe haber un excelente entendimiento de los responsables en las organizaciones para liderar, controlar o mitigar esos ciberriesgos. A partir del conocimiento, entendimiento y la forma de interactuar con el mundo, sería posible determinar unas prácticas propias del negocio para funcionar. Se trata de tomar de todas las posibilidades para aplicarlo en el negocio particular. Es un tema más de conciencia hacia el interior antes de salir a buscar alternativas para convivir con el ciberriesgo.

Alberto León L.

Si consideramos que el ciberriesgo es exponencial y está evolucionando, que es sistémico, las prácti-

cas deben seguir una transición similar. En esa tensión entre el pensamiento lineal y la realidad curva exponencial, ya pasamos el punto de inflexión. Es necesario encontrar un modelo disruptivo para gestionar el ciberriesgo. Ya estamos en ese vacío que debe compensarse y ese ecosistema debe evolucionar y reaccionar. Los modelos sistemáticos que son los de gestión tienen que desarrollar en sus componentes la visión sistémica. Si se habla de contexto y de identificación debe procurarse que estos sean sistémicos. Se trata de establecer en la gestión de tratamiento de los riesgos unas capacidades cada vez más inmersas en la gestión de la empresa. Esa asimetría en que los atacantes están incorporando capacidades digitales, exige que los responsables de la gestión de riesgo deban incluir iguales o superiores capacidades, tales como inteligencia artificial y analítica para gestionar la identificación, claridad y visibilidad de los riesgos. Se debe contar también con herramientas de *machine learning* y aprendizaje para poder entender y enfocar el tratamiento. Estas capacidades se potencian dramáticamente cuando se trabajan en sinergia con otros actores.

Diego Zuluaga U.

En el momento actual existen muchas técnicas de control y posibilidades de transferencia de la parte económica del ciberriesgo a pólizas de seguro especializadas que entienden muchas de las características del mismo; aunque aún hay muchos retos importantes por desarrollar como muchos aspectos de impacto de los sistemas ciberfisicos en la sociedad y los impactos de los ataques cibernéticos, toda vez que no hay suficientes eventos para determinar el tamaño de los impactos y es un área de rápido crecimiento, en la que veremos mucho desarrollo en los próximos años con el aumento de Internet de las cosas, los vehículos autónomos, la digitalización de las empresas, la robótica y la automatización de procesos a gran escala. En este sentido, las empresas y la sociedad en general deben analizar la complejidad de los riesgos que están detrás de cada elemento que involucramos en nuestra vida digital, cada vez que ingresamos tecnologías digitales a nuestros procesos y entornos. Por ejemplo, es necesario un análisis adecuado de riesgos para identificar todas las vertientes de los mismos, desde los puntos de vista alrededor de lo regulatorio, tecnológico, reputacional, social, ambiental y de impacto potencial sobre las vidas humanas; hacerlo es fundamental cuando nos enfrentamos a nuevas tecnologías que ingresan al entorno.

Jeimy J. Cano M.

Si se revisa cómo surgieron estos estándares hace más de cuarenta años, lo que se pone de manifiesto es nuestra visión eminentemente mecánica del mundo. La invitación que surge de este conversatorio es mirar el mundo de una manera co-

nectada y holística. Quienes se resistan a esta transformación, harán que el modelo colapse.

Jaime Eduardo Santos M.
Muchas cosas están sustentadas en criptografía. En marzo del 2017 tuve la oportunidad de informarme sobre cómo la computación cuántica acaba con la criptografía. Entonces ¿cómo será el funcionamiento de los bancos y empresas? ¿De qué manera funcionará la ISO 31000? Nos tocó manejar la crisis causada por los riesgos emergentes y convergentes.

Alberto León L.
En mi opinión, lo que cambia es la tecnología, pero se mantiene el ciclo de identificación, valoración, tratamiento del riesgo. Profundizando en prácticas sobre gobierno de tecnologías emergentes, por ejemplo, la universidad estatal de Arizona, el Instituto de Riesgos Existenciales de la Universidad de Cambridge, el Instituto para el Gobierno de Riesgos Emergentes, el Foro Económico Mundial refieren modelos que se basan en este ciclo y se orientan hacia la prevención y a la resiliencia. Revisando los artículos que se refieren a los riesgos emergentes, encontramos que no se detienen sólo en los riesgos evidentes, sino que abordan aproximaciones hacia los elementos desconocidos y esto se aplica en la identificación del riesgo; en otras palabras, en propiciar la visibilidad. Es imposible gestionar un riesgo no conocido, no identificado, porque sencillamente se hace caso omiso o se ignora.

María Conchita Jaimes G.
La gestión del riesgo tiene que ser asumida de una forma diferente, no necesariamente a partir de las personas responsables de dicha labor. Esto hace que el sistema se abra y genere competencias. Por ejemplo, en la época en que apareció el correo electrónico, en la compañía existía el control para que las cartas

salieran firmadas por un número limitado de personas. Con dicha aparición y mil empleados ¿cómo se controla el uso de mensajes por fuera de la organización? Me refiero sólo a un aspecto que era manejado a través de cultura, políticas y regulaciones que ayudaban a mitigar los riesgos. Hoy son más elementos los que se deben tener en cuenta. Existen principios fundamentales como la disciplina, o los de gobierno que ayudan a mitigar los riesgos por muy exponenciales que sean; esa es una base, que deberá ser complementada con otros temas.

Jeimy J. Cano M.

¿Las compañías saben a qué se están enfrentando? Es necesario abordar el ciberriesgo desde ya, y es necesario comenzar a reflexionar al respecto. En ese contexto, ¿cómo transmitir ese riesgo a los directivos de las organizaciones?, ¿cómo deben asumir las juntas directivas los retos que imponen los ciberriesgos a las empresas con vocación digital?

María Conchita Jaimes G.

Por lo general, las juntas directivas de las compañías han visto su negocio y lo controlan para que éste produzca resultados. La junta directiva orienta los resultados de la organización, los cuales provenían de las acciones internas. Pero hoy, existen factores internos que le están llegando desde afuera e impactando sus resultados, entorno para el que no se han preparado con nuevas competencias. Esto forma parte de lo cibernético, los cambios digitales y demás. En tal sentido, existen dos puntos fundamentales qué abordar. Uno es, romper la barrera del conocimiento, entender qué es el ciberriesgo, no es posible continuar creyendo que el negocio depende de los procesos internos y que los controles son suficientes, cuando existen factores externos que impactan los resultados. El segundo punto tiene que ver con que los responsables de la seguridad de la información tenemos que aprender a cuantificar los riesgos y su impacto en la empresa. Entonces, debe existir una clara comunicación entre el mundo tecnológico y digital y la junta directiva, para ayudarles a asumir los ciberriesgos de una manera más tangible. Para resumir, se requiere: conocimiento de los factores externos que afectan los resultados de la organización, una comunicación clara de los responsables de la seguridad con la junta directiva, mediante la cuantificación de los riesgos, además de una alfabetización digital a la junta directiva.

Jaime Eduardo Santos M.

Con base en mi participación en varias juntas directivas y, en particular en la presidencia de una, mi actuar lo encaminé a la necesidad de que todos los miembros de junta deben asistir anualmente a las ferias de tecnología alrededor del mundo. Me aburrí de las capacitaciones, de invitar distintos conferencistas dentro de unos procesos de capacita-

ción que no producían efectos positivos. A manera de ejemplo, a la feria de tecnología de Hannover, a la de Barcelona, a la de ciudades inteligentes de Taiwan, de manera que todos los miembros de la junta hicieron un barrido en esa dirección. El impacto ha sido enorme y advierten que no tenían ni idea a qué estaban enfrentados. En esos entornos no ven el riesgo como la amenaza de la pérdida de datos u otras posibilidades, sino palpan la posibilidad de que el negocio desaparezca, que se acabe. Los miembros de junta han reconocido que la viabilidad del negocio local perdurará, hasta cuando el subdesarrollo lo proteja. Luego de esto el negocio no tendrá sentido. Y cuando ellos van a las ferias alternativas se dan verdadera cuenta de lo que ya se les había explicado a través de la teoría, porque en ellas no reciben nada de academia, ni de teoría. Van acompañados de una persona del equipo de tecnología para aclarar asuntos sobre lo que están viendo. En dichas ferias alternativas se encuentran con opciones para crear negocio en Colombia, porque se encuentran con jóvenes buscando posibilidades de negocio y de hacer dinero consiguiendo inversionistas. En esa dirección estamos en el proceso de convencer a los miembros de otras juntas directivas.

Alberto León L.

