

esade

Center for Corporate Governance

IBM

Soberanía Digital y Resiliencia Estratégica: La Nueva Agenda del Consejo

Noviembre 2026

Do Good. Do Better.

esade

Center for Corporate Governance

Esade Centro de Gobierno Corporativo:

Mario Lara Sanz
Director del Esade Center for Corporate Governance y Director de Esade Madrid

Nestor U. Salcedo
Investigador postdoctoral en Esade Center for Corporate Governance

IBM:

Belén Martín
Senior Partner y Vicepresidente, líder del Sector Banca y Seguros, España, Portugal, Israel y Grecia de IBM Consulting

Miguel Ángel Morcuende
Associate Partner, Board Ambassador de IBM Consulting

Coordinación y enriquecimiento del informe:

Maite Arcos
Consejera independiente en Enagás; directora general de la Fundación ESYS y miembro del Advisory Group de ENISA

Consejeros participantes en el informe:

Emma Fernández
Consejera independiente de 74Software, Iskaypet, Metrovacesa y Openbank; miembro del Consejo Asesor del Centro de Gobierno Corporativo de Esade

Iván Martén
Consejero independiente de Repsol; presidente de Orkestra y patrono de Tecnalia y Fundación Esade

Juan Antonio Zufiria
Presidente del Patronato de la Fundación Bankinter para la Innovación; consejero de Bankinter; vicepresidente de la Real Academia de Ingeniería de España y exvicepresidente sénior de IBM

CENTRO DE GOBIERNO CORPORATIVO

El Centro de Gobierno Corporativo se crea con el objetivo de convertirse en un referente en el ámbito de Gobierno Corporativo en España que contribuya a la mejora del buen gobierno en las empresas e instituciones. Un Centro que aborde de forma integral los nuevos retos a los que se enfrenta el Gobierno Corporativo, combinando su acción desde la investigación, el debate social y la influencia en los *policy makers*, hasta la formación de los consejeros en las mejores prácticas y tendencias, así como la creación de comunidad con los antiguos alumnos.

IBM

© 2026 by Esade Center for Corporate Governance
Fuencarral - El Pardo, 28034, Madrid

Todos los derechos reservados
Impreso en España
Primera impresión octubre 2026

esadeccg@esade.edu

Esade Centro de Gobierno Corporativo:

La aceleración tecnológica, la fragmentación geopolítica y geoeconómica, el creciente uso de restricciones comerciales y tecnológicas como instrumentos de poder, y la creciente concentración de capacidades digitales críticas están transformando las condiciones en las que las empresas compiten y crean valor. La IA, los datos, la nube, las plataformas, los semiconductores, la energía y el talento especializado ya no constituyen únicamente recursos tecnológicos: son capacidades estratégicas cuya disponibilidad, control y posibilidad de sustitución pueden determinar la continuidad, la adaptación y la competitividad futura de la organización.

Desde la perspectiva del Centro de Gobierno Corporativo de Esade, este cambio afecta directamente a tres dimensiones de la actuación de los Consejos de Administración: su **agenda**, su **rol** y **perfil**, y su **efectividad** en la orientación y supervisión de la creación de valor.

En primer lugar, **se amplía la agenda del Consejo**. La transformación digital ya había situado la inteligencia artificial, la ciberseguridad y la geopolítica entre los asuntos recurrentes y transversales de los órganos de gobierno. El nuevo escenario exige añadir una cuestión más amplia: la capacidad de la empresa para gobernar las dependencias digitales sobre las que se sustenta su estrategia. El Consejo debe comprender qué datos, modelos, infraestructuras, proveedores, jurisdicciones y fuentes de conocimiento son críticos; quién conserva los derechos efectivos de decisión sobre ellos; y qué acontecimientos podrían restringir su acceso, elevar su coste o comprometer su disponibilidad. La soberanía digital deja así de ser un debate tecnológico o institucional para convertirse en una cuestión de estrategia, riesgo, inversión y competitividad empresarial.

En segundo lugar, **evoluciona el rol del Consejo y el perfil de los consejeros**. El Consejo no debe gestionar la tecnología ni sustituir a la dirección ejecutiva, pero sí evaluar, orientar y supervisar las decisiones digitales con impacto material sobre el modelo de negocio. Esto exige consejeros capaces de comprender las implicaciones estratégicas, regulatorias, éticas y geoeconómicas de las tecnologías; cuestionar la concentración de proveedores y la reversibilidad de las decisiones; valorar si la empresa conserva alternativas viables; y exigir una asignación clara de responsabilidades. Como ya se planteó en la Guía de Consejeros para una IA ética, el consejero debe combinar criterio estratégico con capacidad para supervisar transparencia, responsabilidad y rendición de cuentas. El nuevo reporte amplía este precepto: además de gobernar el uso responsable de la tecnología, debe vigilar que su adopción no erosione la libertad futura de actuación de la organización.

En tercer lugar, **la soberanía y la autonomía digitales inciden en la efectividad y el desempeño del propio Consejo**. Un Consejo eficaz no es aquel que recibe más información tecnológica, sino aquel que transforma esa información en deliberaciones y decisiones de mayor calidad. Para ello necesita identificar señales tempranas, contrastar escenarios, cuestionar los supuestos de la estrategia y supervisar si la organización puede mantener sus funciones esenciales, sustituir capacidades críticas y reconfigurar recursos cuando cambian las condiciones. La información debe presentarse de manera comprensible, material y orientada a decisiones, evitando tanto la delegación completa en especialistas como la entrada del Consejo en la gestión operativa.

Este informe propone ordenar esa supervisión mediante tres conceptos relacionados. La soberanía digital representa el control efectivo que conserva la organización sobre las capacidades digitales críticas de las que depende su estrategia. La autonomía digital refleja su libertad real para operar, sustituir, reconfigurar y evolucionar cuando una dependencia cambia sus condiciones o deja de estar disponible. Ambas contribuyen a la resiliencia estratégica, entendida como la capacidad de anticipar cambios relevantes, afrontar sus efectos, adaptar la organización y preservar o renovar la creación de valor. No se trata de eliminar todas las dependencias ni de perseguir una autosuficiencia incompatible con una economía interconectada, sino de conocerlas, gobernarlas y evitar que se conviertan en vulnerabilidades críticas para la organización.

Para facilitar esta labor, el documento plantea un modelo de resiliencia estratégica para Consejos de Administración, un marco inicial de evaluación, un dashboard y una batería de preguntas orientadas a la deliberación. Estas herramientas pretenden reforzar la conexión entre estrategia, riesgos, capacidades, responsabilidades e inversiones, y mejorar la calidad de la interacción entre el Consejo, sus comisiones y la alta dirección.

La cuestión de fondo no es, por tanto, únicamente qué tecnologías debe adoptar la empresa, sino en qué condiciones, bajo qué dependencias y con qué capacidad futura de decisión. Desde la perspectiva del buen gobierno, la prueba definitiva será si el Consejo está contribuyendo a que la organización pueda seguir decidiendo, operando y creando valor cuando cambien las reglas del juego.

ÍNDICE

1 Resumen Ejecutivo

2 La Soberanía Digital entra en el Consejo

3 Soberanía y Autonomía: Los pilares de la Resiliencia Estratégica

4 Mapa Regulatorio

5 Resiliencia Estratégica para el Consejo

6 Cómo supervisar la Resiliencia Estratégica desde el Consejo

7 Un sistema de supervisión de la Resiliencia Estratégica

8 Conclusiones

9 Bibliografía

1. Resumen Ejecutivo

Durante décadas, las organizaciones han competido a través de la escala, la eficiencia y la innovación. Sin embargo, la creciente digitalización de la economía está incorporando un nuevo factor de competitividad: **la capacidad para mantener la independencia sobre aquellas capacidades críticas de las que depende el negocio.**

La inteligencia artificial, la nube, los datos, los semiconductores, la energía o el talento especializado se han convertido en activos estratégicos. Al mismo tiempo, la concentración de estas capacidades en un número reducido de proveedores, países y ecosistemas tecnológicos está generando nuevas dependencias que afectan directamente a la capacidad de las organizaciones para operar, innovar y crecer.

Este fenómeno está desplazando la conversación desde la gestión tecnológica hacia el gobierno corporativo. La cuestión ya no es qué tecnologías utiliza una empresa, sino hasta qué punto conserva libertad de actuación cuando cambian las reglas del juego y puede condicionar decisiones estratégicas o puede implicar impactos muy relevantes en su cuenta de resultados. La gestión de estas dependencias deja de ser una cuestión operativa para convertirse en una responsabilidad directa del Consejo de Administración.

Los Consejos de Administración están comenzando a familiarizarse con conceptos como la **soberanía digital** [1] [2] o la **autonomía estratégica** [3]. Sin embargo, ninguno de ellos responde por sí solo a la pregunta que realmente importa: **¿Seguirá siendo capaz la organización de decidir, operar y crear valor cuando cambien las condiciones del entorno?**

Para responder a esta cuestión, proponemos considerar un marco más amplio: la **Resiliencia Estratégica** [4], [5] y [6]. Un concepto que integra la **soberanía** —el control sobre las capacidades críticas— y la **autonomía** —la capacidad de adaptación— en una única visión orientada a la creación de valor y a la toma de decisiones del Consejo.

