Las juntas directivas y el riesgo cibernético

DOI: 10.29236/sistemas.n169a6

Fundamentos, áreas de riesgo y el proceso de duelo.

Resumen
En un escenario de tiempos posmodernos animados por complejidad, inestabilidad, inciertos y caos, los directorios de las empresas deben encontrar nuevas formas de mantener una vista actualizada sobre las diferentes tendencias y tensiones que marcan el ritmo de la dinámica internacional. En este sentido, el riesgo cibernético como responsabilidad ejecutiva surge como un nuevo reto sistémico que exige reconocer que no se conocen todos los riesgos y abrirse al proceso de construir nuevas reflexiones situadas en la promesa de valor de la organización, y desde allí avanzar en la gestión y gobierno de los ciberriesgos, como un compromiso corporativo con los diferentes grupos de interés para mantener una postura vigilante que habilite una organización más resiliente frente a amenazas cibernéticas. Este artículo, plantea algunas ideas básicas de esta relación naciente entre las juntas directivas y el ciberriesgo, como una excusa académica y práctica para acompañar a los directores en este reto inherente al desarrollo de los negocios en el contexto digital actual y futuro.

Palabras claves
Juntas directivas, Riesgo cibernético, Promesa de valor, Ciberataques, Duelo

Introducción

Los tiempos de inestabilidad y controversia que vive la humanidad establecen y definen nuevos desafíos para las organizaciones. Particularmente establecen retos novedosos para las juntas directivas, las cuales deben orientar y acompañar a la organización para establecer los nuevos rumbos estratégicos en medio de las tensiones, la incertidumbre y el caos propio de una realidad en tiempos posnormales (Sardar, 2010): con mayores complejidades sociales y organizativas a nivel político, económico, social, tecnológico, ambiental y legal.

En este sentido, los ejecutivos actuales deberán mantener una vista en la realidad actual, mientras exploran y actualizan el panorama de retos y riesgos de la empresa, el cual cambia de forma frecuente e inesperada, haciendo que los mejores pronósticos y ejercicios de actualización de sus mapas de ruta, queden obsoletos y muchas veces no respondan a las exigentes contradicciones y novedades del entorno.

Por tanto, no es la metodología que se use para mantenerse sintonizado con los cambios relevantes para el negocio, sino cómo la organización es lo suficientemente flexible y resiliente para aprender rápidamente y adaptarse a las transformaciones aceleradas del entorno. En consecuencia, los ejecutivos de primer nivel deben mantener calibrados sus sensores de la dinámica empresarial y retar sus saberes previos, para salirse de la zona cómoda de los riesgos conocidos y empezar a caminar y descubrir el desafío de tomar decisiones en medio de riesgos emergentes y algunas veces desconocidos (Agua, 2023).

En esta línea, recientemente los cuerpos directivos colegiados, denominados Juntas Directivas o Directorios, han recibido la noticia que ahora son responsables de la vigilancia y monitoreo de los riesgos cibernéticos. Un riesgo novedoso y distinto del riesgo de tecnología de información, que tratan de interpretar como algo tecnológico y cuya gestión le corresponde a los “técnicos”, sin percatarse que es un riesgo que atraviesa la esencia del negocio (interconexiones e interacciones de iniciativas digitales en todas las áreas de la empresa y sus clientes) y que requiere una visión sistémica e interdisciplinar para su adecuado tratamiento (Brinson & Briggs, 2023).

Así las cosas, es necesario visualizar este nuevo escenario de tensiones que genera el riesgo cibernético en las juntas directivas, para establecer orientaciones, alternativas y propuestas que permitan apoyar y acompañar a este cuerpo colegiado en su proceso de comprensión, apropiación y aceptación

de esta nueva responsabilidad (¿o no tan nueva?) con el fin de mejorar el nivel de madurez en la gestión y gobierno de los ciberriesgos, que habiliten a las empresas actuales para desplegar iniciativas innovadoras en sus procesos de transformación digital que cambien la forma de hacer las cosas y concreten nuevas experiencias en sus clientes (Cano, 2023).

