



ALTO REPRESENTANTE
DE LA UNIÓN PARA
ASUNTOS EXTERIORES Y
POLÍTICA DE SEGURIDAD

Bruselas, 3.12.2025
JOIN(2025) 977 final

COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO Y AL CONSEJO

Fortalecer la seguridad económica de la UE

1. Introducción

El uso cada vez más frecuente y específico de **herramientas económicas para la promoción de objetivos estratégicos** se ha convertido en una característica definitoria del panorama geopolítico actual. Desde aranceles con efectos perturbadores y la utilización de las dependencias como arma hasta el despliegue arbitrario de medidas de defensa comercial, los principales agentes están recurriendo a palancas económicas para perseguir sus objetivos estratégicos y geopolíticos, poniendo en riesgo la seguridad, el orden público, la competitividad y la economía de la UE.

Los riesgos para la seguridad económica de la UE no son nuevos, pero últimamente se han intensificado: en la actualidad, las vulnerabilidades son más visibles, más acuciantes y más difíciles de ignorar. Entre estos riesgos figuran los siguientes:

- una creciente **inestabilidad en el entorno mundial del comercio y la inversión**, marcada por el aumento de las medidas comerciales perturbadoras y las restricciones a la exportación para utilizar las dependencias como arma;
- la proliferación de **prácticas predatorias** dirigidas hacia cadenas de suministro y tecnologías críticas, que socavan nuestra base industrial, algunas de las cuales (como el exceso de capacidad financiado por el Estado) crean nuevas dependencias;
- el continuo deterioro del panorama de la seguridad, en particular en el contexto de la **guerra de agresión de Rusia contra Ucrania** y el aumento de los ataques híbridos.

En la **Estrategia Europea de Seguridad Económica** de 2023 se estableció la respuesta inicial de la UE a estos desafíos¹. En dicha estrategia se esbozaron una serie de acciones, basadas en evaluaciones de riesgos, destinadas a reforzar la seguridad económica de la UE mediante el **fomento** de la competitividad, la **protección frente a los riesgos** y la **asociación** con quienes comparten nuestras preocupaciones. Estos tres pilares siguen siendo el núcleo de nuestro enfoque de la seguridad económica, y la Comisión, junto con los Estados miembros, trabaja para integrarlos en cualquier consideración y actuación estratégica. Además, la seguridad económica es esencial para que la UE mantenga sus valores, sus principios y el bienestar de sus ciudadanos, así como para reforzar nuestra independencia económica.

Sin embargo, desde la adopción de la mencionada estrategia en 2023, la necesidad de que la UE actúe con mayor valentía, rapidez y unidad se ha hecho aún más patente. En la presente Comunicación se esboza un uso más estratégico y asertivo de los instrumentos de la Unión — complementando sus objetivos políticos originales— para apoyar la seguridad económica de Europa, que se refiere a la capacidad de la Unión para garantizar la seguridad, junto con otros objetivos, a través de una economía fuerte, dinámica y resiliente mediante la anticipación, la disuasión y la respuesta a amenazas potenciales o reales, vinculadas a las relaciones económicas de la UE con el resto del mundo. Para lograrlo, debe asegurarse de continuar en cabeza en el ámbito de las tecnologías, las industrias y los servicios críticos. Refleja un **cambio de paradigma** con el paso de una postura reactiva a un despliegue más proactivo y sistemático de nuestras herramientas. Además, en determinados casos, la UE, sus Estados

¹ JOIN(2023) 20 final.

miembros y la industria tendrán que estar cada vez más dispuestos a aceptar costes económicos en beneficio de la reducción de las vulnerabilidades y la mejora de la seguridad general.

Este llamamiento a la acción incluye **mejorar** la recopilación, el seguimiento y el análisis de la información, así como la capacidad de anticipar las amenazas emergentes; **disuadir** a terceros países de utilizar como arma las dependencias de la Unión; **reducir** nuestra exposición a terceros países que puedan utilizar dichas dependencias como arma; y **prevenir** los esfuerzos encaminados a socavar nuestras medidas de reducción del riesgo.