La tesis de este documento es sencilla:

01 **La soberanía proporciona libertad de decisión.**

02 **La autonomía aporta capacidad de adaptación.**

03 **La combinación de ambas constituye la base de la resiliencia estratégica.**

Este desafío resulta especialmente relevante para Europa y sus empresas, que mantienen dependencias significativas en ámbitos como la nube, los semiconductores, la inteligencia artificial o el software avanzado. Más allá de una cuestión tecnológica, estas dependencias afectan directamente a la competitividad, la resiliencia y la seguridad económica de empresas e instituciones.

En las páginas siguientes analizaremos cómo estos conceptos se relacionan entre sí, cuál es el papel del Consejo de Administración en su supervisión y qué herramientas pueden utilizarse para evaluarlos y fortalecerlos. Porque, en última instancia, la cuestión de fondo es sencilla: **¿Seguiremos siendo capaces de decidir, operar y crear valor cuando cambien las reglas del juego?**

2. La Soberanía Digital entra en el Consejo

La soberanía siempre ha estado asociada a la capacidad de mantener la libertad de elección sobre aquello que resulta esencial. En el ámbito empresarial, significa preservar la capacidad de decidir, operar y competir sin que dependencias externas comprometan la continuidad del negocio, la creación de valor o el cumplimiento de las obligaciones regulatorias.

En el entorno digital, este principio se extiende a los activos tecnológicos críticos: datos, inteligencia artificial, infraestructuras, plataformas y cadenas de suministro digitales. La soberanía digital no es una cuestión técnica ni una aspiración de autosuficiencia tecnológica. Es la capacidad de una organización para mantener la capacidad de decisión efectiva sobre estos activos y garantizar que siguen estando disponibles, protegidos y que contribuyen a los objetivos del negocio.

La creciente dependencia de capacidades tecnológicas críticas está ampliando el ámbito tradicional de responsabilidad de los Consejos de Administración. Junto al crecimiento, la rentabilidad y la gestión del riesgo emergen nuevas responsabilidades relacionadas con la resiliencia, la seguridad económica, la transición energética y la capacidad de decisión en un entorno cada vez más digital e interdependiente. Hoy, muchas organizaciones descubren que parte de su libertad de elección depende de proveedores, jurisdicciones o ecosistemas tecnológicos sobre los que tienen una influencia limitada.

Bien es cierto que esas dependencias no son un fenómeno nuevo. Desde que se creó el intercambio y el comercio, que son la base de la riqueza de las naciones [7] (como bien decía Smith) los países más avanzados abandonaron la aspiración a la autarquía y comenzaron a depender de forma creciente del comercio internacional como motor de crecimiento económico, gracias a la especialización de los países. Ha ocurrido a lo largo de la historia con la extracción de materias primas (caucho y petróleo) o tecnologías (máquina de vapor, electricidad, motor de explosión…). Y eso nos demuestra que el desarrollo no proviene solo de la posesión y control de estos elementos clave, sino de su uso y aplicación para generar riqueza.

Es cierto que la posesión de materias primas, como por ejemplo el petróleo, concede un poder de negociación enorme a aquellos que lo poseen. Pero también es cierto que cuando no ha sido posible la posesión y el control de esas materias primas (por motivos ineludibles, como la propia geología), la respuesta óptima de gestión del riesgo en las empresas y en los países ha sido diversificar las fuentes de aprovisionamiento de esos recursos clave para reducir el poder y la dependencia de cada uno de los países productores a nivel individual y mitigar de esa manera el riesgo de dependencia.

Esta es una enseñanza de la historia que no debemos dejar de lado cuando hablamos de soberanía digital, especialmente cuando debemos tomar decisiones en el corto plazo que hacen imposible disponer de ciertas capacidades cuya réplica exige una duración de tiempo o un volumen de inversión inalcanzable a corto plazo.

Cuanto mayor es la dependencia, menor es la libertad para responder ante cambios regulatorios, comerciales o tecnológicos o incluso una mezcla de estos, como son las decisiones gubernamentales de prohibir a las empresas del país, o limitar, la exportaciónde ciertos chips o modelos de IA.

Por ello, la soberanía digital debe entenderse como una palanca de resiliencia y competitividad [8]. No se trata de eliminar dependencias (algo imposible en una economía global e interconectada), sino de comprenderlas, gestionarlas y mantener capacidad real de elección cuando cambian los equilibrios tecnológicos, regulatorios, geopolíticos o geoeconómicos.

En este documento distinguimos entre factores **geopolíticos** y **geoeconómicos**. Los primeros hacen referencia a las dinámicas de influencia entre Estados, jurisdicciones y bloques económicos. Los segundos hacen referencia a las dependencias económicas, industriales, tecnológicas y energéticas que condicionan la competitividad y la capacidad de actuación de las organizaciones. Ambos tipos de factores influyen directamente sobre la resiliencia estratégica. La combinación de **riesgos geopolíticos** y **geoeconómicos** está configurando un nuevo conjunto de **riesgos geoestratégicos** que los Consejos de Administración deben comprender y supervisar.

Esta reflexión sobre la soberanía resulta especialmente relevante para Europa. La dependencia [9] en ámbitos como la nube, la inteligencia artificial [10], los semiconductores o el software avanzado no constituye únicamente una brecha tecnológica; en caso de que el riesgo de dependencia no sea bien gestionado también condiciona la capacidad de competir, innovar y capturar el valor generado por la digitalización.

Para los Consejos de Administración, esto supone una ampliación de las obligaciones de gestión de los riesgos de la compañía. La conversación ya no debe centrarse únicamente en tecnologías, proveedores o inversiones digitales en función de su productividad, sino en comprender qué dependencias son estratégicamente aceptables y cuáles pueden comprometer la capacidad futura de la organización para ejecutar su estrategia, adaptarse al cambio y preservar su libertad de actuación. La cuestión para los directivos ya no es únicamente qué tecnologías adoptar, sino en qué condiciones, con qué dependencias, con qué riesgos y con qué grado de autonomía [11].

La soberanía digital no consiste en poseer la tecnología. Consiste en preservar la libertad de decisión y la capacidad de elección cuando se transforman las circunstancias sobre las que se sustenta el negocio. Sin embargo, el control por sí solo no garantiza la capacidad de adaptación necesaria para responder a un entorno cambiante. Por ello, **los Consejos de Administración deben complementar la soberanía con la autonomía, construyendo así las bases de una verdadera resiliencia estratégica.**

Por ello, la pregunta fundamental que debería plantearse cualquier Consejo es: **¿Hasta qué punto limita el margen de maniobra de la empresa el acceso a las capacidades de las que dependerá nuestro futuro?** Si la respuesta no es clara, la soberanía digital ha pasado a ser una prioridad de gobierno corporativo.

> Existe un gran peligro en confundir soberanía digital con algún tipo de proteccionismo o subvención de campeones nacionales. Por el contrario, la soberanía se identifica con la capacidad de elección, el margen de maniobra que mantiene una empresa o un país a la hora de tomar sus decisiones sin condicionantes externos. Y a menudo esa mayor independencia se consigue simplemente diversificando las fuentes de suministro, las vías de aprovisionamiento para no generar dependencias excesivas, también en el terreno de la digitalización. Ese es el camino para conciliar soberanía y competitividad.
>
> **Maite Arcos**, Consejera Independiente en ENAGAS,
> Directora General de la Fundación ESYS y miembro del Advisory Group de ENISA

3. Soberanía y Autonomía: Los pilares de la Resiliencia Estratégica

Los conceptos de **soberanía digital** y **autonomía digital** suelen utilizarse como sinónimos, aunque responden a preguntas diferentes y tienen implicaciones distintas para los Consejos de Administración.

La **soberanía digital** se refiere a la capacidad de mantener la libertad de decisión respecto al modo de integración de tecnologías digitales y de los activos digitales críticos de una organización — datos, infraestructuras, plataformas, inteligencia artificial, proveedores o procesos tecnológicos — y garantizar que continúan alineados con sus objetivos estratégicos. En esencia, responde a una pregunta sencilla: **¿Se podrá elegir libremente cuando cambian las condiciones?**

Por su parte, la **autonomía digital** hace referencia a la capacidad de operar, innovar y evolucionar con una menor dependencia de terceros. El concepto procede de la noción más amplia de autonomía estratégica, ampliamente desarrollada por instituciones europeas y centros de pensamiento [12]. Su foco no está en el control, sino en la ejecución. **¿Hasta qué punto dependemos de otros para competir y operar? ¿Está esa dependencia en el nivel de riesgo que se ha decidido asumir, o es necesario adoptar medidas para gestionarlo y adaptarlo al nivel de apetito al riesgo decidido por el Consejo?**

La Comisión Europea, a través de iniciativas como el paquete europeo de Soberanía Tecnológica [13], junto con propuestas como EuroStack [14] considera que ambas dimensiones son esenciales para reforzar la competitividad [15], la resiliencia y la seguridad económica europeas.