Parto de considerar que el ciberriesgo es un riesgo estratégico, existencial que está siendo abordado en las juntas directivas, entendiendo que es un riesgo sistémico que afecta la viabilidad de la organización. El Foro Económico Mundial acaba de publicar un documento sobre cómo se gestiona la resiliencia digital, en la industria eléctrica y propone un modelo sistémico porque se refiere al ecosistema, de ahí su nombre. “Ciberresiliencia en el ecosistema de energía eléctrica”, dirigido a las juntas directivas. Pasa por una visión sistémica, de integración entre la convergencia tecnológica para llegar a una serie de preguntas orientadas a los miembros de juntas directivas alrededor de la preparación sobre la resiliencia. De manera que contempla cuatro conceptos: continuidad, agilidad, confidencialidad y confiabilidad, asuntos claves para los directivos del negocio. Un escenario de interés para los miembros de las juntas directivas podrían ser los juegos olímpicos de Tokio, en el año 2020, en los que se podrá apreciar el despliegue tecnológico para el tratamiento del ciberriesgo mediante un enfoque ecosistémico.

Gustavo Lozano C.

Las empresas deberán tener vocación digital para existir. Los seres humanos aprendemos en tres dimensiones, viviendo y experimentando. Hasta que los hechos no suceden no los asimilamos y en este entorno es muy recurrente la resistencia por parte de las juntas directivas para adquirir soluciones de protección. El mensaje es que no basta con capacitar técnicamente a un equipo, si no se cuenta con el

apoyo de la gerencia, ellos deben experimentar, vivir las distintas situaciones, para asumir conciencia por sí mismos. El ciberriesgo también debe ser tratado e implementado dentro del plan estratégico de la organización, para que la toma de decisiones contemple la mitigación de tales riesgos e ir más allá de la adquisición de las últimas tecnologías, sin evaluarlas en el marco del propio negocio. Es necesario considerar la existencia del ciberriesgo.

Diego Zuluaga A.
Las empresas que han visto la digitalización como un factor transformador deben estar guiadas por la innovación y las capacidades de transformación, pero a su vez deben estar preparadas para identificar, evaluar y tratar adecuadamente los ciberriesgos. Es por ello que las juntas directivas deben liderar esta tarea, incorporando dentro de sus agendas la revisión de las estrategias de gestión del ciberriesgo y en sus miembros las capacidades para entender el nuevo entorno digital desde sus bondades, sus retos y riesgos. Deben asesorarse y asegurarse de que las evaluaciones de riesgo fueron hechas en forma adecuada y que contemplan todas las dimensiones a las que se está enfrentando la organización; deben preguntarse por ejemplo: ¿a qué posibles consecuencias jurídicas y demandas nos enfrentaremos, si la información de nuestros clientes y proveedores se filtra?, ¿existen riesgos derivados de un ciberataque a esta tecnología que estamos incorporando?, ¿podría afectarse la producción de la compañía si un actor malintencionado logra cambiar las configuraciones de los equipos que se están adquiriendo?, ¿cuál sería el alcance de esta afectación?, ¿está limitada al mundo digital?, ¿puede afectar la maquinaría?, ¿a las personas que estén cerca?, ¿al medio ambiente? Interrogantes sobre los controles y su efectividad deben estar acompañando estas preguntas, así sobre cómo se responderá en caso de que los riesgos se materialicen y cuáles son los mecanismos para regresar un entorno de operaciones que garantice la continuidad del negocio y la rápida recuperación de los procesos críticos, así como el retorno a la operación normal luego de la materialización del evento de ciberriesgo. También se deben considerar las alternativas para transferir el riesgo a terceros especializados en su gestión y la parte económica a pólizas de seguro como apoyo en la recuperación y cubrimiento de las pérdidas, reparaciones, lucro cesante, gastos jurídicos y gastos por responsabilidad civil que puedan presentarse. Estas y otras consideraciones claves deben estar en la mente de los miembros de la junta directiva y deben estar resueltas antes de aceptar cambios relevantes al entorno operativo.

Jeimy J. Cano M.
Les pido algunas reflexiones finales alrededor de lo aquí conversa-

do. ¿Cuáles son las tres recomendaciones que ustedes darían a nuestros lectores?

Gustavo Lozano C.
Considerando que el ciberriesgo es un tema universal, tenemos que entrar en la cultura de la transferencia de conocimiento para poder alimentarnos entre todos frente a tales asuntos. Educar a todas aquellas personas que interactúan con la información de las organizaciones. Y, dentro de ese escenario, lograr una comunicación asertiva al respecto. En otras palabras, crear conciencia. También tener visibilidad de los riesgos, conocer los puntos débiles y fuertes. Saber sobre todas las alternativas existentes para mitigar el ciberriesgo, para poder aplicarlas en la organización.

Jaime Eduardo Santos M.
El ciberriesgo es un asunto que concierne a toda la humanidad, relacionado con su supervivencia.

María Conchita Jaimes G.
El ciberriesgo es una responsabilidad de todos, no sólo de los profesionales de la tecnología. Invito a pensar desde afuera hacia adentro, toda vez que desde el exterior vienen los asuntos que impactan a las organizaciones. Así mismo, considerar lo que no se alcanza a ver, mediante un pensamiento más amplio.

Alberto León L.
Recomiendo una aproximación al ciberriesgo con una visión estratégica desde el punto de vista existencial, en la medida en que toca los objetivos y viabilidad de cualquier organización. La visión debe ser sistémica, exponencial y relacionada con el ecosistema. Otra recomendación es actuar de manera inmediata con lo que tenemos, mientras se incorporan capacidades digitales, y actuando de forma colaborativa con organizaciones pares y autoridades.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión empresarial y Acuc Noticias. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista Infochannel de México; de los diarios La Prensa de Panamá y La Prensa Gráfica de El Salvador y corresponsal de la revista IN de Lanchile e investigadora en publicaciones culturales. Se ha desempeñado también como gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res) y editora de Alfaomega Colombiana S.A.; es editora de esta revista.*

Ciberriesgo

DOI: 10.29236/sistemas.n151a5

Aprendizaje de un riesgo sistémico, emergente y disruptivo.

Resumen

En una sociedad digitalmente modificada como la actual, el aumento de la conectividad da lugar a la aparición de un nuevo tipo de riesgos denominados ciberriesgos o riesgos cibernéticos, los cuales surgen de la convergencia tecnológica entre el mundo físico y el lógico, apalancada por la densidad digital que lo rodea, es decir, de las nuevas conexiones e interfases que generan datos sobre la condición particular del objeto. Estos riesgos, en su naturaleza diferentes a los tecnológicos, establecen un nuevo paradigma de gestión, que demanda una vista interdisciplinar y sistémica para comprender los retos de las tensiones a las cuales se ven sometidas las organizaciones en un escenario global. En consecuencia, este artículo plantea algunas reflexiones conceptuales y prácticas que permitan retar y desconectar algunos saberes previos sobre la gestión de riesgos y explorar nuevas apuestas de comprensión y análisis en escenario volátil, incierto, complejo y ambiguo.

Palabras clave

Ciberriesgo, pensamiento sistémico, interdisciplinar, emergente, disruptivo

Jeimy J. Cano M.

Introducción

La evolución acelerada de la tecnología, los cambios e implicaciones geopolíticas actuales y la insistente demanda de las personas por experiencias cada vez más novedosas y personalizadas, establece un escenario inestable para las organizaciones y la sociedad, que exige reconocer la convergencia de diferentes campos de conocimiento, sus distintas posturas disciplinares y la incorporación de tecnologías emergentes, con el fin de encontrar formas inéditas que desconecten y

reten lo conocido, identifiquen relaciones poco visibles y creen nuevos vínculos entre objetos y las ideas para cambiar el *status quo* vigente.

Esta nueva realidad, más allá de superar las diferentes perspectivas de las disciplinas tradicionales, establece retos para los profesionales en todas las áreas, como quiera que su visión del contexto ahora responde a múltiples relaciones entre los objetos, para tratar de encontrar certezas en medio de las volatilidades propias de las condiciones actuales. Lo anterior, revela comportamientos del entorno que se manifiestan como rarezas, inconsistencias y contradicciones (Charan, 2015), las cuales deben ser identificadas y leídas, como insumo para avanzar y proponer alternativas que hagan del "incierto", una oportunidad para crear incentivos y motivaciones, que quiebren el estándar actual y revelen aquello que no era posible ver previamente.

Por lo anterior, el nuevo contexto digital en el que los objetos son cada vez más digitalmente densos (Zamora, 2017), configura una vista sistémica tanto de los negocios como de la sociedad. La conectividad como habilitador de nuevas formas de encuentro, como facilitador de novedosos flujos de información y la conexión entre mundos u objetos antes aislados, funda una mirada enriquecida de la dinámica global actual, que cuestiona la manera mecanicista y determinista de entender el mundo. Este paradigma sistémico, reconoce en la complejidad, entendida como esa capacidad del observador para distinguir características de los objetos del mundo y sus interacciones, una oportunidad para cambiar las estructuras existentes y las relaciones con su entorno, como un vehículo para "ver" y "darse cuenta" que es posible desafiar y cambiar las reglas.