Cabe señalar que esta llamada a la acción también reconoce la necesidad de **aprovechar las fortalezas de la UE** en lo que respecta, entre otras cosas, al peso sin precedentes del mercado interior de la Unión, nuestras capacidades tecnológicas e industriales, y el acceso a la financiación y los programas de la UE. Esto incluye la determinación de las oportunidades económicas de la UE, así como de aquellos ámbitos en los que otros dependen de la UE. Por lo tanto, la presente Comunicación aboga por **un enfoque integrado a nivel institucional y de la Administración en su conjunto**, una **mejor gobernanza** y una **cooperación aún más estrecha con los socios afines y, cuando proceda, actuaciones conjuntas**. Complementa la amplia Estrategia de Preparación de la Unión. La seguridad económica de la UE se sustenta en la de sus Estados miembros. También está intrínsecamente vinculada a sus relaciones con el resto del mundo y, por tanto, a la política exterior y de seguridad común, que se utilizará de manera más sistemática para apoyar los objetivos declarados.

Sobre esta base, la presente Comunicación, que se apoya en un análisis basado en el riesgo, se centra en seis ámbitos de alto riesgo expuestos en la sección 3, aplica las herramientas de las que disponemos y describe cómo pueden mejorarse.

2. Un enfoque proactivo de la seguridad económica

La UE dispone de una amplia gama de herramientas que contribuyen a su seguridad económica. Ahora debe desplegarlos **de manera más estratégica, eficiente y proactiva** para reforzar su seguridad económica. Aunque la mayoría de estas herramientas no se desarrollaron originalmente teniendo en mente la seguridad económica, resultan muy pertinentes para promover los objetivos de seguridad económica de la Unión.

En el *gráfico 1* se presenta una lista no exhaustiva de herramientas clave, y su aplicación coordinada se articula con más detalle en la *sección 3*.

Gráfico 1. Lista no exhaustiva de herramientas de apoyo a la seguridad económica



Con el objetivo de fomentar la seguridad económica de la UE, la Comisión desplegará estas herramientas, en coordinación con los Estados miembros, del siguiente modo:

- Se utilizarán **instrumentos comerciales y de defensa de la competencia** para reducir de manera progresiva la exposición de la UE a los riesgos y evitar que se socaven los objetivos de reducción del riesgo de la UE. Esto incluye ampliar las oportunidades de diversificación y, por tanto, de nuestra seguridad global en el marco de los acuerdos comerciales de la UE, usar estratégicamente las herramientas aduaneras y luchar contra las distorsiones causadas por las subvenciones extranjeras, tanto en el seno del mercado interior como a través de subvenciones o importaciones objeto de dumping.
- Las herramientas de **resiliencia y ciberseguridad** se centrarán en la preparación para situaciones de emergencia y en su gestión, así como en la reducción de la exposición a amenazas externas, tales como las ciberamenazas.
- Se utilizarán **herramientas de seguridad y orden público** para reducir la exposición excesiva de la UE a los riesgos con el fin, entre otros objetivos, de garantizar el normal funcionamiento de la sociedad, al tiempo que se apoyan acciones destinadas a desarrollar su posición en tecnologías e industrias críticas, así como a evitar que se socaven sus objetivos de reducción del riesgo.
- Las **medidas anticoercitivas y restrictivas** tendrán por objeto disuadir y hacer frente a situaciones en las que terceros países intenten coaccionar a la UE, así como proteger a

las empresas de la Unión de las medidas extraterritoriales impuestas por terceros países y, cuando proceda, provocar un cambio de comportamiento por parte del país afectado.

- La **financiación y las restricciones** a través de herramientas de la UE como el Instrumento de Vecindad, Desarrollo y Cooperación Internacional o IVDCI (Global Gateway), Horizonte Europa, NextGenerationEU, InvestEU, el programa Europa Digital, el Mecanismo «Conectar Europa», los Instrumentos de Ayuda Preadhesión (IAP), los planes de crecimiento para los Balcanes Occidentales y Moldavia, así como el Mecanismo para Ucrania, EU4Health y el futuro Fondo Europeo de Competitividad, deben reforzar la seguridad económica de la UE o, como mínimo, no debilitarla, en consonancia con las normas de los programas.
- Las **iniciativas sectoriales** se utilizarán para desarrollar la propia capacidad de la UE y sus capacidades estratégicas en los ámbitos de alto riesgo determinados en el proceso de evaluación de riesgos.