La siguiente figura muestra cómo la **soberanía digital** y la **autonomía digital** responden a desafíos distintos pero complementarios, constituyendo conjuntamente la base de la resiliencia estratégica.



Fig 1. Soberanía Digital, Autonomía Digital y Resiliencia Estratégica
La resiliencia estratégica surge de la combinación entre libertad de decisión y capacidad de adaptación.

3.1 La soberanía no exige propiedad

Uno de los errores más frecuentes consiste en asociar soberanía con propiedad. Sin embargo, una organización no necesita poseer toda su infraestructura tecnológica para mantener un elevado grado de soberanía digital. Lo relevante no es quién es propietario de la tecnología, sino quién conserva la capacidad de decisión y de actuación cuando se produce una interrupción, una crisis política o un cambio regulatorio. Este matiz es relevante en el ámbito digital. En muchos casos, la infraestructura tecnológica puede no estar necesariamente en riesgo. Por ejemplo, los centros de datos de nube pueden estar ubicados dentro del territorio nacional o europeo y seguir plenamente operativos. Sin embargo, los servicios asociados a esa infraestructura pueden depender de compañías privadas sujetas a jurisdicciones, regulaciones y obligaciones que pueden cambiar con el tiempo. Estas circunstancias pueden limitar la capacidad de la organización para operar o adaptarse y provocar impactos significativos sobre la cuenta de resultados. Por ello, la soberanía exige preservar un grado suficiente de **opcionalidad estratégica** que permita reubicar, sustituir o reconfigurar capacidades digitales críticas cuando las condiciones lo requieran.

Una organización puede utilizar servicios de terceros y mantener un elevado grado de soberanía si conserva capacidad de elección, evita dependencias que conllevan un nivel de riesgo de dependencia superior al elegido conscientemente y dispone de alternativas viables ante situaciones de concentración o bloqueo tecnológico. Por el contrario, una organización puede disponer de tecnología propia y seguir siendo vulnerable si depende de una única plataforma, proveedor o jurisdicción para operar.

3.2 Del control tecnológico a la libertad de decisión

La soberanía digital no debe interpretarse como una aspiración de autosuficiencia tecnológica. La OCDE [16], la Comisión Europea [17] y el Informe Draghi [15], coinciden en que ninguna economía moderna puede aspirar a la independencia absoluta. El objetivo no es eliminar las dependencias, sino reconocerlas, comprenderlas y evitar que se conviertan en vulnerabilidades críticas para la organización.

La soberanía no equivale a autarquía. En una economía interdependiente, el reto no es producirlo todo, sino mantener capacidad de elección, diversificar riesgos y gestionar dependencias con criterio [18]. La soberanía no implica aislamiento; implica la capacidad de adaptarse sin perder supervisión ni capacidad de actuación.

Desde la perspectiva del Consejo, la soberanía digital no se mide por el grado de control sobre la tecnología, sino por la capacidad de mantener opciones disponibles cuando cambian las circunstancias.

Una organización soberana no es aquella que no depende de nadie, sino aquella que conoce sus dependencias, las gobierna activamente y mantiene capacidad real de elección. Esta capacidad de elección no siempre está garantizada. Según IBM, el **71% de los directivos** considera que tendría dificultades para **sustituir su principal proveedor o modelo de inteligencia artificial** si tuviera que hacerlo hoy, lo que pone de manifiesto hasta qué punto determinadas dependencias tecnológicas pueden limitar la autonomía efectiva de las organizaciones **ante cambios significativos en su contexto operativo** [19].

Como señalan diversos análisis recientes, la soberanía debe entenderse como un espectro y no como una condición absoluta. Las organizaciones necesitan equilibrar independencia, flexibilidad, coste y resiliencia en función de la criticidad de cada capacidad [20].

Por ello, la pregunta relevante para cualquier Consejo no es si utiliza tecnología propia o de terceros, sino: **¿Conservamos la capacidad de decidir, operar y competir si una dependencia crítica deja de estar disponible o cambia sus condiciones?**

3.3 De la Soberanía y la Autonomía a la Resiliencia Estratégica

Ni la soberanía ni la autonomía son suficientes por sí solas. Una organización puede mantener un elevado margen de maniobra sobre sus capacidades críticas y, sin embargo, carecer de la flexibilidad necesaria para adaptarse a una disrupción significativa. Del mismo modo, una organización puede operar con gran autonomía y seguir siendo vulnerable si no controla adecuadamente los activos sobre los que sustenta su actividad.

Por ello, los Consejos de Administración deben considerar ambos conceptos como capacidades complementarias. La soberanía aporta poder de decisión estratégico. La autonomía proporciona capacidad de adaptación. La combinación de ambas constituye la base de la **resiliencia estratégica** [4], [5] y [6]: la capacidad de preservar la continuidad, adaptarse al cambio y conservar el control cuando cambian las condiciones del entorno.



Fig 2. Soberanía Digital, Autonomía Digital y Resiliencia Estratégica
La resiliencia estratégica combina libertad de decisión y capacidad de adaptación.

La soberanía digital y la autonomía digital constituyen capacidades complementarias. La primera proporciona libertad de decisión; la segunda, capacidad de adaptación. Juntas permiten construir la resiliencia estratégica sobre la que se sustenta la continuidad, la competitividad y la creación de valor.

> "Soberanía digital es preservar la capacidad de decisión. El Consejo debe conocer y evaluar los niveles de dependencia tecnológica de la organización y establecer alternativas, planes de sustitución y estrategias de salida ante la concentración de proveedores críticos y los riesgos derivados de tensiones geopolíticas."
>
> **Emma Fernández**, consejera independiente de 74Software, Iskaypet, Metrovacesa y Openbank y miembro del Consejo Asesor del Centro de Gobierno Corporativo de Esade

4. Mapa Regulatorio

La soberanía digital se ha convertido en una prioridad estratégica para Europa, impulsando una agenda regulatoria orientada a reforzar la resiliencia, la competitividad y la autonomía tecnológica del continente. Para las organizaciones, esta evolución traslada el debate desde el ámbito del cumplimiento normativo hacia una cuestión más amplia de gobierno corporativo y resiliencia estratégica. Asimismo responde a una realidad cada vez más evidente: la dependencia de capacidades tecnológicas críticas desarrolladas fuera de Europa en ámbitos como la nube, la inteligencia artificial, los semiconductores, el software avanzado o las infraestructuras digitales y las experiencias en momentos de ruptura de flujos, como ocurrió en la pandemia o más recientemente, ante decisiones en las que se mezclan la geopolítica con la guerra comercial y se materializan en prohibiciones o limitaciones a las exportaciones de elementos tecnológicos como los chips o los modelos de IA frontera.

4.1 España: la aplicación práctica de la agenda europea

España ha alineado su estrategia digital con las prioridades impulsadas por la Unión Europea mediante iniciativas como la Agenda España Digital [21], la Estrategia Nacional de Inteligencia Artificial (ENIA) [22], la Estrategia Nacional de Ciberseguridad, incluida dentro del Plan Industrial y Tecnológico para la Seguridad y la Defensa [23] y la creación de la Agencia Española de Supervisión de Inteligencia Artificial (AESIA) [24].

Desde la perspectiva empresarial, el mensaje es claro: la digitalización ya no se limita a la incorporación de tecnología. También exige fortalecer la gobernanza de la inteligencia artificial, la ciberresiliencia, la protección de datos y la gestión de dependencias tecnológicas críticas.

4.2 Europa: de la regulación a la Soberanía Digital

Europa ha demostrado históricamente una gran capacidad para establecer estándares regulatorios globales, como ocurrió con el Reglamento General de Protección de Datos (GDPR) [25]. Sin embargo, la agenda actual va más allá del cumplimiento normativo. Iniciativas como el mencionado paquete europeo de Soberanía Tecnológica [13], el Programa de Europa Digital [26], la iniciativa EuroStack [14], la Ley de Chips [27] o las nuevas inversiones en capacidad computacional e inteligencia artificial [28] reflejan una ambición común: reforzar las capacidades tecnológicas europeas y reducir dependencias estratégicas en ámbitos críticos.

Esta evolución amplía el debate sobre soberanía digital más allá de la protección de datos o la regulación tecnológica. Iniciativas como EuroStack en Europa o India Stack [29] en India reflejan aproximaciones diferentes a un mismo desafío: cómo reforzar la facultad de decidir, la resiliencia y la competitividad en un entorno cada vez más digital. El foco pasa a situarse sobre toda la cadena de valor digital —infraestructuras, semiconductores, plataformas, software, datos y servicios— con el objetivo de reforzar las capacidades críticas de cada economía. Desde esta perspectiva, la soberanía no se entiende como aislamiento tecnológico, sino como la capacidad de mantener libertad de decisión sobre capacidades estratégicas dentro de ecosistemas abiertos e interoperables. Esta visión reconoce que la cooperación internacional, la diversificación, la interoperabilidad y los ecosistemas abiertos siguen siendo elementos esenciales para la innovación y la competitividad. La soberanía digital no implica operar de forma aislada, sino participar en redes globales preservando la libertad de actuación sobre las capacidades estratégicas.

Para las organizaciones, este cambio implica que la soberanía digital deja de ser un concepto político para convertirse en un factor que afecta directamente a la resiliencia operativa, la capacidad de innovación y la competitividad.