Por consiguiente, al desarrollar nuevas propuestas disruptivas, generalmente basadas en iniciativas digitales, se introducen distinciones que tensionan el estado del arte de la técnica y la práctica en los diferentes negocios, configurando experiencias inéditas que capturan la atención de los clientes, pero al mismo tiempo, desarrollan zonas de incertidumbre, ambigüedad y complejidad, que pueden crear situaciones o eventos en los que se ponen en juego las expectativas y necesidades humanas, y cuyos resultados son aún desconocidos.

En consecuencia, explorar y analizar el ciberriesgo o riesgo cibernético, como esa nueva gama emergente de riesgos en las organizaciones, abre un ámbito de participación activa de los diferentes actores empresariales, no sólo para aceptar, mitigar o transferir la gestión de su tratamiento, sino para configurar una visión pedagógica corporativa que prepare la corporación para entender, aprender y

responder a los retos de la inevitabilidad de la falla y así mismo, anticipe las acciones necesarias y suficientes para dar cuenta de los estados de incertidumbre que implica estar inmersos en un mundo digitalmente modificado.

Luego, desde una lectura sistémica, este artículo plantea la emergencia de un nuevo tipo de riesgo en un contexto digital, como lo es el ciberriesgo, que busca ilustrar cómo las situaciones inciertas y volátiles se convierten en oportunidades y retos para comprender las inestabilidades de las nuevas relaciones generadas por la convergencia tecnológica, y responder a las amenazas emergentes que nacen de los intereses encontrados de los distintos actores participantes de la dinámica social y digital.

Perspectiva sistémica del ciberriesgo: aumento de la densidad digital

Para comprender la nueva realidad del ciberriesgo, es necesario reconocer que tenemos un incremento de la conectividad en los objetos físicos, generando datos sobre la condición del mismo, los cuales son transmitidos a sistemas conocidos en las organizaciones, como también a infraestructuras en la nube, en donde cada vez más se pierde su control.

Este incremento de interfases en los objetos físicos, introduce el concepto de densidad digital (Zamora, 2017), como una propuesta inédita hacia nuevas experiencias de las personas con los objetos de la realidad, de tal manera que es posible una mayor conectividad e información en tiempo real, que puede ser (y será) utilizada para superar las expectativas de los clientes. Esta nueva condición de objetos "inteligentes" revela originales propuestas de valor que las organizaciones están dispuestas a explorar y explotar para crear nuevos activos digitales (Porter & Heppelmann, 2014).

Al incrementarse la conectividad y la caracterización de novedosos objetos o dispositivos inteligentes, se define un nuevo tejido de conexiones en el marco de relaciones conocidas y desconocidas que transforman la manera de hacer las cosas y, que terminan cambiando la realidad de los clientes. En este sentido, si bien se habilitan espacios para lograr experiencias distintas, de igual forma se configuran posibilidades que pueden motivar usos no autorizados, como quiera que es la información personal la que ahora se moviliza en estas nuevas interfases.

En perspectiva sistémica de la construcción social, podemos indicar como anota Luhmann (1998), que el sujeto deja de ser el centro del análisis, para centrarse en los sistemas y sus relaciones con el entorno. Esto es, que una persona efectúa nuevas indicaciones y distinciones (Brown, 1979) de la reali-

dad interconectada para advertir nuevas propiedades emergentes del sistema que analiza y que, en el escenario de la densidad digital, es habilitado por la conectividad y las expectativas de los diferentes participantes de la sociedad.

En lectura de una vista de ecosistema, es posible entender la densidad digital como el habilitador de una red de fenómenos interconectados e interdependientes, donde las actuaciones y actividades de los participantes son relevantes para darle sentido a la dinámica del sistema interrelacionado. En este contexto, se entiende que una mayor conectividad enfatiza los valores y principios de la cooperación, la creatividad, la síntesis, la asociación y la experiencia de vida, con fines superiores para actuar de esta misma forma (Capra, 2003), sin perjuicio de la canalización de estos mismos principios y valores, para concretar acciones abiertamente contrarias a la ética digital de los datos y en favor de intereses particulares, que afecten el interés general sobre el cual evoluciona el ecosistema.

Por consiguiente, la actual omnipresencia de las tecnologías de información y el aumento de la dependencia de la conectividad para el desarrollo de los negocios a nivel internacional, hacen que cualquier evento de inestabilidad, fallo o interrupción genere impactos globales con afectaciones en la estabilidad de las economías, las dinámicas sociales, las tensiones políticas, las innovaciones tecnológicas y hasta impactos de nivel ecológico, cuando artefactos tecnológicos son los responsables del monitoreo de condiciones particulares del ambiente y sus relaciones (WEF, 2019).

Ciberriesgo: una realidad emergente

Al entender el ciberriesgo como una realidad sistémica de las organizaciones, es necesario comprender en perspectiva relacional la forma de pensar y concebir el mundo. La vista mecanicista basada en causa-efecto, en la homogeneidad de los resultados y la predictibilidad de los procesos deja de ser funcional, como quiera que efectos de borde o no documentados, se pueden presentar sin explicación aparente.

El ciberriesgo, como una propiedad emergente de las relaciones digitalmente modificadas de la realidad, establece un reto cognitivo y social, que demanda romper con los paradigmas disciplinares, para encontrar respuestas o mejores preguntas en escenarios cada vez más inestables e inciertos, fruto de una mayor densidad digital en la dinámica de los elementos sociales. En este sentido, el ciberriesgo se configura como una apuesta relacional entretejida en la conectividad de los objetos físicos y las realidades sociales, que cambia la manera como se percibe el mundo y crea escena-

rios inéditos que retan las prácticas de gestión de riesgos actuales.

En consecuencia, el ciberriesgo desarrolla una serie de características que lo configuran como una realidad emergente, la cual demanda una vista interdisciplinar, para tratar de comprender sus movimientos en el contexto organizacional y establecer patrones que puedan ser de interés para los objetivos estratégicos de las empresas. A continuación, se detallan siete (7) características claves que revelan la presencia del ciberriesgo en las corporaciones modernas (Fahrenthold, P. et al, 2010).

- *Alta incertidumbre*: la frecuencia y el potencial de impacto son difíciles de valorar. Es necesario comprender la dinámica del todo y sus relaciones con el entorno para tratar de leer la inestabilidad del sistema y la asimetría de la información disponible.

- *Sin consenso*: tanto analistas como ejecutivos no alcanzan acuerdo sobre la forma de enfrentar o reconocer los inciertos que se presentan en un entorno digitalmente modificado.

- *Relevancia incierta*: existe poca guía o información sobre situaciones planteadas, que pueden sonar futuristas o poco creíbles.

- *Difícil de comunicar*: existe bajo entendimiento y, en tal sentido, no se les presta atención, dando lugar a puntos ciegos en la organización que pasan desapercibidos dentro de la dinámica empresarial.

- *Sin dueño concreto*: comprender el ciberriesgo implica superar la visión disciplinar y salir al encuentro de las diferentes formas de ver la realidad, para comprender sus alcances e impactos. No es el ejercicio de un área, sino la construcción colectiva de diferentes actores.

- *Tiene carácter sistémico*: son riesgos que sólo se manifiestan en relación con otros. Se entiende la densidad digital como el tejido que habilita esta nueva comprensión de la realidad.

- *Tendencias imperceptibles*: se manifiestan en rarezas, inconsistencias y contradicciones en el entorno. Son revelaciones de señales y eventos que para muchos pueden ser imperceptibles y para otros, la identificación de realidades que pueden llegar a ser relevantes para el negocio.

Al ser el ciberriesgo un riesgo emergente es necesario reinventar la práctica de la gestión de riesgos, desde el pensamiento sistémico, de tal forma que no sólo prime la vista de las probabilidades asociadas con los riesgos conocidos, sino que se incorpore la dinámica de las posibilidades, en las que se perciben y entienden los riesgos latentes y emergentes (Cano, 2017). Por

tanto, movilizar los esfuerzos en el tratamiento de los ciberriesgos significa comprender que el entorno es cambiante y demanda superar las cegueras cognitivas (Meyer & Kunreuther, 2017) propias de los saberes previos y las exigencias de certezas de los ejecutivos actuales.