En este sentido, este artículo inicia con una revisión de los fundamentos de las juntas directivas y su relación con el riesgo cibernético, para luego entrar en detalle en aquellas temáticas internacionales que son relevantes para dicho riesgo en las organizaciones. Seguidamente se explora el proceso de duelo que surge en estos cuerpos colegiados con ocasión de la responsabilidad que se les asigna a pesar de su poca experiencia y la negativa natural que surge, así como algunas ideas concretas para acompañarlos en este proceso. Finalmente se concluye con breves reflexiones que re-dondean las ideas planteadas a lo largo de este documento.

Fundamentos de las Juntas Directivas y el ciberriesgo

Las juntas directivas como cuerpos colegiados representan los órganos de gobierno naturales de las empresas (Calleja & Rovira, 2015).

Sus retos y responsabilidades implican condiciones particulares de sus participantes, que es necesario comprender y analizar con el fin de establecer puentes efectivos que permitan conversar y conectar en términos de sus intereses, exigencias y relaciones para hacer realidad la visión de una organización.

Por tanto, las juntas directivas cada vez más están expuestas a juicios de responsabilidad frente a eventos cibernéticos adversos que comprometan las operaciones de las organizaciones donde ellas operan, así como la promesa de valor para sus clientes. En este sentido, estos cuerpos colegiados deben desarrollar acciones concretas que les permitan mantener la confiabilidad, la vigilancia y la resiliencia de la organización en el contexto digital, como fundamento de su “debido cuidado” y demostración de su actuación deliberada y consciente frente a la inevitabilidad de la falla (Oktem, Pederson & Sallet, 2023).

En este escenario, los miembros de la junta deben asegurar que sus actuaciones son coherentes con esta realidad y dar cuenta de sus acciones respecto de estos eventos, para movilizar las acciones requeridas para proteger los intereses de la empresa y el cuidado de la imagen corporativa. Por consiguiente, cada miembro de la junta debe asegurar el cumplimiento de al menos cinco deberes (Frappolli, 2015, pp. 316-317) frente a la dinámica de las tensiones que provoca un ciberataque y las exigencias que la ciberseguridad demanda tanto para la organización como para sus ejecutivos de primer nivel:

- *Deber de cuidado*. Cada miembro de la junta debe mantenerse informado de los eventos y noticias relevantes sobre ciberseguridad o ciberataques, con el propósito de asegurar un tono adecuado de las discusiones en el contexto de los objetivos y estrategias de la organización.

- *Deber de lealtad*. Cada miembro de la junta no debe tener negocios o participar en negocios que compitan con la organización para la cual sirve, y más aún, comunicar situaciones adversas que conozca, las cuales afecten las condiciones de seguridad y control que tenga la empresa de la que es miembro en su directorio ejecutivo.

- *Deber de divulgación* (transparencia). Los miembros de la junta están obligados a revelar los hechos que son relevantes para los grupos de interés de la empresa para la cual trabajan. En particular, establecen el mecanismo y la estrategia que permiten dar cuenta de eventos desafortunados en ciberseguridad, con impactos en alguno de sus grupos de interés.

- *Deber de obediencia*. Los miembros de la junta deben ceñir sus actuaciones a la Constitución y la ley, así como frente a los fundamentos del gobierno corporativo. En otras palabras, asegurar las prácticas y los estándares requeridos para aumentar la resistencia de la empresa frente a ciberataques, así como motivar y apoyar comportamientos adecuados en el tratamiento de la información de la compañía.

- *Deber de verificación*. Los miembros de la junta deben contar con mecanismos para validar las acciones que sobre el tema de ciberseguridad se llevan a cabo en la empresa, motivar los planes de mejora que sean del caso y asegurar los recursos necesarios para incorporar las buenas prácticas en normativas, personas, procesos y tecnología.

Las juntas directivas y las áreas de riesgo cibernético

Los directorios comienzan a mantener en su radar las implicaciones y efectos nocivos de la materialización de los ataques cibernéticos. Las noticias permanentes de los impactos de los ciberataques en todo tipo de industria, así como las sanciones que revelan por cuenta de estos eventos, cada vez llaman la atención, no sólo por las posibles demandas o acciones legales que se puedan derivar, sino por el nivel de exposición que tiene la empresa a esta nueva realidad, que puede llevarla incluso a desaparecer del negocio (Myles, 2023).