Es más importante que nunca mantener una cooperación y coordinación estrechas con los países que conceden una importancia similar a la seguridad económica y a un orden mundial basado en normas. La UE trabajará para reforzar la **cooperación internacional en cuestiones de seguridad económica**, sobre todo con **socios de confianza**, en particular a través de **diálogos específicos sobre seguridad económica, tanto bilaterales como multilaterales**. Esta cooperación apoyará una acción conjunta en relación con intereses o preocupaciones comunes en materia de seguridad económica. Asimismo, profundizará en la comprensión colectiva de los riesgos, ayudará a anticipar amenazas, permitirá diseñar medidas de mitigación que **minimicen las externalidades negativas**, contribuirá a crear y mantener cadenas de suministro fiables y resilientes en sectores estratégicos clave, y ayudará a evitar efectos negativos en nuestros socios internacionales afines.

La Comisión tratará de entablar una cooperación bilateral con terceros países a través del Grupo de los Siete (G7), y también en el marco de iniciativas como el Tratado Integral y Progresista de Asociación Transpacífico y otros foros pertinentes. Trabjará con sus socios en la elaboración e implantación de normas de seguridad económica para unas cadenas de suministro resilientes. Una cooperación más estrecha puede incluir la **implantación coordinada de herramientas** y la creación de coaliciones con socios que compartan objetivos de seguridad económica similares o se enfrenten a retos semejantes.

Implantación de normas de seguridad económica

Sobre la base de los trabajos del G7 sobre el comercio basado en normas, la Comisión fomentará la elaboración y el uso de normas de seguridad económica. Dichas normas:

- se centrarán en medidas destinadas a diversificar las cadenas de suministro críticas mediante la creación de condiciones que regulen el acceso de nuevos proveedores al mercado o la limitación del acceso de proveedores dominantes;
- se guiarán por los principios de transparencia, interoperabilidad y cumplimiento de las normas internacionales;
- serán de tipo selectivo y estarán diseñadas a medida, teniendo en cuenta los riesgos específicos, las repercusiones económicas y las realidades empresariales de cada cadena de suministro.

También deben tenerse debidamente en cuenta la pertinencia y los efectos de la **política de vecindad y ampliación** de la UE. Los riesgos y las oportunidades para la seguridad económica de la UE se integrarán en la aplicación por parte de la Comisión de las políticas y los programas con estas regiones. Los países candidatos están en vías de convertirse en futuros Estados miembros de la UE; su alineación con la política de seguridad económica, así como su integración gradual en el mercado interior, son esenciales para garantizar el éxito de su adhesión, al tiempo que se mejora la capacidad de la UE para hacer frente tanto a los riesgos existentes como a los nuevos. Por lo tanto, es importante que los países candidatos reflejen el enfoque de la UE en materia de seguridad económica y, cuando proceda, se adapten gradualmente a la legislación de la UE relevante para los objetivos de seguridad económica.

3. Promoción de la seguridad económica de Europa: ámbitos de alto riesgo

La Estrategia de 2023 puso en marcha evaluaciones de riesgos que abarcaban la resiliencia de la cadena de suministro y la seguridad energética, las infraestructuras críticas, la utilización de las dependencias económicas como arma y, por último, la seguridad tecnológica y las fugas de tecnología. Ya se han evaluado cuatro tecnologías críticas [la inteligencia artificial (IA), las tecnologías cuánticas, los semiconductores y la biotecnología]. Sobre la base de este trabajo, la Comisión ha determinado **seis ámbitos de alto riesgo** en los que concentrará sus esfuerzos de inmediato y a corto plazo, en estrecha cooperación con los Estados miembros, la industria y sus socios de confianza. Al mismo tiempo, la Comisión seguirá llevando a cabo un seguimiento de la evolución de la situación y, en caso necesario, evaluará nuevos ámbitos emergentes de alto riesgo y actuará en consecuencia.

Resumen de los seis ámbitos de alto riesgo

Fortalecer la resiliencia de la cadena de suministro y contrarrestar las **dependencias estratégicas en bienes y servicios**

Atraer inversiones con **valor añadido** que refuercen la seguridad económica de la UE

Apoyar una **base industrial de defensa y espacial** dinámica y otros sectores industriales de alto riesgo

Desarrollar y mantener el **liderazgo en tecnologías críticas**

Impedir el acceso a **información y datos sensibles** que puedan socavar la seguridad económica de la UE

Prevenir y mitigar las **perturbaciones en las infraestructuras críticas de la UE** que afecten a la economía de la Unión

Indicadores no acumulativos de una dependencia de alto riesgo:

- el 60 % o más del suministro de la UE está controlado por un único tercer país u operador;
- los insumos o servicios tienen un valor sistémico para la economía de la UE debido al papel que desempeñan en múltiples sectores, por ejemplo, las materias primas fundamentales o los semiconductores;
- los insumos o servicios son esenciales para la industria o las capacidades estratégicas de defensa de la UE o para cadenas de suministro de tecnologías críticas específicas, como las tecnologías energéticas limpias;
- el tercer país ya ha utilizado las dependencias económicas como arma o ha amenazado con hacerlo, por ejemplo, mediante restricciones a la exportación;
- ya existe un exceso de capacidad no basado en el mercado o se está creando.