Ciberriesgo: un escenario disruptivo para las empresas

Si entendemos que un escenario disruptivo es aquel proceso a través del cual una empresa pequeña con menos recursos, es capaz de desafiar las empresas ya establecidas, concentrándose con éxito en segmentos olvidados, ganando terreno mediante la entrega de una funcionalidad más adecuada, a menudo a un precio más bajo (Christensen, Raynor & McDonald, 2015), se ingresa en terrenos donde la convergencia tecnológica y la densidad digital, habilitan nuevas posibilidades para crear distinciones inexistentes.

Esto es, que la disrupción surge de la incorporación y desarrollo de nuevas relaciones entre los negocios existentes, la conectividad, el aumento de la densidad digital de los objetos físicos y la mayor dependencia de los terceros de confianza, donde se apalancan las capacidades requeridas para enriquecer la experiencia diferenciadora que esperan los clientes. En este sentido, se advierte una acelerada disrupción digital, en la que las empresas deben transformar rápidamente su modelo operativo y de negocio, además de las experiencias del cliente, con el fin de mantener su posición estratégica vigente y repensar la forma como genera valor dentro y fuera de su segmento de negocio (Kane, Nguyen, Copulsky & Andrus, 2019).

Así las cosas, el ciberriesgo se advierte como una realidad emergente, ahora en un ecosistema digital, en el que los diferentes participantes cooperan entre sí, intercambian conocimientos, desarrollan tecnologías abiertas y adaptables; proponen modelos de negocios novedosos que buscan encontrar patrones diferenciadores para que los clientes puedan explorar los límites de sus expectativas (Jimeno, 2017). En efecto, al aumentar la interacción y flujo de datos, generalmente personales, se crean contextos digitales enriquecidos para los individuos, de manera de dar respuesta a situaciones particulares y alimentar un escenario de vulnerabilidades emergentes, cuya naturaleza y efectos pueden ser desconocidos, y requieren un gobierno y gestión diferentes.

En una realidad como la actual, digital y tecnológicamente modificada es necesario desarrollar un nuevo paradigma de confianza, para que tanto las empresas como las personas establezcan relaciones de confiabilidad, sobre la base de la vulnerabilidad por defecto. Es decir que, a pesar de los esfuerzos y acciones adelantadas para evitar un evento no deseado, se tendrán

acuerdos concretos de acción y respuesta, cuando se materialice la inevitabilidad de la falla (Cano, 2017b).

Bajo esta perspectiva, las organizaciones deberán estar preparadas para enfrentar la materialización de un ciberriesgo, de escalas locales o de proporciones internacionales, como lo puede ser un ciberataque coordinado y desplegado desde diferentes lugares, con capacidad de infección viral sobre diferentes tipos de dispositivos de escritorio o móviles y secuestro de la información allí contenida (Daffron, Ruffle, Andrew, Copic, Quantrill, Smith & Leverett, 2019). De esta forma, la gestión de incidentes deberá ser la capacidad más relevante que deberán desarrollar las empresas frente al reto de la materialización de un riesgo cibernético.

Retos de la gestión del riesgo cibernético

Un reciente estudio de Deloitte (2018) revela algunos aspectos claves de la gestión del riesgo cibernético, los cuales advierten la necesidad de una visión holística por parte de las organizaciones, inversiones requeridas para configurar visiones prospectivas de las amenazas y contratación de talento especializado para reinventarse frente a la volatilidad del entorno. A continuación, se detallan algunas reflexiones alrededor de tres (3) de los elementos que mayor puntuación tuvieron en el estudio en mención.

El primer elemento, no hace referencia a aspectos técnicos o tácticos de la organización, sino a consideraciones estratégicas como "estar adelante en los cambios de las necesidades del negocio", parafraseado como "**anticipar escenarios emergentes para la organización**". Este primer punto, establece una declaración clave para las empresas y sus ejecutivos; no se trata de repetir aquello que se conoce o generalmente se lleva para presentar en la junta, sino crear un espacio para retar aquello que se hace a la fecha y tratar de imaginar cómo se puede afectar el modelo de generación de valor de la empresa.

Lo anterior, significa revisar y comprender el riesgo cibernético como una malla de implicaciones técnicas, sociales, económicas y políticas que ubica a la empresa en un ecosistema tecnológico dinámico, espacio en el que se reconocen actores relevantes de su entorno, incluidos sus aliados y competidores estratégicos, para identificar las interacciones de interés, y así crear zonas de ventajas competitivas (OECD, 2015), las cuales deben protegerla de las amenazas digitales naturales, que contemplan actores conocidos y desconocidos, los cuales hacen parte del nuevo paisaje digital.

El segundo aspecto clave identificado en el estudio se refiere a "hacer frente a las amenazas de actores sofisticados", que pudiésemos

configurar como "**enfrentar las amenazas de actores desconocidos**".

Cuando se entiende que en la actualidad una organización se encuentra ubicada en un espacio en el que existe una confrontación de intereses por activos digitales estratégicos, se quiebra el marco general de prácticas asociadas con los riesgos informáticos, dedicado a proteger y asegurar, para inaugurar la incorporación de las capacidades críticas como defender y anticipar.

Mientras en los estándares tradicionales de seguridad se busca alcanzar certezas sobre el incierto que puede producir un ataque, en el escenario del riesgo cibernético, no solamente hay que considerar lo anterior, sino reconocer el territorio de acción de los adversarios, sus recursos, sus posibilidades, capacidades e impactos con el fin de modelar acciones en diferentes aspectos: técnico, políticos, económicos y sociales, de tal forma, que enfrentar las amenazas digitales actuales, no responde a un ejercicio de los "técnicos", sino a una visión estratégica del negocio, que da cuenta de comportamientos y movimientos coordinados para demorar, interrumpir, contener o anticipar los efectos de una ciberoperación deliberada para afectar los intereses claves de la compañía (Donaldson, Siegel, Williams & Aslam, 2015).

Un tercer elemento es "incorporar talento especializado en ciberseguridad", frase que se puede adaptar como "**incorporar analistas de ciberriesgos especializados**". Los nuevos profesionales especializados en riesgos cibernéticos, no sólo deben demostrar competencia técnica básica en los aspectos de seguridad de la información, sino exponer capacidades analíticas de inteligencia, análisis y correlación de eventos, reflexiones y formación geopolítica e infopolítica, cooperación interorganizacional y gubernamental, reconocimiento de patrones de amenazas emergentes y suficiencia en el diseño, análisis y simulación de escenarios.

Este profesional, ya no tiene una visión disciplinar de un dominio de conocimiento específico, sino la construcción de saberes interdisciplinares, que configuran marcos de trabajo agregados, que revisan una realidad inestable e incierta, para dar respuesta a las propuesta de los atacantes, que no vacilan en proponer retos complejos a las organizaciones, los cuales van desde el secuestro de datos, pasando por las noticias y videos falsos, las agresiones a las marcas, las afectaciones a la infraestructura tecnológica, hasta la creación de amenazas digitales desconocidas basadas en la inteligencia artificial.

De modo que, adelantar la gestión del riesgo cibernético, no será viable si no se entiende desde la perspectiva sistémica de las relaciones entre los objetos. Esto es, entender el entorno

como un todo que evoluciona y se transforma conforme sus diferentes actores toman posiciones respecto a temas específicos, las cuales, terminan afectando la dinámica de una sociedad digital y tecnológicamente modificada que demanda mayores y mejores experiencias en sus productos y servicios (Saran, 2017).

Reflexiones finales

Al tener en la base de su fundamentación una visión mecanicista y los saberes de la seguridad de la información, el riesgo cibernético ha heredado una gestión de riesgos, por lo general, desconocidos. En este sentido, cuando se incorpora una vista sistémica extendida de la organización para comprender cómo los efectos de la materialización de los ciberataques pueden comprometer la promesa de valor de la empresa, se cruzan los límites de los estándares tradiciones de gestión de riesgos, para darle paso a una revisión amplia de las amenazas que pueden ser conocidas, latentes y emergentes (Cano, 2017).

Por tanto, en un entorno de "disrupción digital", entendida ésta como "un efecto que cambia las expectativas fundamentales y comportamientos en una cultura, mercado, industria o proceso causada por, o expresada a través de, capacidades digitales, canales o activos" (Yockelson & Smith, 2018), es necesario mantener una monitorización del ambiente, identificando aquellas anomalías, rarezas y contradicciones, que adviertan patrones no conocidos, los cuales marcan las nuevas capacidades y habilidades de los adversarios (Charan, 2015), con el fin de anticipar sus movimientos y crear acciones de defensa tanto activas como pasivas, que permitan, no evitar ser atacados exitosamente, sino prevenir, demorar, distraer o interrumpir sus acciones bajo condiciones inciertas.

