El papel del Consejo ante la presión tecnológica

"Decisiones que impacten en sistemas, datos o algoritmos son más que instrumentales y deben llevarse al Consejo. Independientemente de la confianza en la gestión".

¿Y si correr por decidir fuera la peor estrategia? ¿Y si lo urgente nos hiciera perder lo importante? En la mesa del consejo de administración se toman decisiones de máxima exigencia financiera y donde el rigor debe estar igual de presente que la estrategia. Una adecuada gestión del riesgo requiere visión, criterio y una lectura integral del contexto empresarial, de los competidores directos e indirectos y del mercado en el que operamos. Entre los asuntos prioritarios y de forma cada vez más apabullante, encontramos la gobernanza de la tecnología (muy especialmente, de la inteligencia artificial). Más allá del cliché de que se trata de asuntos técnicos o del estereotipo de que estamos ante factores operativos, los líderes de las organizaciones deben comprender que estamos ante el epicentro del buen gobierno. La tecnología está en todo y su gobernanza exige mecanismos sólidos de supervisión y control, habilitadores, para empujar con criterio, espolear el avance y, a la vez, para tener una mejor capacidad de evaluar adecuadamente frente al empuje de soluciones aparentemente inmediatas e incluso ofrecidas como infalibles. Gobernar requiere comprender qué sistemas se están utilizando, con qué proveedores, bajo qué condiciones contractuales, con qué finalidad y con qué implicaciones. En el caso de la inteligencia artificial, se traduce en refuerzo de la explicabilidad de los modelos y su trazabilidad, esto es, que se entiendan y se puedan seguir. Con estructuras internas que tiendan puentes entre los departamentos de tecnología, legal, ventas y auditoría, y un control interno que eleve el listón, desde el mensaje de que el cumplimiento normativo es innegociable y viene en forma de tsunami de referencias regulatorias.

A estas alturas, resulta insuficiente limitarse a saber que existen controles. Hace falta conocer cuándo se han realizado las auditorías, en qué contexto, con qué alcance y cuáles han sido sus conclusiones. Y, a partir de ahí, realizar una valoración efectiva del riesgo, con un cierto nivel técnico, sí, pero ante todo estratégico, y sin perder de vista las tensiones que pueden generar problemas reputacionales. Complicaciones que llegan por prácticas de alto riesgo, como todo lo que tiene que ver con automatismos en los procesos de selección de personal o los sistemas de 'scoring' crediticio; y problemas severos que llegan por las prácticas prohibidas expresamente en entornos como el de la Unión Europea, donde el 'social scoring' (puntuación ciudadana general) o la explotación de las personas más vulnerables son consideradas inadmisibles. La presión tecnológica ha dejado de ser coyuntural y la mentalidad digital es clave en los órganos de gobierno para ejercer adecuadamente la función de supervisión, por convicción y por obligación. Debe comprenderse que las decisiones que impactan en sistemas, datos o algoritmos son más que meramente instrumentales, y deben elevarse al nivel del consejo. Independientemente de la confianza en la gestión, afectan directamente a la capacidad de la organización para cumplir su propósito, proteger a sus grupos de interés y responder ante accionistas, reguladores y ante la sociedad en su conjunto en los sectores más estratégicos. Gobernar exige formular las preguntas relevantes, más que recibir respuestas a las preguntas de otros. Pensar en el impacto de la tecnología implica ir más allá del corto plazo y exigir indicadores que orienten decisiones bien informadas, que miren al medio y largo plazo. La innovación necesita respaldo y guía, y decidir hasta dónde está dispuesta a llegar la organización en materia de riesgo y qué niveles son realmente asumibles es algo que compete a los máximos órganos de gobierno (sin un seguidismo que sea temerario para la marcha del negocio).

"El Reglamento Europeo de Ciberresiliencia, que tiene efectos plenos previstos para 2027, añade exigencias que miran a todo el ciclo de vida del producto digital, para elevar la exigencia en el diseño"

Una de las principales misiones a las que se debe el consejo es a la anticipación de las circunstancias que puedan acontecer. Entre ellas, qué

sucede cuando la inteligencia artificial tiene un impacto directo sobre el empleo, las condiciones laborales, las capacidades internas o la retención del talento. ¿Cómo navegamos cuando la cultura corporativa se ve tan impactada por el entorno digital? Si hablamos de tecnología a nivel internacional, el panorama regulatorio se encuentra en plena efervescencia, con más de mil iniciativas solo sobre inteligencia artificial. Y en tanto que los nuevos desarrollos pueden estar condicionados por el entorno de regulación, las diferentes normativas deben ser asimiladas desde el comienzo, por su incidencia en todos los ámbitos: desde la importancia de la protección de datos a los límites para operar en cada mercado. Las normas contribuyen a elevar los estándares de las compañías. Y tener visión de hacia dónde van es muy importante en un contexto de mercados globales, cadenas de valor interconectadas y proveedores tecnológicos transnacionales. Por ejemplo, muy relevante para sortear la vulnerabilidad, llegado el caso, por depender de servidores ubicados en países con turbulencias.