3.1. Fortalecer la resiliencia de la cadena de suministro y contrarrestar las dependencias de alto riesgo en bienes y servicios esenciales

El riesgo. Las economías modernas presentan un alto grado de interconexión y dependen de una amplia gama de insumos, bienes intermedios y servicios esenciales de socios de todo el mundo. En algunos casos, el suministro está fuertemente concentrado, a menudo en

países que no comparten los mismos intereses estratégicos y que tienen la capacidad y la voluntad de aumentar y utilizar estas dependencias como arma. Estos riesgos para las cadenas de suministro de la UE son especialmente visibles en nuestra dependencia de determinadas **materias primas fundamentales, materiales transformados y avanzados, componentes de tecnologías limpias y semiconductores convencionales**, así como en los **servicios financieros, los productos farmacéuticos, la industria aeronáutica y las tecnologías digitales y espaciales**. También son visibles en el **sector agroalimentario**, en el que la visión para la agricultura y la alimentación² establece la necesidad de reducir las dependencias estratégicas, en particular cuando la UE depende de un reducido número de socios para las importaciones de piensos y aditivos para piensos, así como de fertilizantes.

Las dependencias de alto riesgo pueden: i) ser **utilizadas como arma** con fines coercitivos (por ejemplo, materias primas fundamentales, semiconductores convencionales, materiales avanzados, productos energéticos, amenazas de desactivar determinados servicios); ii) crear una **vulnerabilidad económica sistémica** o un riesgo sistémico para el orden público y la protección de la salud pública en situaciones de crisis (por ejemplo, equipo de protección individual, suministro de medicamentos esenciales, suministro de alimentos); iii) crear el riesgo de perturbaciones a gran escala y de naturaleza intersectorial (por ejemplo, al penetrar en las redes de telecomunicaciones, depender de un único proveedor de servicios en la nube o interrumpir los servicios digitales); iv) **afectar a la competitividad de la UE y ralentizar las transiciones ecológica y digital** si se interrumpe el suministro (por ejemplo, baterías, imanes permanentes, productos y componentes de tecnologías limpias, materiales avanzados); v) afectar a la autonomía de los Estados miembros para desarrollar y explotar **capacidades militares**; o vi) amenazar la soberanía alimentaria de la UE.

Ejemplo de aplicación: semiconductores convencionales

Riesgo: la dependencia estructural de un único proveedor de un tercer país para la fabricación de chips esenciales de bajo margen pone en riesgo a varias industrias europeas. Estos semiconductores constituyen una parte fundamental de múltiples cadenas de suministro.

Uso de herramientas: la Comisión trabajará con socios de confianza para diversificar las fuentes de suministro y tratará de fomentar el aumento de la producción en el seno de la UE. En la próxima revisión del Reglamento de Chips se establecerán medidas de mitigación eficaces. La ciberseguridad de determinados semiconductores convencionales importados, utilizados en aplicaciones relacionadas con la seguridad debe evaluarse con más detalle en el marco del Reglamento de Ciberresiliencia.

Objetivo. La Comisión y los Estados miembros tratarán de **minimizar el potencial de perturbaciones a corto plazo** y pondrán en marcha al mismo tiempo medidas para **reducir de manera progresiva las dependencias de alto riesgo actuales en el mercado interior y contrarrestar los esfuerzos encaminados a crear otras nuevas**. Utilizará sus herramientas para llevar a cabo un seguimiento de la cadena de suministro y crear un marco que apoye la diversificación del suministro y evite que se socave la acción de la UE abordando las

² COM(2024) 75 de 19 de febrero de 2025.

distorsiones de la competencia en el mercado interior. Las acciones en el contexto del avance hacia la economía circular también desempeñarán un papel importante.

La Comisión adoptará las medidas necesarias para garantizar que sus cadenas de suministro alternativas no se vean socavadas por el dumping y la manipulación de los precios.