De esta forma, las organizaciones siguiendo las reflexiones de Schoemaker & Day (2017) deberán desarrollar una **mentalidad de experimentación permanente** para anticipar los efectos adversos de los atacantes, contar con **equipos de trabajo con personal calificado** en el riesgo cibernético, que al experimentar y simular, puedan codificar, compartir y aplicar los nuevos conocimientos y patrones identificados, y finalmente, **mirar más allá de sus fronteras organizaciones y de mercado** buscando puntos de vista distintos, que reten sus saberes previos, no sólo para aprender/desaprender, sino para obtener una ventaja estratégica competitiva en un mundo turbulento que a menudo paraliza a los demás.

Finalmente, vale la pena recordar que los ciberriesgos definen una forma distinta de entender la dinámica de las organizaciones y que sus impactos, frente a hechos materializados, pueden tener conse-

cuencias globales, muchas de ellas no conocidas. En consecuencia, es necesario tener presente que los riesgos cibernéticos:

- No son retos aislados, son un resultado de la lectura sistémica de sus componentes (personas, procesos, tecnología y regulaciones).
- Son desafíos complejos en los que no tenemos la variedad requerida para poderlos comprender y atender.
- Son desafíos que generan tensiones socioeconómicas globales y asimetrías de información.
- Son emergentes, fruto de las relaciones entre los diferentes elementos y actores de los nuevos ecosistemas digitales, los cuales generalmente son puntos ciegos para la gestión tradicional de riesgos.
- Son interdisciplinares y demanda el desarrollo de lenguajes alternativos entre las disciplinas actuales, para darle forma y sentido a los efectos e impactos de su posible materialización.

Referencias

Brown, S. (1979). *Laws of Form*. New York, USA: E.P. Dutton

Cano, J. (2017). La ventana de AREM. Una estrategia para anticipar los riesgos y amenazas en ciberseguridad empresarial. *ISACA Journal*. vol. 5. Recuperado de: https://www.isaca.org/Journal/archives/2017/Volume-5/Pages/the-arem-window-spanish.aspx

Cano, J. (2017b). Riesgo y seguridad. Un continuo de confianza imperfecta. En Dams, A., Pagola, H., Sánchez, L. y Ramio, J. (eds) (2017) *Actas IX Congreso Iberoamericano de Seguridad de la Información*. Universidad de Buenos Aires - Universidad Politécnica de Madrid. 34-39

Capra, F. (2003). *Las conexiones ocultas: implicaciones sociales, medioambientales, económicas y biológicas de una nueva visión del mundo*. Barcelona, España: Anagrama.

Charan, R. (2015). *The attacker's advantage. Turning uncertainty into breakthrough opportunities*. New York, USA: Perseus Books Groups.

Christensen, C., Raynor, M. & McDonald, R. (2015) What is disruptive innovation? *Harvard Business Review*. December. 44-53

Daffron, J., Ruffle, S., Andrew, C., Copic, J., Quantrill, K., Smith. A. & Leverett, E. (2019). Bashe Attack: Global Infection by Contagious Malware. Cambridge Centre for Risk Studies. *Research Report*. Recuperado de: https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/bashe-attack

Deloitte (2018). Global Risk Management Survey, 11 edition. *Deloitte Insights*. Recuperado de: https://www2.deloitte.com/content/dam/insights/us/articles/4222_Global-risk-management-survey/DI_global-risk-management-survey.pdf

Donaldson, S., Siegel, S., Williams, C. & Aslam, A. (2015). *Enterprise cybersecurity. How to build a successful cyber-defense program against advanced threats*. New York, USA: Apress.

Fahrenthold, P. et al (2010). Emerging risk and Enterprise risk management. *RIMS Executive Report*. Recuperado de: https://www.rims.org/resources/ERM/Documents/EmergingRisk_ERMweb.pdf

Jimeno, J. (2017). *La responsabilidad civil en el ámbito de los ciberriesgos*. Madrid, España: Fundación MAPFRE.

Kane, G., Nguyen, A., Copulsky, J. & Andrus, G. (2019). *The technology falacy. How people are the real key to digital transformation*. Cambridge, MA. USA: MIT Press.

Luhmann, N. (1998). *Complejidad y modernidad. De la unidad a la diferencia*. Madrid, España: Trotta.

Meyer, R. & Kunreuther, H. (2017). *The ostrich paradox. Why we underprepare for disasters*. Philadelphia, PA. USA: Wharton Digital Press.

OECD (2015). Digital Security Risk Management for Economic and Social Prosperity: *OECD Recommendation and Companion Document*, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en

Porter, M. & Heppelmann, J. (2014). How Smart, connected products are transforming competition. *Harvard Business Review*. Noviembre.

Saran, S. (2017). Time to face up to cyber threats. *Observer research foundation*. Recuperado de: https://www.orfonline.org/research/time-to-face-up-to-cyber-threats/

Schoemaker, P. & Day, G. (2018). Strategic actions in the face of uncertainty. *Revista Brasileira de Marketing – ReMark*. Special Issue. 17(5). 700-712

WEF (2019). The Global Risks Report 2019. 14th Edition. *Insight Report*. World Economic Forum. Recuperado de: https://www.weforum.org/reports/the-global-risks-report-2019

Yockelson, D. & Smith, D. (2018). Willful Disruption — Scaling, Operating and Changing the Digital Game: A Gartner Trend Insight Report. *Gartner Research*.

Zamora, J. (2017). ¿Es posible programar modelos de negocio? *IESE Insight*. II Trimestre de 2017.

Jeimy J. Cano M., Ph.D, CFE, CICA. *Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*

Dos

Ciberriesgo desde la perspectiva de riesgo sistémico

DOI: 10.29236/sistemas.n151a6

"El simple aleteo de las alas de una mariposa puede originar un tsunami al otro lado del mundo". Proverbio Chino

Resumen

"*No importa los riesgos que asumamos, siempre consideramos que el final es demasiado pronto, aunque en la vida, más que nada, la calidad debe ser más importante que la cantidad*"- Alex Honnold. Actualmente la humanidad está enfrentándose a una nueva dinámica social, a unas nuevas formas de convivencias reales no virtuales inmersas en un nuevo espacio de convivencia social que no es territorial ni material, sino un espacio meta-espacial, más que una representación virtual -siendo un ambiente intangible, pero a la vez muy real- (Suñé, 2015). Se trata del ciberespacio, constituido como el quinto entorno estratégico, tras Tierra, Mar, Aire y Espacio (Adams, 2015). Durante el año 2018, el mundo llegó a enfrentar un crecimiento significativo y complejo en los desafíos que trae la "hiperconectividad", enfrentándonos a problemáticas desde el cambio climático, hasta la crisis financiera global. No podemos caer en el error de pensar que exclusivamente las grandes empresas y multinacionales serán las afectadas por este tipo de riesgo, teniendo como referencia que la afectación de cualquier participante de un ecosistema cibernético podrá reflejar su impacto en todos los que en él conviven.

Palabras clave

Riesgo sistémico, ciberriesgo, ciberseguridad, ciberespacio

Introducción

Anualmente el World Economic Forum (WEF) presenta el Global Risks Report (World Economic Forum, 2019), exponiendo para el presente año un contexto de preocupantes tensiones geopolíticas y geoeconómicas. Si no se resuelven, dificultará la capacidad del mundo para enfrentar una gama creciente de desafíos colectivos, desde la evidencia progresiva de la degradación ambiental hasta las crecientes interrupciones y amenazas que ha conllevado el desarrollo de una nueva revolución, donde Klaus Schwab autor del libro "La cuarta revolución industrial", vaticina "*Estamos al borde de una revolución tecnológica que modificará fundamentalmente la forma en que vivimos, trabajamos y nos relacionamos. En su escala, alcance y complejidad, la transformación será distinta a cualquier cosa que el género humano haya experimentado antes*". Son precisamente aquellos países más avanzados los que experimentaron los cambios con mayor rapidez, pero a la vez las economías emergentes las que llegaron a identificar mayores beneficios. Figura 1

La tecnificación y evolución a la interconexión alrededor de las áreas de los sistemas tradicionales de automatización de fabricación continuará ganando impulso; por lo tanto, la convergencia de TI y las tecnologías operativas será un

Figura 1. Resumen Riesgos Top 5 - 2015 a 2019, (WEF, 2019)

punto fuerte de discusión dentro de las organizaciones, enfocando nuevas plataformas y servicios empresariales que potencialmente integrarán diferentes áreas, desde datos empresariales a nivel corporativo, hasta automatización a nivel de campo y proceso. Estas plataformas serán altamente deseables en la búsqueda de la digitalización, ya que ofrecerían mejores diseños, visualizaciones, ergonomía y comodidad de accesibilidad. Sin embargo, estas plataformas presentan el desafío de administrar la privacidad al mismo tiempo que aumentan el área de exposición a las amenazas cibernéticas y, a la vez mantener un nivel similar o superior de seguridad y confiabilidad en torno a las operaciones de estos sistemas interconectados.

