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.*