En línea con lo anterior, la junta directiva debe mantener una visual de áreas clave susceptibles a los

riesgos cibernéticos, que puede concretar consecuencias adversas graves para dinámica empresarial. Las áreas donde se debe mantener el foco vigilante y sobremanera resiliente se ubican en:

- *Tensiones geopolíticas y cibernéticas globales y locales* - Para ello el equipo ejecutivo debe mantener y actualizar un diseño base de amenaza, que se traduzca en un análisis de escenarios posibles y probables de alto impacto.

- *Tratamiento de datos* – En esta temática el cuerpo colegiado debe asegurar un adecuado uso y explotación de datos con una visual de seguridad, privacidad y ética por defecto y desde el diseño.

- *Terceros de confianza* – La junta directiva deber conocer y asegurar la cadena de suministro y su relación con los objetivos del negocio para hacerla flexible, adaptable y resiliente frente a ciberataques.

- *Transformación digital* – El directorio debe definir y actualizar el apetito de riesgo corporativo frente a las iniciativas digitales estratégicas de la organización, para asegurar las capacidades cibernéticas necesarias para defender la promesa de valor de la empresa.

- *Cumplimiento normativo* – Los directores son particularmente sensibles al tema legal y normativo, por tanto deberán asegurar el cumplimiento de las exigencias de los reguladores locales e internacionales.

- *Brechas y vulnerabilidades* – Los miembros de junta deben comprender que no existe riesgo cero ni seguridad ciento por ciento. Por tanto, deben mantener una postura y protocolos concretos para atender una crisis cibernética, lo que exige desarrollar, ejecutar y aprender de simulaciones y ejercicios que revelen puntos ciegos en el modelo de seguridad y control de la organización.

Si bien pueden existir otras áreas que requieren atención frente al riesgo cibernético, las mencionadas previamente recogen las expectativas más sensibles y visibles de las organizaciones actuales, así como los efectos más adversos que pueden enfrentar las empresas y sus ejecutivos de primer nivel.

Por consiguiente, los equipos ejecutivos se sienten en una encrucijada que les genera tensiones y sentimientos encontrados, que se traducen en emociones y posturas que terminan generando rechazo y negación en la atención del riesgo cibernético y sus implicaciones empresariales.

Las junta directivas y el proceso de duelo frente a la responsabilidad del riesgo cibernético

Con el advenimiento de la formalización de las nuevas reglas de la Comisión del Mercado de Valores Norteamericano (SEC) sobre la ciberseguridad para las organizaciones que cotizan en bolsa donde entre otras normas se tienen: (Toscano, 2023)

- Notificar los incidentes de ciberseguridad importantes en un plazo de cuatro días laborables a partir de su detección y proporcionar actualizaciones periódicas sobre los incidentes de ciberseguridad notificados anteriormente.

- Divulgar las políticas y procedimientos mediante los cuales la organización identifica y gestiona los riesgos de ciberseguridad.

- Revelar cómo se consideran los riesgos cibernéticos como parte de la estrategia empresarial, la planificación financiera y la asignación de capital de la organización.

- Detallar la supervisión del riesgo cibernético por parte del consejo de administración, así como el papel de la dirección -y su experiencia- en la evaluación y gestión del riesgo cibernético y en la aplicación de políticas y procedimientos de ciberseguridad,las juntas directivas han entrado en tensiones y controversias comoquiera que estas nuevas responsabilidades (que no son tan nuevas) generan dinámicas distintas y exigencias que los cuerpos colegiados directivos no tienen en la actualidad, pues consideran que los temas de ciberseguridad son temas técnicos y procedimentales que no son de su nivel.

En este sentido, se podría decir que estos equipos viven un duelo, una pérdida irreparable que por exigencias de los supervisores deben ahora incorporar, muy a pesar de su negativa y posiblemente poca experiencia en el tratamiento de este tipo de riesgo de negocio en el contexto digital (Gorge, 2021).

De acuerdo con la psicología, "*la pérdida de cualquier objeto de apego provoca un duelo, si bien la intensidad y las características de éste pueden variar en gran medida en función del grado de vinculación emocional o de la propia naturaleza de la pérdida. Las pérdidas no siempre son físicas, sino que también pueden tener un carácter abstracto*" (Martin, 2019).