Dicha revolución posee la capacidad de incrementar los niveles de ingreso globales y brindar un mejoramiento en la calidad de vida de sociedades y comunidades enteras, apunta Schwab, las mismas que se han beneficiado con la llegada de los diferentes entornos digitales (asignación de parqueaderos en zonas metropolitanas, transporte compartido mediante redes sociales, plataformas de comercio electrónico, servicios financieros, entre otros). Sin embargo, el proceso de transformación sólo beneficiará a quienes sean capaces de innovar y adaptarse.

La interconectividad y la adopción de las nuevas tecnologías traen consigo un incremento en la exposición a una nueva naturaleza de riesgos denominado riesgos cibernéticos, que están demandando por parte de entidades y autoridades esfuerzos importantes para identificarlos y gestionarlos. Uno de los grandes retos de las organizaciones lo constituye la seguridad de la información, en particular, la que reside o se procesa en medios electrónicos, la cual, ahora más que nunca, se encuentra expuesta a las amenazas cibernéticas, dada la naturaleza global de Internet y de los sistemas de información, que no tienen una limitación fronteriza.

Por otro lado, el riesgo sistémico se refiere al riesgo de una avería de todo un sistema en lugar de simplemente la falla de partes individuales. Un ejemplo de ello en un contexto financiero, es el riesgo de una falla en cascada en el sector causada por las interconexiones dentro del sistema financiero, teniendo como resultado una grave recesión económica. Una pregunta clave para los formuladores de estrategias para la gestión de riesgos es cómo limitar la acumulación de riesgo sistémico y contener los eventos de crisis cuando ocurren. Figura 2

Un ecosistema con varios participantes

Podemos entonces decir que el ciberespacio, dentro de su misma definición se podría considerar como un ecosistema cibernético que comprende una variedad de diver-

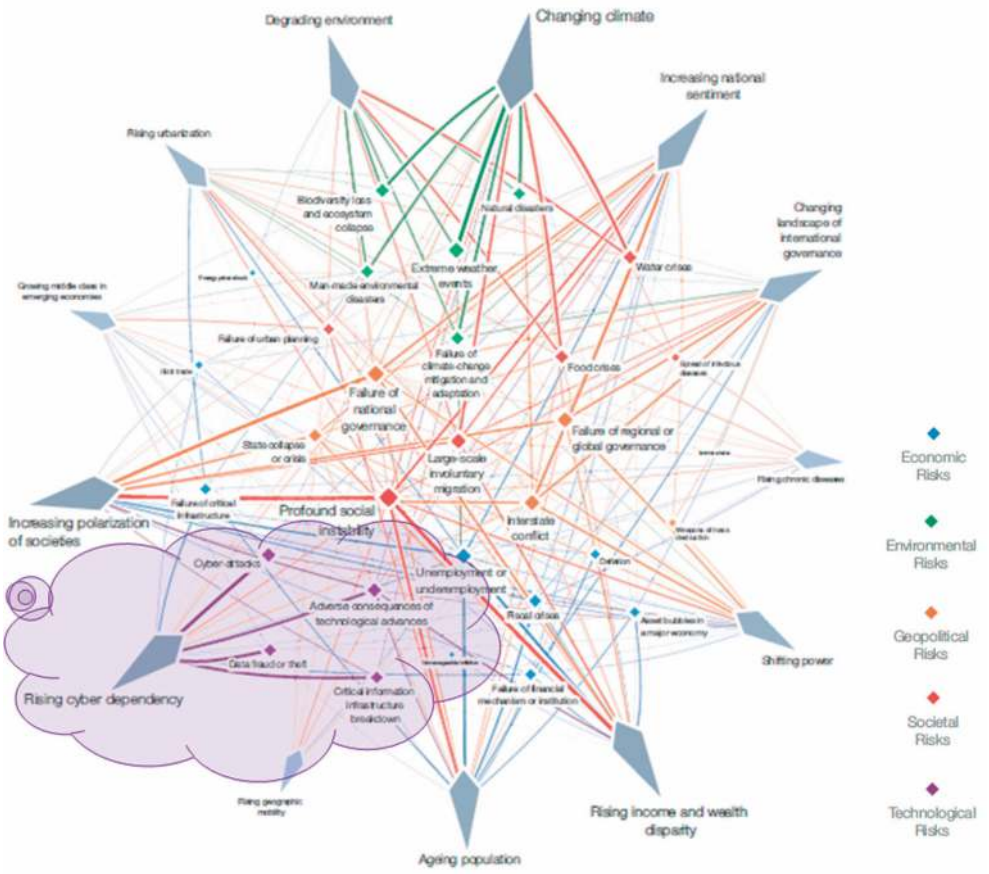


Figura 2. Interdenpencias de los Riesgos, (WEF, 2019)

sos participantes como empresas privadas, organizaciones sin fines de lucro, gobiernos, individuos y dispositivos cibernéticos que interactúan con múltiples propósitos. Son las infraestructuras de TI, que de manera interconectada brindan un sinnúmero de interacciones entre personas, procesos, datos y tecnologías de comunicación junto con el entorno y las condiciones que influyen en esas interacciones.

Las organizaciones de todos los tamaños, tanto en el sector público como en el privado, dependen cada vez más de los activos de información y tecnología, sin embargo, es necesario contar con el apoyo de las personas para ejecutar con éxito procesos de negocios que, a su vez, respaldan la prestación de servicios. La falla de estos activos tiene un impacto directo y negativo en los procesos de negocios que soportan. Esto, además, puede convertirse en una incapacidad para la prestación de los servicios, lo que finalmente afecta la misión de la organización. Dadas estas relaciones, la gestión de los riesgos para estos activos es un factor clave para posicionar la organización para el éxito. Aun cuando se pueda caer

en la falla que la identificación de riesgos cibernéticos aplica única y exclusivamente a las organizaciones de TI, nuestra vida diaria, vitalidad económica y seguridad nacional dependen de un ciberespacio estable, seguro y resistente que se encuentra comprendido por diferentes sectores e industrias.

El ciberespacio y su infraestructura subyacente son vulnerables a una amplia gama de riesgos derivados de amenazas y peligros tanto físicos como cibernéticos. Los sofisticados actores y los estados nacionales explotan las vulnerabilidades para robar información y dinero y están desarrollando capacidades para interrumpir, destruir o amenazar la prestación de servicios esenciales.

En 2017, la firma Deloitte informó que la industria de la energía era el segundo objetivo más popular para los ataques cibernéticos en 2016. Casi tres cuartos de las compañías de petróleo y gas de los Estados Unidos, según la consultora, tuvieron un incidente cibernético en dicho año; no obstante, sólo una pequeña mayoría citaron el riesgo como una de las principales preocupaciones en sus informes anuales. Estas compañías al día de hoy tienen miles de dispositivos conectados y esto conlleva a una situación muy preocupante de ciberriesgo en el petróleo y el gas.

Se espera que el mercado de IoT (internet de las cosas por sus siglas en inglés) para la industria del petróleo y el gas crezca a una tasa del 82% entre 2017 y 2022.

En los últimos años, la industria global del petróleo y el gas ha sido testigo de desafíos como la caída de los precios, la poca demanda y las preocupaciones ambientales. IoT permite monitorear las instalaciones de forma remota y obtener conocimiento sobre los inventarios diarios y las condiciones de los equipos que soportan la operación. El creciente número de compañías de petróleo y gas está invirtiendo en sistemas de control, software y análisis mejorados para optimizar sus operaciones y darles una ventaja competitiva.

Según *MarketsandMarket*, hasta el año 2022 se espera que el mercado general de tecnología operacional (OT) se valúe en USD 42 mil millones, con un crecimiento anual del 6,7%. Los factores que impulsan el crecimiento de este mercado es la creciente demanda de industrialización en economías emergentes; evolución de IIoT (internet de las cosas en el sector industrial), y aumento de las máquinas de comunicación y monitoreo; junto a la creciente demanda de soluciones de automatización inteligente.

Con el sector del petróleo y el gas, adoptar IoT para mejorar sus procesos es parte de su futuro, pero su primer objetivo es aprender cómo implementar la seguridad en su infraestructura e identificar clara-

mente que los ciberriesgos presentes podrán llegar a verse reflejados en otros sectores o hasta en la misma sociedad. Las amenazas cibernéticas para las compañías de petróleo y gas son una realidad en incremento exponencial. El objetivo de un atacante no sólo contempla equipos de campo, sino subcontratistas y bufetes de abogados que trabajan para varias de estas compañías. En junio de 2017, el virus informático NotPetya afectó a muchas compañías en todo el mundo, incluido el gigante ruso Rosneft.