4.3 De la ciberseguridad a la resiliencia digital

Uno de los cambios más relevantes para los Consejos de Administración es que la regulación europea ha trasladado la responsabilidad de la resiliencia digital desde el ámbito técnico al ámbito del gobierno corporativo. La figura siguiente resume las principales iniciativas regulatorias europeas —SRI2 (también conocida como NIS2) [30], la Ley de Ciberresiliencia (CRA) [31], la Ley de Resiliencia Operativa Digital (DORA) [32], la Directiva de Resiliencia de Entidades Críticas (CER) [33] y el Reglamento de Inteligencia Artificial (RIA o AI Act) [34]—, destacando su objetivo principal y las implicaciones más relevantes para los Consejos de Administración.

A esta evolución normativa se suma la propuesta de modificación de la Cybersecurity Act (CSA2), presentada por la Comisión Europea en 2026, que apunta a una consideración creciente de factores geopolíticos y geoestratégicos en la gestión de riesgos asociados a tecnologías y proveedores críticos. Aunque su redacción definitiva sigue en proceso de definición, la propuesta refuerza la idea de que los Consejos deberán supervisar no solo riesgos técnicos, sino también aquellas dependencias externas que puedan afectar a la continuidad, la resiliencia y la capacidad de actuación de la organización.



Fig 3. La Resiliencia Estratégica como responsabilidad del Consejo de Administración
La evolución regulatoria europea traslada la resiliencia digital y la supervisión de las dependencias críticas desde el ámbito tecnológico al gobierno corporativo.

En conjunto, estas iniciativas reflejan una tendencia clara: la resiliencia digital deja de ser una responsabilidad exclusivamente tecnológica para convertirse en una responsabilidad de gobierno corporativo. La aprobación de la estrategia y la supervisión de su implementación, incluyendo la utilización de las capacidades digitales críticas pasan así a formar parte de las funciones del Consejo de Administración. Esta evolución regulatoria comparte una misma lógica: **los Consejos deben comprender, supervisar y gobernar las estrategias y sus riesgos, especialmente en relación con las dependencias digitales críticas de la organización.**

4.4 El Marco Europeo de Soberanía de la Nube: una referencia para el Consejo

Quizá la iniciativa más relevante, desde la perspectiva del gobierno corporativo, sea el Marco Europeo de Soberanía de la Nube (Cloud Sovereignty Framework) [17], impulsado por la Comisión Europea. Tradicionalmente, la soberanía digital se asociaba a la localización de los datos. Este marco introduce una visión mucho más amplia basada en el control sobre los proveedores, las infraestructuras y servicios, los datos, la tecnología, la cadena de suministro, la seguridad y la capacidad operativa.

Su principal aportación es que transforma la soberanía digital en una capacidad medible. A través de las **dimensiones de soberanía** (SOV) y los **niveles de madurez** (SEAL), permite evaluar hasta qué punto una organización mantiene capacidad de decisión sobre sus activos digitales críticos.

Más allá de sus aspectos técnicos, el valor de este marco europeo para los Consejos de Administración radica en una idea fundamental: la soberanía digital puede gestionarse y supervisarse, como cualquier otra capacidad estratégica de la organización.

4.5 Implicaciones para el Consejo

La evolución regulatoria europea apunta en una dirección inequívoca: la soberanía digital se ha convertido en una responsabilidad de gobierno corporativo. En la práctica, los Consejos deben:

- Comprender las dependencias digitales críticas de la organización.
- Supervisar la resiliencia de proveedores y plataformas estratégicas.
- Incorporar la soberanía digital a la gestión de riesgos.
- Garantizar capacidades adecuadas en ciberseguridad e inteligencia artificial.
- Asegurar la coherencia entre estas cuestiones y la estrategia corporativa.

Más allá del cumplimiento normativo, la soberanía digital no debe entenderse como una restricción para la innovación, sino como una capacidad que refuerza la resiliencia, la competitividad y la creación de valor [35]. La cuestión ya no es únicamente si la organización cumple la normativa, sino si dispone de las capacidades necesarias para preservar su margen de maniobra estratégico en un entorno cada vez más incierto. Esta capacidad para mantener el control, adaptarse al cambio y seguir creando valor es lo que en este documento denominamos **Resiliencia Estratégica**.

5. Resiliencia Estratégica para el Consejo

La aceleración tecnológica, la fragmentación geopolítica, y la creciente concentración de capacidades críticas están transformando las reglas de la competitividad global. Para los Consejos de Administración, la cuestión ya no es únicamente qué tecnología utiliza la organización, sino hasta qué punto conserva la capacidad de decidir, operar y crear valor cuando cambian las condiciones del entorno.

5.1 Europa en Cifras

El Foro Económico Mundial identifica la fragmentación geoeconómica, los riesgos tecnológicos y la ciberseguridad entre los principales desafíos para empresas y gobiernos [36], mientras que el Informe Draghi señala las dependencias tecnológicas como un factor determinante para la competitividad y la resiliencia europeas [15].

En este contexto, la cuestión para Europa ya no es únicamente innovar más rápido, sino garantizar el acceso, la libertad de decisión y la capacidad de adaptación sobre las tecnologías que determinarán su competitividad futura. La posición competitiva de Europa está cada vez más condicionada por su dependencia de capacidades tecnológicas críticas desarrolladas fuera de la Unión.



Fig. 4. Riesgos Geoestratégicos y Resiliencia Estratégica
La convergencia de riesgos geopolíticos, geoeconómicos y tecnológicos redefine el contexto competitivo y condiciona la capacidad futura de decidir, operar y crear valor.

El Centro de Gobierno Corporativo de Esade y EsadeGeo, en la tercera edición del ciclo de conferencias *Geopolítica en la Agenda del Consejo* [18], puso de manifiesto una realidad cada vez más evidente: Europa está perdiendo posiciones en la carrera tecnológica global.

Según el informe *Critical Technology Tracker de ASPI* [37], la competición tecnológica mundial se concentra crecientemente en Estados Unidos y China (que lidera la producción de quince de las dieciséis tecnologías críticas con mayor riesgo de concentración), mientras que Europa mantiene una dependencia significativa en ámbitos como la inteligencia artificial, los semiconductores, la nube (cloud) o el software avanzado. Esta dependencia tiene también una dimensión económica: la Comisión Europea estima que Europa destina anualmente alrededor de 264.000 millones de euros a productos y servicios digitales procedentes de terceros países [13].

A medida que la inteligencia artificial se convierte en un activo estratégico, el acceso a determinadas tecnologías puede quedar condicionado por decisiones tomadas fuera del control de la organización [38]. Esta situación no representaba un riesgo excesivo en un mundo de organizaciones multilaterales y con mecanismos de resolución de conflictos eficaces. Pero en la situación actual en la que la geopolítica está abandonando progresivamente el multilateralismo, para los Consejos de Administración, es imprescindible comprender qué dependencias son aceptables y cuáles pueden comprometer la competitividad, la resiliencia y la capacidad de actuación futura. Esta evolución se refleja también en la agenda de riesgos de las organizaciones europeas, donde la disrupción digital asociada a la IA, la incertidumbre geopolítica y la resiliencia empresarial figuran entre los ámbitos cuyo nivel de riesgo más ha aumentado durante el último año [39].



Fig 5. Europa en el nuevo tablero tecnológico global
La libertad de decisión y la capacidad de adaptación emergen como factores clave de competitividad y resiliencia.

Ya sea en inteligencia artificial, nube (cloud), semiconductores, sistemas de pago [40] o infraestructuras digitales, emerge una misma conclusión: la resiliencia no depende de la autosuficiencia, sino de la capacidad de elección [41]. Las organizaciones más resilientes son aquellas que comprenden sus dependencias, mantienen alternativas viables y conservan margen de maniobra estratégico frente a escenarios de disrupción.

La evolución de este debate refleja un cambio más amplio en la agenda económica y tecnológica internacional. Si hace apenas unos años el foco se situaba en la autonomía estratégica, la resiliencia de las cadenas de suministro o las estrategias de friendshoring, hoy la atención se desplaza progresivamente hacia la diversificación, como mecanismo básico e inmediato de gestión del riesgo, así como la recuperación y localización de capacidades consideradas críticas para la competitividad y la seguridad económica, a más largo plazo [42]. En Europa, esta evolución se traduce en una creciente preocupación por la soberanía digital y la necesidad de reforzar capacidades propias en ámbitos como la inteligencia artificial, los semiconductores, la nube (cloud) o las infraestructuras digitales.

La concentración de capacidades tecnológicas críticas exige analizar diversos escenarios a futuro más o menos probables pero plausibles y plantea una pregunta relevante para cualquier Consejo de Administración: **¿Cuáles de nuestras dependencias pueden convertirse en una vulnerabilidad competitiva?**

Para responder a esta cuestión proponemos un modelo de **Resiliencia Estratégica** orientado específicamente al gobierno corporativo.