En este sentido, los directorios ejecutivos pierden la comodidad de su dinámica actual y conocida, para ser lanzados a entender, atender y asegurar un riesgo del cual poco se conoce y del cual poseen poca in-

formación, generando incertidumbre, dudas y miedos.

Para apoyar a los ejecutivos en su proceso de duelo, la literatura plantea dos alternativas para concretar el proceso cognitivo propio del estrés que esta nueva responsabilidad genera y las tensiones que puede suscitar en el ejercicio mismo de su función ejecutiva y directiva.

Lazarus y Folkman (1986) establecen dos modos de afrontamiento de la situación:

- *Dirigidos a la emoción* – regular las respuestas emocionales que surgen por causa del problema.

- *Dirigidos al problema* - buscar soluciones que reduzcan o desaparezcan el problema basado en un proceso analítico dirigido principalmente al entorno.

Una primera connotación del proceso de duelo de los directores frente al riesgo cibernético, el cual se percibe como una amenaza personal a su labor y posición ejecutiva, son las emociones que por lo general se producen entre las cuales se encuentran: *ansiedad*, *confusión* y *enojo*, las cuales surgen, entre otras, por la falta de conocimiento, información y manejo de una temática que resulta novedosa y que puede generarle afectaciones a su imagen, posición y capital político dentro y fuera de la organización.

Los ejecutivos de ciberseguridad frente este primer momento deben, con apoyo de un consultor externo, construir un entorno psicológicamente seguro, donde los directivos puedan liberarse de estas emociones y encontrar un escenario para poder preguntar sin temores, sin restricciones y de forma abierta, para conocer, explorar y aprender el tema, de tal forma que se liberen de sus propios miedos y se abran a construir en conjunto su propia versión de la temática situada en la realidad de la organización.

La segunda connotación para el tratamiento del duelo de los miembros de junta es trabajar dirigido al problema y los impactos que genera el asumir la responsabilidad del riesgo cibernético como son: *las sanciones*, *la pérdida de reputación* y *la pérdida de su posición*, las cuales se presentan por los efectos que se producen por cuenta de la materialización de un ciberataque, que termine no sólo afectando la dinámica de la empresa, sino comprometiendo datos sensibles y personales que generen grandes afectaciones a la corporación que sea referida a la falta de adecuada supervisión de dicho riesgo por cuenta de los miembros de junta.

Frente a esta forma de afrontamiento, los ejecutivos de ciberseguridad tienen una mayor participación comoquiera que demanda un proceso de compartir y conversar con los miembros de junta sobre los hechos y datos disponibles

en la compañía frente al tratamiento del riesgo cibernético. Esto es, construir, conversar y aprobar el nivel de apetito de riesgo de la empresa frente a dicho riesgos, desarrollar y desplegar el marco de debido cuidado necesario y establecer los acuerdos de nivel de protección que deberán ser supervisados de forma periódica e independiente, de tal manera que se interroguen todo el tiempo las capacidades de defensa y anticipación de la organización, así como la prácticas de protección y aseguramiento que tiene en la actualidad.

Reflexiones finales

El riesgo cibernético llegó a las organizaciones para generar incomodidad, incierto e inestabilidad, como una oportunidad para movilizar a las empresas de su zona cómoda y reconocer la nueva dinámica digital e interconectada de la sociedad y el mundo en general. Es el reconocimiento de los ecosistemas digitales de negocio tanto interno como externos para motivar transformaciones que cambien la dinámica de una industria y habiliten a las compañías para renovar y concretar ventajas competitivas en medio de zonas de inestabilidad y cambios permanentes (Woerner, Weill & Sebastian, 2022).

En este nuevo contexto, las juntas directivas deben actualizar su carta de navegación vigente y tradicional, basada en ejercicios de planeación estratégica y pronósticos de mercados en su sector de negocio, para reconocer una realidad cambiante, dinámica y exigente, que demanda una estrategia digital de las empresas, no sólo para acelerar sus iniciativas estratégicas, sino para tomar riesgos calculados que permitan cautivar a sus clientes y movilizar nuevas formas de monetizar el uso y explotación de los datos, consciente de la responsabilidad digital que implica ahora navegar en un entorno digital novedoso y particularmente volátil (Wucker, 2021).