Basado en ello, gobiernos como el de Estados Unidos vienen trabajando en estrategias que proporcionan al Departamento de Seguridad Nacional un marco para identificar las responsabilidades de seguridad cibernética durante los próximos cinco años. De esta manera buscan mantener el ritmo del panorama de riesgo cibernético en evolución, mediante la reducción de las vulnerabilidades y la creación del concepto de ciberresiliencia; contrarrestar a los actores maliciosos en el ciberespacio; responder a incidentes, además de que el ecosistema cibernético sea más seguro y resistente.

Contextualización del riesgo sistémico

Los riesgos generalmente son abordados de manera individual por una organización dentro de la gestión para sus procesos de negocio. Uno de los aspectos relevantes es la identificación y diferenciación de lo que es un riesgo sistémico y un riesgo sistemático. Al referirnos al primero se enfoca al reconocimiento de un sistema, como un conjunto de diferentes elementos que se encuentran relacionados entre sí, teniendo una o varias interdependencias con un objetivo en común; ejemplo de ello es un equipo de futbol, donde cada uno de los integrantes del equipo cumple una función para el objetivo común. El riesgo sistemático, por su parte, se refiere a la metodología de hacer las cosas, donde se debe identificar y analizar el problema antes de realizar cualquier acción, formular múltiples opciones, definir y establecer los criterios de selección, como también elegir y ejecutar la decisión final. Cuando se habla de riesgos sistémicos, el contexto es importante. Un riesgo que parece generalizado cuando se observa desde un país puede parecer diferente al de otro. Por ejemplo, durante la recesión de 2008 a 2010, las economías que para ese momento se encontraban en desarrollo como India y China obtuvieron mejores resultados que el resto de naciones. El impacto de la recesión fue mínimo para estos países.

La identificación de un marco de referencia es importante para juzgar si un riesgo tiene la naturaleza de ser sistemático o no. Pongamos por caso la existencia de dos países que tienen relaciones comerciales con la Unión Europea. El primero, completamente dependiente

(basado en exportaciones) y el segundo con una sola exposición parcial a los mercados de la Unión.

Adicional a esto, contemplemos la hipótesis de que dentro del plan de desarrollo de la Unión Europea se lleguen a realizar algunas modificaciones en el ámbito jurídico legal para disminuir las relaciones del mercado de exportación con ambos países, estableciendo un alto impuesto a las importaciones, lo cual afecta negativamente las exportaciones de cualquiera de los dos países, en donde el riesgo relativo se fundamenta en el marco de referencia. Para el primero, el riesgo tiene una naturaleza sistémica, pero, para el segundo país sólo representará una afectación para una pequeña cantidad de compañías. Por lo tanto, desde la perspectiva del segundo país, el riesgo puede llegar a no ser considerado sistémico.

Si no está seguro de la naturaleza del riesgo, definiendo si es sistémico o no, simplemente hágase esta pregunta, ¿es posible eliminar o equilibrar los impactos negativos sin llegar afectar a terceros o llegar a generar agentes de masificación de nuevos riesgos? Si la respuesta es afirmativa, ese riesgo no es sistémico.

El riesgo sistémico aplicado a las finanzas tiene muchas analogías con el análisis de riesgos que otros sistemas (no financieros) pueden exhibir. Fundamentalmente, el estudio del riesgo sistémico (financiero) se deriva de la constatación de que los sistemas financieros son frágiles. Hay cuatro elementos fundamentales para un mejor entendimiento del riesgo sistémico (Danielsson, 2016):

Riesgo endógeno
Se considera aquel riesgo creado por y dentro del propio ecosistema, en lugar de un resultado a un evento devastador fuera del sistema.

Mecanismos de amplificación
El origen de las crisis sistémicas generalmente se desencadena por un pequeño evento, cuyo impacto se magnifica por los vínculos dentro del ecosistema. En otras palabras, existen elementos que llegan a potencializar el impacto producido, viéndose reflejado en consecuencias a otros dentro del ecosistema.

Identificación de riesgos
Más allá de los factores comunes generados dentro de la identificación de riesgo es necesario establecer variables como la afectación de diferentes elementos del entorno, como el comportamiento de la materialización del riesgo y su magnificación, teniendo como focos las interdependencias que la organización posea en el ecosistema.

Creación de políticas
Los entes reguladores deben centrarse en iniciativas que reduzcan el riesgo sistémico y evitar aquellas

que, incluso con buenas intenciones, conduzcan realmente a la creación de nuevos y mayores riesgos.

Presencia del ciberriesgo en el sector financiero

Las entidades financieras en Colombia están comenzando a usar conceptos como blockchain para el registro y aseguramiento de las transacciones; big data y data analitics para el almacenamiento de grandes volúmenes de información y la toma de decisiones; *machine learning* para el otorgamiento de créditos, reconocimiento de siniestros y prevención del fraude; *algorithmic trading* para la compra y venta de valores en los mercados electrónicos; *cloud computing* para el desarrollo, pruebas y operación de aplicaciones administrativas y misionales; *artifitial intelligence* para manejar portafolios financieros; *biometrics* para el reconocimiento y autenticación de los clientes; IoT o internet de las cosas para lograr una tarifación adecuada de las pólizas de seguros; *smart contracts* o contratos inteligentes, en operaciones de comercio electrónico; APIs y *web services* para proveer información a otras organizaciones sin depender de elementos computacionales particulares. Estas tecnologías ya se han consolidado, están al alcance de personas y entidades de todo tipo y tamaño y su aplicación en diferentes sectores y actividades sólo está limitada por la creatividad.

El sector financiero ha estado durante mucho tiempo a la vanguardia de la ciberseguridad y el intercambio de información y cooperación en toda la industria. Aun así, los ataques cibernéticos a las diferentes instituciones financieras alrededor del mundo y las infraestructuras de los mercados financieros se han vuelto más frecuentes y sofisticados, lo que ha provocado inversiones de seguridad cada vez mayores y un mayor enfoque en la mitigación y gestión del riesgo cibernético. Paralelamente a estos esfuerzos, el sector financiero, los reguladores y los gobiernos nacionales han estado trabajando para mejorar la resistencia y la estabilidad en general con la esperanza de evitar una repetición de pánicos como la crisis financiera hace una década.

Otros ejemplos incluyen las intrusiones norcoreanas en el banco central de Bangladesh para intentar robar USD 951 millones a través del sistema de mensajes de pago global SWIFT (The New York Times, 2017) y el ataque al Banco de Chile, el banco más grande de dicho país, que “denegó el servicio a más de 9,000 computadoras y más de 500 servidores, para acceder a los sistemas conectados a la red SWIFT local del banco y realizar transacciones internacionales" (Cimpanu, 2018). A continuación, una breve reseña de los últimos 7 años que muestran algunos ciberataques significativos.

Figura 3

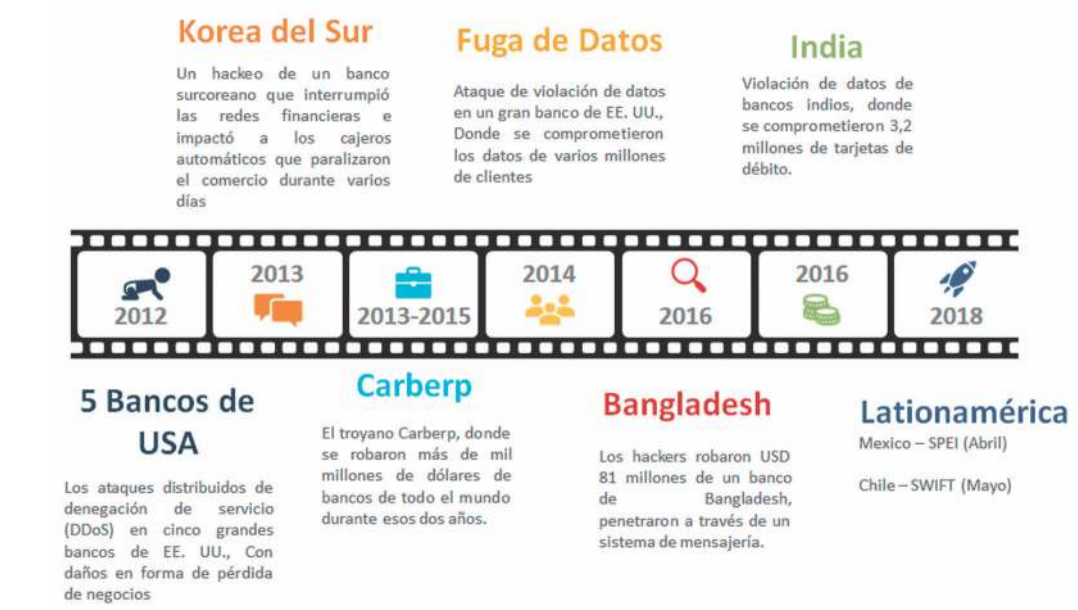


Figura 3. Reseña ataques cibernéticos 2012 - 2018. Adaptación del autor

Entonces surge la duda de, ¿cómo podrían los riesgos cibernéticos y los riesgos financieros interactuar para causar crisis sistémicas?, ¿hay algo fundamentalmente nuevo o diferente acerca de los riesgos cibernéticos?, ¿cómo deberían los economistas, reguladores, legisladores y bancos centrales enfocados en la estabilidad financiera incorporar los riesgos cibernéticos en sus modelos y pensamiento?