La evolución del ordenamiento es especialmente relevante para los consejos de administración. En Europa, en materia de ciberseguridad y resiliencia digital, la Directiva NIS2 refuerza las obligaciones de aquellas empresas consideradas más importantes (respecto a su antecesora NIS de sistemas de redes e información o 'Network and Information Systems'). Tiene como finalidad que las infraestructuras críticas y los servicios 'esenciales' estén garantizados, en un escenario de crecientes amenazas. A su vez, el Reglamento Europeo de Resiliencia Operativa Digital ('Digital Operational Resilience Act' o DORA) viene a robustecer la perspectiva de aguante, tan relevante en los sectores más regulados y con efectos ramificados a lo largo y ancho del mapa empresarial. Se evalúa nuestra capacidad de resistencia, de respuesta y de recuperación ante incidentes tecnológicos, y esto es determinante para la continuidad del negocio y para el buen hacer del consejo de administración. Un consejo que, más que pensar en cómo evitar lo inevitable, debe liderar la aprobación de planes de previsión y respuesta, de crisis.

El Reglamento Europeo de Ciberresiliencia ('Cyber Resilience Act'), que tiene efectos plenos previstos para 2027, añade exigencias que miran a todo el ciclo de vida del producto digital, para elevar la exigencia en el diseño. Tiene un impacto directo en las decisiones de qué proveedor elegir en cada momento, las decisiones de compra y de desarrollo y todo el esquema de supervisión por parte del consejo. El Reglamento de Auditoría Legal y la trasposición de la Directiva previa concretan obligaciones y responsabilidades. En España o en Francia, la dirección es la de un refuerzo del deber de diligencia. Pensemos en la Ley de Coordinación y Gobernanza de la Ciberseguridad (trasposición de la NIS2) y cómo consolida el esquema ordenado de notificación y gestión de incidentes, con un papel relevante para el Centro Nacional de Ciberseguridad. En Francia, la ambición la vemos al integrar NIS2, CER ('Critical Entities Resilience' Directive', directiva europea sobre resiliencia de entidades críticas) y DORA, en un mismo proyecto de ley de resiliencia de las infraestructuras críticas y de ciberseguridad.

En paralelo, el supervisor ve una responsabilidad ineludible de los consejos de administración. En España, desde la misma Guía Técnica 1/2024 de la CNMV se aprecia un enfoque de vigilancia, que apunta a que las comisiones de auditoría tienen encomendada la ciberseguridad. Al final, para dejar claro que ni la tecnología es un asunto colateral ni tampoco lo son los retos derivados de su uso. El buen juicio conlleva ir más allá de lo burocrático y tener en la mira, de manera permanente, la protección y defensa de los accionistas y del resto de grupos de interés. Entre los fundamentos del liderazgo tecnológico tenemos la exigencia de capacidad de reconstruir los procesos de decisión, la asignación de responsabilidades y, siempre, la rendición de cuentas. Vivimos en un mundo enormemente complejo, de colaboración público-privada sumamente necesaria para que un futuro de mejora se materialice. Donde el liderazgo, con valores, requiere como nunca una visión global de las tendencias que vienen y los retos que acechan. Desde ese conocimiento ampliado, surgido de combinar lo local con lo global, los consejos estarán en mejor posición para reconocer los límites y dirigir el paso en el camino de gobierno. ■

"En la NIS2, que refuerza las obligaciones de las empresas con infraestructuras críticas o servicios esenciales. En el DORA, que evalúa nuestra capacidad de resistencia... El supervisor ve una responsabilidad ineludible en los consejos. En España, desde la Guía Técnica 1/2024 de la CNMV se apunta que las comisiones de auditoría tienen encomendada la ciberseguridad"

* Consejero independiente y patrono, autor del libro *Gobernar con lo que viene* (LID Editorial 2026).