5.2 Resiliencia Estratégica: las capacidades que sostienen la creación de valor

La resiliencia estratégica ya no puede entenderse únicamente como la capacidad de recuperarse de una crisis con el menor daño posible para la entidad. Para los Consejos de Administración, implica también anticipar cambios, adaptarse con rapidez y preservar la capacidad de actuación en entornos inciertos. Las tensiones geopolíticas, la aceleración tecnológica, la dependencia de infraestructuras digitales, la evolución regulatoria y la creciente relevancia de la inteligencia artificial están transformando el perfil de riesgos de las organizaciones. En este contexto, la resiliencia ya no depende de una única tecnología o función empresarial, sino de un conjunto de capacidades que deben ser gobernadas de forma integrada para preservar la continuidad, la adaptación y la capacidad de actuación.

La siguiente figura presenta un modelo de **Resiliencia Estratégica** para Consejos de Administración. El modelo conecta la creación de valor con las capacidades que permiten preservar la continuidad, la capacidad de adaptación y la autonomía estratégica de la organización.

5.3 La creación de valor como objetivo último

En la parte superior del modelo se sitúa la **creación de valor**, principal responsabilidad del Consejo. Crecimiento, competitividad e innovación dependen cada vez más de la capacidad de la organización para anticipar cambios, adaptarse con rapidez y mantener la libertad de decisión sobre sus capacidades críticas.

Para alcanzarla, la organización debe desarrollar una capacidad intermedia: la resiliencia estratégica. En la era de la inteligencia artificial, la soberanía digital ya no es solo una cuestión de control. Diversos estudios señalan que las organizaciones con mejor gestión y mayor control sobre sus datos e infraestructuras pueden **obtener retornos hasta cinco veces superiores en sus iniciativas de inteligencia artificial** [43], convirtiendo la soberanía digital en un factor de creación de valor y no únicamente de mitigación de riesgos. Asimismo, las organizaciones capaces de ejercer un control selectivo sobre datos, modelos e infraestructuras logran proteger **hasta un 55% más de su beneficio operativo** frente a disrupciones asociadas a la inteligencia artificial, reforzando la relación entre soberanía digital, resiliencia y creación de valor [19].



Fig 6. Modelo de Resiliencia Estratégica para la Creación de Valor
Las capacidades que permiten preservar la libertad de decisión, la capacidad de adaptación y la libertad de actuación necesarias para seguir creando valor

La **resiliencia estratégica** actúa como elemento integrador y se apoya en tres capacidades fundamentales:

- Mantener la continuidad de las operaciones críticas.
- Adaptarse a cambios internos y externos.
- Preservar la capacidad de actuación de la organización.

Desde esta perspectiva, la resiliencia deja de ser una cuestión exclusivamente operativa para convertirse en un factor de competitividad, adaptación y gobierno corporativo. Su objetivo no es eliminar todas las dependencias, sino preservar la capacidad de elección y adaptación de la organización en entornos inciertos.

5.4 Los pilares de la resiliencia estratégica

La resiliencia estratégica se sustenta sobre diez capacidades agrupadas en dos grandes ámbitos complementarios.

Antes de analizar estas capacidades conviene destacar una de las transformaciones más relevantes de la última década: la creciente convergencia entre geopolítica y geoeconomía. Las decisiones relacionadas con el comercio, la tecnología, la energía, los datos o las infraestructuras críticas ya no responden únicamente a criterios económicos, sino también a objetivos de seguridad, influencia y competitividad. En este contexto, las organizaciones deben comprender sus **dependencias geoestratégicas**: aquellas dependencias tecnológicas, energéticas, regulatorias o jurisdiccionales que pueden afectar a su capacidad de decidir, operar y crear valor.

Soberanía: aquello que debemos controlar

La soberanía hace referencia al grado de libertad de decisión que la organización mantiene sobre los activos, recursos y capacidades que resultan esenciales para su actividad. Sus dimensiones son:

- **Dependencias Geoestratégicas**, para identificar aquellas dependencias externas que podrían afectar al acceso, control o disponibilidad de capacidades críticas para la organización (factores externos que condicionan la competitividad).
- **Datos**, como activo crítico para la operación y la inteligencia artificial.
- **Inteligencia Artificial**, asegurando el control sobre modelos, datos, capacidades y conocimiento.
- **Nube e Infraestructura Digital**, evitando dependencias que limiten la capacidad de elección.
- **Cumplimiento Normativo**, garantizando la adaptación continua a un entorno regulatorio cada vez más exigente.

La creciente relevancia de la soberanía digital está impulsando modelos de soberanía operativa que integran capacidades de gobernanza, cumplimiento, seguridad e inteligencia artificial desde el diseño, permitiendo reforzar la libertad de decisión y la independencia operativa de las organizaciones [44]. En el ámbito de la inteligencia artificial, la soberanía implica no solo controlar la tecnología utilizada, sino también mantener visibilidad y capacidad de supervisión sobre los procesos de decisión que esta genera [39].

Autonomía: aquello que debemos ser capaces de hacer

La autonomía refleja la capacidad de la organización para operar y adaptarse incluso cuando determinadas dependencias dejan de estar disponibles.

Sus dimensiones son:

- **Cadena de Suministro Digital**, para gestionar dependencias tecnológicas críticas.
- **Talento y Capacidades**, que permiten gobernar la transformación digital.
- **Energía**, como requisito indispensable para la continuidad de las operaciones digitales.
- **Seguridad**, preservando la capacidad de operación frente a incidentes tecnológicos, físicos o ambientales que puedan afectar a los recursos digitales críticos de la organización.
- **Resiliencia Operativa**, garantizando respuesta y recuperación ante interrupciones.

La resiliencia estratégica no depende únicamente de la tecnología. Depende también de las **capacidades de las personas** que la gobiernan. En un contexto de creciente adopción de la inteligencia artificial y de escasez de talento especializado, la formación, la capacitación digital y la alfabetización en IA se convierten en responsabilidades crecientes para la alta dirección. Esta preocupación trasciende el ámbito empresarial y se refleja también en las prioridades europeas, que aspiran a que el 80% de la población disponga de competencias digitales básicas [45] y a alcanzar 20 millones de especialistas TIC para 2030.

Para muchas organizaciones, el desafío ya no consiste únicamente en desarrollar capacidades internas, sino también en asegurar el acceso al talento necesario en un mercado cada vez más competitivo. La disponibilidad de talento especializado se está convirtiendo en una capacidad estratégica tan relevante como el acceso a la tecnología o al capital. Las dependencias tecnológicas ya no se limitan a infraestructuras o proveedores. También incluyen capacidades humanas, ecosistemas de innovación y acceso a conocimiento especializado, factores que condicionarán cada vez más la competitividad futura de las organizaciones.

En última instancia, la ventaja competitiva no dependerá únicamente de los algoritmos, sino de la capacidad de las personas para comprenderlos, supervisarlos y utilizarlos con criterio. La resiliencia operativa constituye la prueba práctica de la resiliencia estratégica. Una organización solo será verdaderamente resiliente si puede mantener la continuidad de sus operaciones críticas cuando se producen interrupciones significativas.

La creciente convergencia entre seguridad física y digital está ampliando el alcance tradicional de la ciberseguridad. Fenómenos meteorológicos extremos, interrupciones energéticas, fallos en infraestructuras críticas o incidentes en la cadena de suministro pueden afectar a la continuidad de las operaciones digitales de la misma forma que un ciberataque. La seguridad debe entenderse, por tanto, como una capacidad transversal al servicio de la resiliencia operativa.

La **Resiliencia Estratégica** surge del equilibrio entre **soberanía** (la libertad de decisión de las dependencias críticas) y la **autonomía** (la capacidad de adaptación ante un entorno cambiante).

5.5 El papel del Consejo

La base del modelo está constituida por el **Gobierno Corporativo**. Corresponde al Consejo supervisar que estas capacidades se desarrollan de manera equilibrada, comprendiendo las dependencias críticas de la organización y asegurando que las decisiones de inversión, riesgo y estrategia fortalecen la resiliencia a largo plazo.

Ninguna de estas capacidades debe analizarse de forma aislada. La resiliencia estratégica surge del equilibrio entre soberanía y autonomía, permitiendo mantener la continuidad del negocio, preservar la capacidad de actuación y seguir creando valor en un entorno cada vez más incierto [4], [5] y [6].

El papel del Consejo no consiste en maximizar la libertad de decisión en todos los ámbitos ni minimizar todas las dependencias, sino en mantener el equilibrio adecuado entre libertad de decisión y capacidad de adaptación para preservar la creación de valor a largo plazo.

> “La verdadera resiliencia estratégica no consiste en eliminar las dependencias, sino en evitar que condicionen nuestra capacidad de decidir, adaptarnos y competir. En un entorno cada vez más incierto, preservar esa libertad de acción es una fuente esencial de competitividad y de creación de valor a largo plazo.”
>
> **Iván Martén**, consejero independiente de Repsol; presidente de Orkestra y patrono de Tecnalia y Fundación Esade

6. Cómo supervisar la Resiliencia Estratégica desde el Consejo

La **resiliencia estratégica** es una **responsabilidad compartida de todos los órganos de gobierno y alta dirección, es decir, el Consejo de Administración** [46], CEO y Comité de Dirección o similar. No depende exclusivamente de las áreas de tecnología, riesgo o ciberseguridad, sino de la capacidad de la organización para mantener la libertad de decisión sobre sus capacidades críticas, responder eficazmente a escenarios de disrupción y preservar la creación de valor a largo plazo.