Algunas de las iniciativas más directas sobre estas preguntas comenzaron en 2013, luego de que una Orden Ejecutiva de la Casa Blanca instruyera al Departamento de Seguridad Nacional, en consulta con el Departamento del Tesoro, a identificar aquellas instituciones financieras para las cuales “(...) un incidente cibernético tendría un impacto de gran alcance, en seguridad económica regional o nacional" (Casa Blanca, 2014). En respuesta, ocho instituciones financieras líderes crearon el Centro de Análisis y Resiliencia Sistémica Financiera (FSARC) en 2016, concentrando los esfuerzos del sector en el "riesgo sistémico para el sistema financiero de los Estados Unidos, la seguridad cibernética actual y las amenazas emergentes" (FS-ISAC,2016).

Convergencia hacia una ciberresiliencia

La gestión del riesgo cibernético no es fundamentalmente diferente de la gestión del riesgo. Sin embargo, hay aspectos de los ecosistemas cibernéticos que hacen que la gestión del riesgo sea un desafío. La principal característica es el uso del ciberespacio. Las tecnologías de la

información y el ciberespacio han traído mejoras significativas para los individuos, las empresas y la sociedad en general en numerosas áreas, que incluyen la vida social, los servicios públicos, el comercio y la economía, el entretenimiento y las infraestructuras críticas. Al mismo tiempo, el uso y la dependencia del ciberespacio han introducido una serie de nuevas amenazas y vulnerabilidades. La ciberresiliencia se entiende como la capacidad de los sistemas para anticipar y adaptarse al potencial de sorpresa y falla, debiendo considerarse en el contexto de sistemas complejos que comprenden no sólo los dominios físicos y de información, sino también los dominios cognitivos y sociales, garantizando que la recuperación del sistema ocurra al considerar el *hardware*, el *software* y los componentes de detección interconectados de la infraestructura cibernética (Kott & Linkov, 2019).

Otro desafío importante con respecto a la gestión del ciberriesgo es que el ciberespacio evoluciona rápidamente y con frecuencia de una manera que es difícil de predecir. Los sistemas que hacen presencia en este ambiente meta espacial deben ser capaces de hacer frente a esta evolución. De hecho, se ven obligados a evolucionar en respuesta a la evolución del ciberespacio. Esto requiere un mayor enfoque en el monitoreo y la evaluación de riesgos en tiempo real como parte de la gestión general del riesgo cibernético.

Aunque los sistemas cibernéticos suponen un desafío desde el punto de vista de la gestión de riesgos, también existen características que podemos aprovechar y que tienen un efecto simplificador. El hecho de que estén hiperconectados en gran medida es beneficioso cuando se trata de la recopilación de datos, por lo que hemos enfatizado el uso de técnicas como el monitoreo y las pruebas. Además, la recolección de datos puede reducir la incertidumbre en la evaluación de riesgos con el uso de tecnologías emergentes como lo es Data Analytics y Big Data.

Finalmente es necesario la aceptación que el mundo en el cual vivimos ahora posee una dependencia tecnológica que obliga a desarrollar capacidades y metodologías que ofrezcan una identificación clara de aquellos riesgos cibernéticos teniendo como precedente que dichos riesgos tienden a ser sistémicos debido a su naturaleza la cual atenta contra más de un elemento dentro del ecosistema que representa el ciberespacio.

Día a día, nos enteramos de más ataques cibernéticos en nuestro país y en todo el mundo. Nuestra dependencia tecnológica hace que estos ataques lleguen a poseer el potencial de destruir nuestra seguridad militar y económica y, quizás, impactar el proceso que usamos para elegir a nuestros líderes.

Referencias

Adams, J. (2015). Cyber blackout (1st ed., pp. 15-21). Victoria, BC, Canada, FriesenPress.

Casa Blanca. (2014). *3 CFR 13636* - Executive Order *13636* (p. Sec. 7). Washington D.C.

Cimpanu, C. (2018). Hackers Crashed a Bank's Computers While Attempting a SWIFT Hack. Recuperado de: https://www.bleepingcomputer.com/news/security/hackers-crashed-a-bank-s-computers-while-attempting-a-swift-hack/

Danielsson, J. Fouché, M. & Macrae, R. (2016). Cyber risk as systemic risk. Recuperado de: https://voxeu.org/article/cyber-risk-systemic-risk

FS-ISAC Announces the Formation of the Financial Systemic Analysis & Resilience Center (FSARC) | FS-ISAC: Financial Services - Information Sharing and Analysis Center. (2016). Recuperado de: https://www.fsisac.com/article/fs-isac-announces-formation-financial-systemic-analysis-resilience-center-fsarc

Kott, A., & Linkov, I. (2019). *Cyber Resilience of Systems and Networks*. [S.l.]: Springer Nature (1st ed., pp. 4-7).

The New York Times (2017). North Korea Said to Be Target of Inquiry Over $81 Million Cyberheist. Recuperado de: https://www.nytimes.com/2017/03/22/business/dealbook/north-korea-said-to-be-target-of-inquiry-over-81-million-cyberheist.html

Refsdal, A., Bjørnar, S., & Stølen, K. (2015). *Cyber-risk management* [Cham]: Springer. (pp. 4, 9-25,26).

Suñé Llinás, E. (2015). La constitución del ciberespacio (1st ed.). Madrid: Porrúa México.

Ventre, D. (2014). Chinese cybersecurity and defense (1st ed., p. 46). London: ISTE. Edward

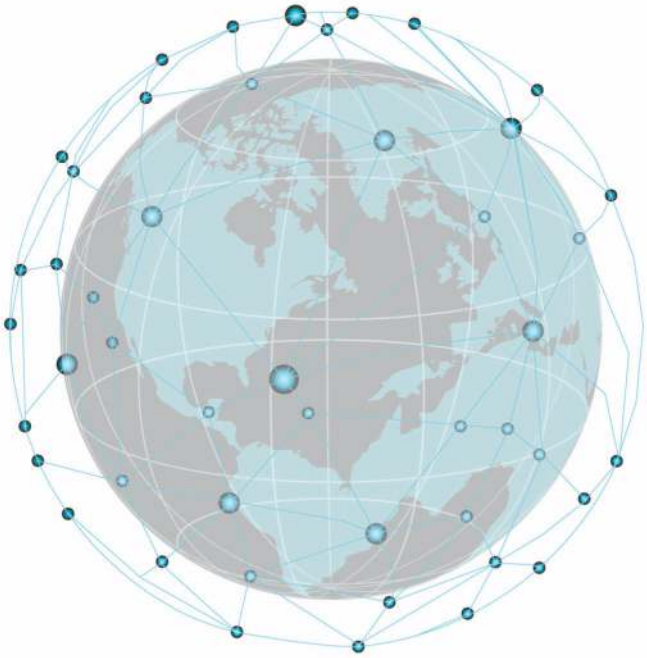
Griffor (2017) *Handbook of System Safety and Security: Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems.* Cambridge, MA. USA: Singress.

World Economic Forum. (2019). *The Global Risks Report 2019* (pp. 5-8). Geneva: World Economic Forum. Recuperado de: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Joshsua J. González Díaz, M.Sc. *Ingeniero de Sistemas de la Pontificia Universidad Javeriana, especialista en seguridad de la información de la Universidad de los Andes, Especialista en Derecho Informático de la Universidad Externado de Colombia y Magister en Seguridad de la Información de la Universidad de los Andes. Actualmente se desempeña como profesor catedrático e investigador de la maestría en Seguridad de la Información de los Andes y la Pontificia Universidad Javeriana. Líder del grupo de competencia en CTF Av3ng3rs 1n1t14t1v3 y CEO de la empresa de consultoría Stark Industries SAS.*

II ENCUENTRO DE GEODATOS:

TECNOLOGÍAS GEOESPACIALES PARA LA VIDA



LABORATORIO DE ENTRENAMIENTO : 15 DE AGOSTO

ENCUENTRO: 16 DE AGOSTO

XIX Jornada Internacional de Seguridad Informática

PRE-JORNADA: 19 DE JUNIO

JORNADA: 20 Y 21 DE JUNIO

POS-JORNADA: 22 DE JUNIO