Así las cosas, el riesgo cibernético se asoma y sitúa en la dinámica de la organización como un elemento intrínseco a su modelo de generación de valor, que es necesario comprender, atender y vigilar, comoquiera que se convierte en la piedra angular de las iniciativas que se van a desplegar en sus clientes, donde la confianza digital se revela como el referente natural de la relación de las compañías con sus consumidores. En este escenario, las juntas directivas deben conectar con esta nueva realidad, para asistir la empresa en el reto de aprovechar la oportunidad de una sociedad más digital e interconectadas (Brill, 2021).

El riesgo cibernético debe ser a las juntas directivas, como la promesa de valor de las empresas es a sus clientes. Esto es, una responsabilidad que se asume como parte natural e integral del compromiso del comprender, acompañar y responder a las expectativas y retos de los

consumidores cautivados por la manera que se provee de hacer las cosas de forma distinta. Por tanto, mientras se avanza en la solución del proceso de duelo de las juntas directivas frente a la responsabilidad del riesgo cibernético, es necesario avanzar en crear encuentros más constructivos y pedagógicos basados en un proceso cognitivo situado, para fundar las bases de un diálogo informado que haga del riesgo cibernético un reto para construir sinergias y no un juego de tensiones políticas.

Referencias

Agua, P. (2023). A Framework For Risk Governance. European Business Review. https://www.europeanbusinessreview.com/a-framework-for-risk-governance/

Brill, J. (2021). Rogue Waves. Future-proof your business to survive & profit from radical change. New York, USA: Mcgraw Hill

Brinson, R. & Briggs, R. (2023). Effective board governance of cyber security – A source of competitive advantage. Savanti Insight. https://info.savanti.co.uk/hubfs/Savanti%20Insight%20%20Effective%20Board%20Governance%20Of%20Cyber%20Security.pdf

Calleja, L. & Rovira, M. (2015). Gobierno institucional. La dirección colegiada. Navarra, España: EUNSA.

Cano, J. (2023). Maturity Model for Boards of Directors in Cyber Risk Governance. A Conceptual and Practical Proposal. En: Rocha, Á., Fajardo-Toro, C.H., Riola, J.M. (eds) Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies. Vol 328. 39–510. Springer, Singapore. https://doi.org/10.1007/978-981-19-7689-6_4

Frappolli, M. (2015). Managing cyber risk. Malvern, Pennsylvania. USA: American Institute for Chartered Property Casualty Underwriters.

Gorge, M. (2021). The cyber elephant in the boardroom. Cyber-accountability with the five pillars of security framework. Charleston, South Carolina, USA.: ForbesBooks.

Lazarus, R. & Folkman, S. (1986). Estrés y procesos cognitivos. España: Martínez Roca.

Martin, E. (2019). Las 5 fases (o etapas) del duelo: la teoría de Kübler-Ross. https://centrodepsicologiaintegral.com/las-5-fases-o-etapas-del-duelo-la-teoria-de-kubler-ross/

Myles, D. (2023). Waking up to cyber risks. FDI Intelligence. https://www.fdiintelligence.com/content/feature/waking-up-to-cyber-risks-83005

Oktem, C., Pederson, K. & Sallet, J. (2023). How boards can support resiliency in the face of constant crisis. EY Board Matters. https://shorturl.at/uHMO2

Sardar, Z. (2010). Welcome to postnormal times. Futures. 42(5). 435–444. doi:10.1016/j.futures.2009.11.028

Toscano, J. (2023). Final Decision On SEC's Cybersecurity Disclosure Rules Pushed To October. Forbes. https://www.forbes.com/sites/joetoscano1/2023/07/02/final-decision-on-secs-cybersecurity-disclosure-rules-pushed-to-october-2023/

Woerner, S., Weill, P. & Sebastian, I. (2022). Future ready. The four pathways to capturing digital value. Boston, MA. USA: Harvard Business Review Press

Wucker, M. (2021). *You are what you risk. The new art and science of navegating an uncertain world*. New York, USA: Pegasus Book

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, 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–.*