Desde esta perspectiva, el Consejo debe supervisar de forma integrada los diez pilares de la resiliencia estratégica. Del mismo modo que los riesgos financieros, regulatorios u operativos se gestionan de forma transversal, las capacidades que sustentan la resiliencia estratégica deben incorporarse a los mecanismos ordinarios de gobierno corporativo [30], [31], [32], [33] y [34].

La resiliencia estratégica no constituye una nueva función corporativa. Constituye una nueva forma de supervisar las capacidades que sostienen la creación de valor.

6.1 La resiliencia estratégica vista desde las comisiones

La resiliencia estratégica es una responsabilidad compartida. Cada comisión contribuye a preservar el margen de maniobra estratégico, la continuidad y la creación de valor de la organización.

6.2 Una responsabilidad compartida

Todas las comisiones comparten una misma misión: garantizar que la organización mantiene el equilibrio adecuado entre la libertad de decisión y la capacidad de adaptación. Por tanto, la resiliencia estratégica no es responsabilidad de una única comisión ni de una única función corporativa.

La creciente relevancia de la inteligencia artificial, la concentración tecnológica, la evolución regulatoria, las tensiones geopolíticas y geoeconómicas están llevando a considerar la soberanía digital como un riesgo estratégico que debe ser supervisado por el propio Consejo. Ya no basta con gestionar riesgos aislados. La supervisión de la resiliencia estratégica exige comprender las dependencias críticas de la organización, distinguir cuáles son, cuáles podrían comprometer su autonomía estratégica [47] y cómo gestionar (mitigar, transferir o asumir) los riesgos que las pueden afectar, teniendo en cuenta los costes de estas medidas de gestión.

La cuestión no es eliminar toda dependencia, sino gestionar aquellas que resultan críticas para la creación de valor.

"***Las empresas ya no pueden seguir abordando los riesgos de ciberseguridad de forma separada de los riesgos de seguridad física o industrial. Todos ellos son componentes de un mismo riesgo operacional que requiere una aproximación integral, poniendo el foco no solo en la protección, sino especialmente en la resiliencia***" [48].

Y, en última instancia, todas las comisiones deberían ser capaces de responder una misma pregunta: **¿Estamos supervisando las capacidades que sostendrán la competitividad futura de la organización?**

Supervisión de la Resiliencia Estratégica desde las Comisiones

Comisión	Capacidades que supervisa	Pregunta clave
Consejo Pleno	Visión integrada de soberanía, autonomía y resiliencia	¿Estamos fortaleciendo nuestra capacidad de creación de valor cuando cambian las condiciones del entorno?
Auditoría y Riesgos	Seguridad, Resiliencia Operativa y Cadena de Suministro Digital	¿Qué ocurriría si una capacidad crítica dejara de estar disponible mañana?
Nombramientos y Retribuciones	Talento y Capacidades	¿Disponemos de las capacidades necesarias para gobernar nuestra transformación digital?
Tecnología	Datos, IA, Nube e Infraestructura Digital	¿Mantenemos una capacidad real de elección sobre nuestras tecnologías críticas?
Sostenibilidad	Energía, IA Responsable y adaptación regulatoria	¿Es sostenible y responsable nuestro modelo digital a largo plazo?

La resiliencia estratégica es una responsabilidad compartida. Cada comisión contribuye a preservar la capacidad de decisión, continuidad y creación de valor de la organización.

Fig 7. Supervisión de la Resiliencia Estratégica desde las Comisiones
Cada comisión contribuye a preservar la libertad de decisión, la capacidad de adaptación y la creación de valor de la organización.

> "La soberanía digital no consiste en tenerlo todo bajo control, sino en saber de qué dependemos y asegurarnos de que esas dependencias no condicionan nuestra capacidad de decidir e innovar. Preservar esa libertad de decisión es una cuestión de competitividad."
>
> **Juan Zufiría**, presidente del Patronato de la Fundación Bankinter para la Innovación; consejero de Bankinter; vicepresidente de la Real Academia de Ingeniería de España y exvicepresidente sénior de IBM

7. Un sistema de supervisión de la Resiliencia Estratégica

La resiliencia estratégica exige algo más que intuición. Requiere mecanismos que permitan al Consejo disponer de visibilidad sobre las capacidades que sostienen la creación de valor y comprender hasta qué punto la organización mantiene el equilibrio adecuado entre la asunción de riesgos y capacidad de adaptación.

Desde esta perspectiva, el Consejo debería ser capaz de responder periódicamente a tres preguntas fundamentales:

- ¿Qué capacidades son críticas para nuestra competitividad futura?
- ¿Hasta qué punto disponemos de libertad de decisión sobre dichas capacidades?
- ¿Disponemos de la capacidad de adaptación necesaria para responder ante escenarios de disrupción?

El Modelo de **Resiliencia Estratégica** para la Creación de Valor muestra que la resiliencia estratégica surge del equilibrio entre soberanía y autonomía. Por ello, la supervisión del Consejo debe centrarse en comprender cómo evolucionan ambos elementos y cómo afectan a la capacidad de la organización para seguir creando valor. Para facilitar esta supervisión proponemos un enfoque sencillo basado en tres niveles complementarios:

1. **El Modelo de Resiliencia Estratégica**, que permite identificar las capacidades críticas que sustentan la creación de valor y comprender cómo contribuyen a la soberanía y a la autonomía de la organización.

2. **El Índice de Resiliencia Estratégica para Consejos (IRE)**, que proporciona una visión sintética del equilibrio entre libertad de decisión y capacidad de adaptación.

3. **El Dashboard de Resiliencia Estratégica**, que permite monitorizar la evolución de las capacidades críticas, las dependencias clave y aquellas vulnerabilidades que pueden afectar al margen de maniobra estratégico de la organización.

Tomados en conjunto, estos tres elementos permiten al Consejo identificar las capacidades críticas para la organización; evaluar el equilibrio entre soberanía y autonomía; y supervisar su evolución para apoyar la toma de decisiones estratégicas.



Fig 8. Sistema de Supervisión de la Resiliencia Estratégica
El Modelo identifica las capacidades críticas, el IRE evalúa el equilibrio entre libertad de decisión y capacidad de adaptación, y el Dashboard monitoriza su evolución para apoyar la toma de decisiones del Consejo.

7.1 Índice de Resiliencia Estratégica para Consejos (IRE)

El Índice de Resiliencia Estratégica para Consejos (IRE) proporciona una visión sintética de la capacidad de la organización para preservar la creación de valor mediante el equilibrio entre libertad de decisión y capacidad de adaptación.

Su finalidad no es medir la madurez tecnológica ni la implantación de determinadas soluciones digitales. Desde la perspectiva del Consejo de Administración, su propósito es ayudar a comprender si la organización mantiene el nivel de resiliencia necesario para decidir, operar y crear valor en entornos caracterizados por la incertidumbre y el cambio.

El índice se construye a partir de los dos pilares que sustentan la resiliencia estratégica:

- **Soberanía**, entendida como la capacidad de mantener la libertad de decisión sobre las capacidades críticas.
- **Autonomía**, entendida como la capacidad de adaptación ante cambios tecnológicos, regulatorios, económicos o geopolíticos.

La combinación de ambas dimensiones proporciona una visión sintética del nivel de resiliencia estratégica de la organización.



Fig 9. Índice de Resiliencia Estratégica para Consejos (IRE)
Valoración ejecutiva del equilibrio entre libertad de decisión y capacidad de adaptación que sustenta la resiliencia estratégica.

El IRE no pretende proporcionar una medición precisa, sino una valoración eficaz del equilibrio entre soberanía digital y capacidad de adaptación.

La evaluación se apoya en el análisis de las diez capacidades que conforman el Modelo de Resiliencia Estratégica y en la información proporcionada por el Dashboard de Resiliencia Estratégica. A partir de esta información, el Consejo puede formarse una visión estructurada sobre el grado de margen de maniobra que mantiene sobre sus capacidades críticas y sobre su capacidad de adaptación ante escenarios de disrupción.

Más que una fórmula matemática, el IRE debe entenderse como una herramienta de supervisión que facilita la conversación del Consejo sobre aquellas dependencias que podrían afectar a la capacidad futura de decidir, operar y crear valor.

El valor del IRE no reside en la precisión de la puntuación, sino en la capacidad de identificar si la organización está fortaleciendo o debilitando su resiliencia estratégica a lo largo del tiempo.

7.2 Dashboard de Resiliencia Estratégica

El Dashboard de Resiliencia Estratégica complementa al IRE proporcionando una visión continua de la evolución de las capacidades críticas y dependencias clave de la organización.

Mientras el IRE ofrece una visión sintética del nivel de resiliencia estratégica, el dashboard permite identificar tendencias, vulnerabilidades emergentes y posibles deterioros que puedan afectar al margen de maniobra estratégico.

El dashboard no pretende sustituir el criterio del Consejo ni gestionar la operación de la organización. Su finalidad es proporcionar una visión eficaz de aquellas capacidades que sustentan la resiliencia estratégica, facilitando la identificación temprana de vulnerabilidades y prioridades de actuación.



Fig 10. Dashboard de Resiliencia Estratégica
Visión de las capacidades críticas, dependencias clave y vulnerabilidades relevantes para el Consejo.

7.3 Cómo interpretar el IRE

El propósito del IRE no es alcanzar la máxima puntuación posible. Su finalidad es ayudar al Consejo a comprender y decidir qué dependencias son aceptables, cuáles requieren mitigación o transferencia y cuáles podrían comprometer la capacidad futura de decidir, operar y crear valor.

Las dependencias rara vez son absolutas. No todas las capacidades requieren el mismo grado de libertad de decisión, sobre todo teniendo en cuenta que las medidas de gestión del riesgo de dependencia siempre tienen un coste asociado y por tanto es necesario sopesar el grado óptimo de asunción de ese riesgo. La cuestión para el Consejo no es maximizar la soberanía en todos los ámbitos, sino identificar qué capacidades son estratégicamente críticas y requieren mayores niveles de supervisión, control o capacidad de sustitución.

La monitorización de estos indicadores resulta especialmente relevante en un contexto marcado por una creciente fragmentación tecnológica, geopolítica y regulatoria [35].

El verdadero valor del índice reside en determinar si la organización mantiene el equilibrio adecuado entre **libertad de decisión** y **capacidad de adaptación**, los dos pilares sobre los que se construye la resiliencia estratégica.

Una **organización resiliente** no es aquella que elimina todas sus dependencias, sino **aquella que dispone de la visibilidad, la libertad de decisión y la capacidad de adaptación necesarias para que ninguna de ellas comprometa su libertad de actuación**.

Y, en última instancia, el Consejo debería utilizar el IRE para responder a una única pregunta clave: ¿Mantenemos el equilibrio adecuado entre libertad de decisión y capacidad de adaptación?

7.4 Preguntas para el Consejo

La utilidad del Modelo de Resiliencia Estratégica, del IRE y del Dashboard no reside únicamente en proporcionar información, sino en facilitar una conversación estructurada en el seno del Consejo de Administración.

El objetivo no es eliminar todas las dependencias ni maximizar las puntuaciones de los indicadores, sino comprender qué capacidades son críticas para la organización, cómo y cuánto costaría ganar independencia y hasta qué punto podrían afectar a su capacidad futura de decidir, operar y crear valor.

Desde esta perspectiva, todo Consejo debería ser capaz de responder a las siguientes preguntas

Libertad de decisión (Soberanía)

La **soberanía** determina aquello que la organización debe controlar. Las siguientes preguntas ayudan al Consejo a identificar las dependencias que podrían comprometer su capacidad de decisión.

- ¿Qué dependencias son críticas para nuestro modelo de negocio y nuestra capacidad para crear valor?
- ¿Quién controla los datos, plataformas o capacidades sobre las que construiremos nuestro futuro?
- ¿Qué dependencias geoestratégicas, jurisdiccionales o regulatorias podrían afectar nuestra estrategia?
- ¿Qué capacidades tecnológicas críticas podrían dejar de estar disponibles, verse restringidas o encarecerse por factores fuera de nuestro control?
- ¿Qué alternativas viables existen para reducir esas dependencias (por ejemplo, diversificación, internalización) en plazos compatibles con la continuidad del negocio?
- ¿Qué capacidades debemos mantener necesariamente bajo nuestro control directo y reforzado dentro de la organización?

Capacidad de Adaptación (Autonomía)

La **autonomía** refleja la capacidad de la organización para seguir operando cuando una dependencia crítica deja de estar disponible o modifica sus condiciones. Las siguientes preguntas permiten evaluar su capacidad de adaptación.

- ¿Podríamos seguir operando si una capacidad crítica dejara de estar disponible mañana?
- ¿Disponemos de alternativas viables para nuestras capacidades más importantes?
- ¿Tenemos el talento necesario para gobernar nuestra transformación en esta nueva era?
- ¿Comprendemos nuestras dependencias energéticas y el impacto que podrían tener sobre la continuidad del negocio?
- ¿Qué capacidades críticas dejarían de estar disponibles si se produjera una interrupción significativa?
- ¿Hemos probado nuestra capacidad de respuesta ante escenarios disruptivos?

Resiliencia Estratégica y Creación de Valor

La verdadera prueba de la resiliencia estratégica consiste en verificar si la organización puede seguir creando valor cuando cambian las reglas del juego.

- ¿Qué ocurriría si cambiasen significativamente las condiciones tecnológicas, regulatorias o geoestratégicas?
- ¿Podríamos mantener y mejorar nuestras ventajas competitivas actuales?
- ¿Podemos reconfigurar recursos, proveedores, procesos o modelos de negocio dentro de un plazo compatible con la preservación de valor?
- ¿Estamos invirtiendo hoy en las capacidades que necesitaremos mañana?
- ¿Seguiríamos siendo capaces de decidir, operar y crear valor en nuestros propios términos?

Si mañana cambiaran las condiciones tecnológicas, regulatorias, energéticas o geoestratégicas, ¿seguiríamos siendo capaces de decidir, operar y crear valor?

8. Conclusiones

La aceleración tecnológica, la inteligencia artificial, la fragmentación geopolítica, geoeconómica y la creciente concentración de capacidades críticas están redefiniendo las reglas de la competitividad. En este contexto, la responsabilidad del Consejo sigue siendo la misma: preservar la capacidad de la organización para crear valor de forma sostenible.

Sin embargo, las capacidades necesarias para lograrlo han cambiado. La competitividad ya no depende únicamente del acceso a la tecnología, sino de la capacidad para comprender, gobernar y gestionar las dependencias sobre las que se sustenta el negocio.

A lo largo de este documento hemos planteado que la **Resiliencia Estratégica** constituye una nueva responsabilidad de gobierno y supervisión para los Consejos de Administración. Una capacidad que permite mantener la continuidad de las operaciones, adaptarse a los cambios del entorno y preservar el margen de maniobra estratégico cuando cambian las reglas del juego.

La resiliencia estratégica se construye sobre dos pilares complementarios:

- **La soberanía**, que proporciona la libertad de decisión estratégica sobre las capacidades críticas.
- **La autonomía**, que aporta la capacidad de adaptación necesaria para operar y evolucionar en entornos inciertos.

Ninguna organización puede aspirar a la autosuficiencia. El objetivo no es eliminar las dependencias, sino comprenderlas, gobernarlas y asegurar que no comprometan la competitividad futura de la organización. La **resiliencia estratégica se construye mediante la existencia de alternativas, capacidad de elección y ecosistemas capaces de evolucionar con el entorno.**

En este contexto, la próxima generación de ventajas competitivas no surgirá únicamente de la posesión de tecnologías avanzadas, sino de la capacidad para integrarlas, coordinarlas y gobernarlas eficazmente dentro de ecosistemas cada vez más interdependientes.

Para los Consejos de Administración, esto supone ampliar la visión tradicional de la supervisión. Además de los riesgos financieros, regulatorios y operativos, resulta necesario comprender los **riesgos geoestratégicos** (las dependencias tecnológicas, energéticas, geopolíticas y de talento) que condicionarán la competitividad futura, garantizando al mismo tiempo que la inteligencia artificial se despliega de forma transparente, responsable y generadora de confianza. Como señala la Guía para Consejeros para una IA Ética de Esade [46], la supervisión de la inteligencia artificial constituye ya una responsabilidad de gobierno corporativo.

En este nuevo entorno, la capacidad de demostrar libertad de decisión, transparencia y buena gobernanza sobre las capacidades críticas se está convirtiendo en un factor de confianza para reguladores, clientes, inversores y otros grupos de interés.

La Soberanía Digital proporciona libertad de decisión. La Autonomía Digital aporta capacidad de adaptación. La combinación de ambas permite preservar la libertad de actuación necesaria para seguir creando valor. Esa capacidad es lo que denominamos Resiliencia Estratégica.

Y, en última instancia, toda la discusión puede resumirse en una única pregunta: **Si mañana cambiaran las condiciones tecnológicas, regulatorias, energéticas, geopolíticas o geoeconómicas, ¿seguiríamos siendo capaces de decidir, operar y crear valor en nuestros propios términos?**

Los Consejos que puedan responder afirmativamente a esta pregunta estarán mejor preparados para proteger la competitividad, impulsar la innovación y preservar el valor de sus organizaciones durante la próxima década.

La **Resiliencia Estratégica** no consiste en predecir el futuro. Consiste en preservar la libertad de actuación necesaria para seguir decidiendo, operando y creando valor cuando cambian las reglas del juego.

9. Bibliografía

[1] Digital Sovereignty of Companies and Other Organizations—An Introduction. In *New Digital Work II: Digital Sovereignty of Companies and Organizations* (pp. 1-16). Cham: Springer Nature Switzerland. Hartmann, E. A., Shajek, A., & Schmuntzsch, U. (2025). (https://doi.org/10.1007/978-3-031-69994-8_1)

[2] Digital sovereignty and artificial intelligence: a normative approach. *Ethics and information technology,* 26(4), 70. Roberts, H. (2024). (https://doi.org/10.1007/s10676-024-09810-5)

[3] Organizational autonomy: A review and agenda for future research. *Journal of Management,* 49(1), 85-124. Arregle, J. L., Dattée, B., Hitt, M. A., & Bergh, D. (2023). (https://doi.org/10.1177/01492063221123264)

[4] Resilience in organizations: An integrative multilevel review and editorial introduction. *Group & Organization Management*, 46(4), 709–739. Raetze, S., Duchek, S., Maynard, M. T., & Kirkman, B. L. (2021). (https://doi.org/10.1177/10596011211032129)

[5] Organizational resilience: A capability-based conceptualization. *Business Research*, 13, 215–246. Duchek, S. (2020).(https://doi.org/10.1007/s40685-019-0085-5)

[6] The quest for resilience. *Harvard Business Review*, 81(9), 52-65. Hamel, G., & Valikangas, L. (2003).

[7] Investigación sobre la naturaleza y causas de la riqueza de las naciones. Adam Smith (1776)

[8] Building digital resilience against major shocks. *MIS quarterly*, 47(1), 343-360. Boh, W., Constantinides, P., Padmanabhan, B., & Viswanathan, S. (2023). (https://doi.org/10.25300/MISQ/2023/47.1.12)

[9] Comisión Europea, *Reforzar la Soberanía Tecnológica de Europa*, 2026. (https://digital-strategy.ec.europa.eu/es/policies/eu-tech-sovereignty)

[10] Stanford University, The 2025 AI Index Report. (https://hai.stanford.edu/ai-index/2025-ai-index-report)

[11] Esade, *Tecnología, geopolítica y soberanía: el nuevo tablero estratégico para los Consejos de Administración*, 2026. (https://www.esade.edu/faculty-research/es/centro-gobierno-corporativo/publication/tecnologia-geopolitica-y-soberania-el-nuevo-tablero)

[12] Real Instituto Elcano, *El Reto de la soberanía tecnológica: hacia un ecosistema digital europeo propio,* 2025. (https://www.realinstitutoelcano.org/analisis/el-reto-de-la-soberania-tecnologica-hacia-un-ecosistema-digital-europeo-propio/)

[13] Comisión Europea, *Paquete Europeo de Soberanía Tecnológica*, 2026. (https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty)

[14] EuroStack, *A European Alternative for Digital Sovereignty*, 2025. (https://assets.filedock.xyz/public/EuroStack_2025.pdf)

[15] Comisión Europea, *The Draghi report on EU competitiveness*, 2025. (https://commission.europa.eu/topics/competitiveness/draghi-report_en)

[16] OECD, *Digital Economy Outlook*, 2024 (*https://www.oecd.org/en/publications/oecd-digital-economy-outlook_f0b5c251-en.html*)

[17] Comisión Europea, *Cloud Sovereignty Framework*, 2025. (https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en)

[18] Esade, 3a Ed. 'Geopolítica en la agenda del Consejo' | *Tecnología: gobernanza, disrupción y soberanía* (III), 2026. (https://www.youtube.com/watch?v=wNHO-t2XH80)

[19] IBM, *AI in motion Orchestrating AI at scale for sovereignty and resilience*, 2026. (https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ai-orchestration-layer)

[20] Gartner, *Digital Sovereignty Is Needed for Future Technological Resilience and Business Outcome*, 2026. (https://www.gartner.com/en/documents/7393130)

[21] Ministerio para la Transformación Digital y de la Función Pública, España Digital 2026. (https://digital.gob.es/ministerio/programas/programas-avance-digital/espana-digital-2026)

[22] Gobierno de España, *Conoce la Estrategia Nacional de Inteligencia Artificial* (ENIA), 2023. (https://planderecuperacion.gob.es/noticias/conoce-Estrategia-Nacional-Inteligencia-Artificial-ENIA-IA-prtr)

[23] La Moncloa, *El Gobierno presenta el Plan Industrial y Tecnológico para la Seguridad y la Defensa*, 2025. (https://www.lamoncloa.gob.es/consejodeministros/resumenes/paginas/2025/220425-rueda-de-prensa-ministros.aspx)

[24] Agencia Española de Supervisión de Inteligencia Artificial, *Garantizando una IA ética y responsable* (AESIA), 2025. (https://aesia.digital.gob.es/es)

[25] Boletín Oficial de Estado, Reglamento (UE) 2016/679, *Reglamento General de Protección de Datos* (RGPD), 2016. (https://www.boe.es/doue/2016/119/L00001-00088.pdf)

[26] Comisión Europea, *The Digital Europe Programme,* 2021. (https://digital-strategy.ec.europa.eu/en/activities/digital-programme)

[27] Comisión Europea, *Chips Act 2.0*, 2026. (https://digital-strategy.ec.europa.eu/en/policies/chips-act-2)

[28] Comisión Europea, *Shaping Europe's leadership in artificial intelligence with the AI continent action plan*, 2025. (https://commission.europa.eu/topics/competitiveness/ai-continent_en)

[29] European Centre for Development Policy Management (ECDM), *From India Stack to EuroStack: Reconciling approaches to sovereign digital infrastructure*, 2025. (https://ecdpm.org/application/files/2117/3874/5474/From-India-Stack-to-EuroStack-Reconciling-Approaches-Sovereign-Digital-Infrastructure-ECDPM-Discussion-Paper-384.pdf)

[30] Comisión Europea, Directiva *SRI 2: asegurar las redes y los sistemas de información* (o NIS 2), 2022. (https://digital-strategy.ec.europa.eu/es/policies/nis2-directive)

[31] Comisión Europea, *Ley de Ciberresiliencia* (CRA), 2024. (https://digital-strategy.ec.europa.eu/es/policies/cyber-resilience-act)

[32] Diario Oficial de la Unión Europea, Reglamento (UE) 2022/2554, *Ley de Resiliencia Operativa Digital* (DORA) (https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022R2554)

[33] Diario Oficial de la Unión Europea, *Directiva de Resiliencia de Entidades Críticas* (CER), 2022. (https://www.boe.es/doue/2022/333/L00164-00198.pdf)

[34] Consejo Europeo, *Reglamento de Inteligencia Artificial* (RIA), 2024. (https://www.consilium.europa.eu/es/policies/artificial-intelligence-act/)

[35] IBM, *Digital Sovereignty for Civilian Government*, 2026. (https://www.ibm.com/forms/mkt-whitepaper-47608)

[36] Foro Económico Mundial, *Global Risk Report*, 2026. (https://www.weforum.org/publications/global-risks-report-2026/)

[37] Australian Strategic Policy Institute, *ASPI's Critical Technology Tracker update*, 2025. (https://www.aspi.org.au/news/aspis-critical-technology-tracker-update-2025-dataset-monopoly-risk-insights/)

[38] The Economist, "*America's AI power grab*", 2026. (https://www.economist.com/weeklyedition/2026-06-20).

[39] Internal Audit Foundation, *Risk in Focus, Hot Topics for Internal Auditors,* Global Summary, 2026. (https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/risk-in-focus/2026/2026-global-report-en-riskinfocus.pdf)

[40] European Credit Research Institute (ECRI), *Payment sovereignty without walls: the case for Europe's multi-rail ecosystem*, 2026. (https://www.ecri.eu/publications/policy-briefs/payment-sovereignty-without-walls-case-europe%E2%80%99s-multi-rail-ecosystem)

[41] *Comisión de Transformación Digital del Senado,* Maite Arcos, directora general ESYS, 2026. (https://www.youtube.com/watch?v=hjZtzktlHuU)

[42] Geopolitical risk and uncertainty: *How transnational corporations can use scenario planning for strategic resilience.* Transnational Corporations Review, 14(4), 339-352. Kitsing, M. (2022). (https://doi.org/10.1080/19186444.2022.2145865)

[43] MIT Technology Review and EDB, *Establishing AI and data sovereignty in the age of autonomous systems*, 2026. (https://www.enterprisedb.com/sites/default/files/pdf/MITTR-Insights-EDB-report.pdf)

[44] IBM, Presentamos IBM® *Sovereign Core: una nueva base de software para la soberanía*, 2026. (https://www.ibm.com/es-es/new/announcements/introducing-ibm-sovereign-core-a-new-software-foundation-for-sovereignty?regionCode=es&languageCode=es&cm-history=es-es=)

[45] Comisión Europea, *Competencias Digitales*, 2026. (https://digital-strategy.ec.europa.eu/es/policies/digital-skills)

[46] Esade, *Guía de Consejeros para una IA Ética*, 2025. (https://www.esade.edu/itemsweb/wi/research/cgc/Guia_de_Consejeros_para_una_IA_etica.pdf)

[47] IBM Institute for Business Value, *The calculus of AI sovereignty*, 2026. (https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ai-sovereignty)

[48] Fundación ESYS, *Seguridad en Tiempos de Incertidumbre*, 2025. (https://www.fundacionesys.com/wp-content/uploads/2025/10/INFORME-ANUAL-FUNDACION-ESYS-2025.pdf)

esade

Center for Corporate
Governance

IBM