La Comisión ayudará a los Estados miembros a implantar de manera plena y eficaz las herramientas existentes, en particular los criterios de resiliencia que los Estados miembros deberán aplicar a partir de enero de 2026 en la contratación pública, las subastas y los regímenes de ayudas públicas en el marco del Reglamento sobre la Industria de Cero Emisiones Netas.

La Comisión adoptará asimismo medidas para desarrollar la **capacidad interna de la UE** y para diversificar el suministro **mediante la cooperación con sus socios, basándose, en particular, en su amplia red de acuerdos comerciales y otras formas de cooperación bilateral y multilateral**. Esto incluirá considerar la producción de determinados productos esenciales en nuestros países candidatos y en nuestros países socios en general, también con regiones como Oriente Próximo y Norte de África. Esto reforzará la resiliencia de las cadenas de suministro diversificadas de la UE y abrirá nuevas oportunidades para las empresas de la Unión. La Comisión seguirá detectando y llevando a cabo un seguimiento constante de las vulnerabilidades de la cadena de suministro y las **dependencias de alto riesgo** a través de su proceso de evaluación de riesgos y su compromiso con los Estados miembros y la industria.

3.2. Atraer inversiones con valor añadido que refuercen la seguridad económica de la UE

El riesgo. La afluencia de inversiones impulsa la resiliencia y la competitividad de la UE mediante la creación de empleo, el desarrollo de capacidades industriales, el aprovechamiento de la financiación y la dimensión, el apoyo a la innovación y la transferencia de tecnología. Sin embargo, determinadas formas de inversiones entrantes pueden plantear riesgos. Entre ellos figuran los siguientes: i) riesgos para la **seguridad y el orden público**, en particular el acceso a datos sensibles (por ejemplo, geolocalización, datos biométricos, secretos comerciales), el acceso a infraestructuras críticas y el acceso a tecnologías de doble uso y a otras tecnologías críticas; y ii) **riesgos para la resiliencia económica**, como una profundización de las dependencias o un punto único de fallo en cadenas de suministro críticas controladas por entidades de alto riesgo o terceros países que socaven nuestros intereses en materia de seguridad económica (por ejemplo, baterías, materias primas fundamentales, programas informáticos y componentes), que hagan que la Unión sea vulnerable a perturbaciones económicas o a la utilización de esas dependencias como arma; y iii) **problemas de baja competitividad**, como la falta de transferencia tecnológica, la creación limitada de valor añadido (por ejemplo, el hecho de disponer únicamente de líneas de montaje), la contratación de personal procedente del país inversor y, por tanto, la incidencia, entre otros, en el mercado laboral local.

Objetivo. La Comisión se centrará en garantizar que la UE mantenga su atractivo para las inversiones extranjeras y su apertura a estas. Tratará de equilibrar esta apertura, cuando sea necesario para la seguridad económica

de la UE, con la necesidad de evitar que se agraven las dependencias o se creen otras nuevas. Además, es fundamental preservar la capacidad de innovación de las empresas de la UE, en particular mediante la adquisición de propiedad intelectual clave de líderes emergentes por parte de entidades extranjeras, así como garantizar la seguridad del suministro y la continuidad del servicio. La Comisión utilizará sus herramientas e iniciativas para establecer y aplicar medidas específicas, como la fijación de condiciones a las inversiones entrantes que fomenten la transferencia de tecnología para entidades ubicadas en países que socaven intencionadamente nuestra seguridad económica.

Ejemplo: vehículos eléctricos de batería (VEB).

Riesgo. La posición dominante de determinados proveedores de VEB y los estrictos controles de las tecnologías necesarias para la producción de estos vehículos corren el riesgo de socavar el papel clave que ejerce el sector del automóvil en la economía de la UE, mientras dichos proveedores se benefician del mercado de la UE. Además, los vehículos conectados conllevan riesgos inherentes para la ciberseguridad.

Uso de herramientas: la Comisión está estudiando maneras de fomentar inversiones con valor añadido, en particular mediante el uso de iniciativas de política comercial y de defensa de la competencia. La Comisión continuará llevando a cabo un seguimiento de los flujos comerciales e implantará su conjunto de herramientas de mitigación del riesgo para reducir el riesgo de los elementos de conectividad, apoyar las inversiones en la próxima generación de tecnologías de VEB para garantizar que Europa siga siendo resiliente y competitiva y, en caso necesario, limitar la exposición a entidades de alto riesgo en los componentes conectados pertinentes de los VEB. La Comisión incentivará asimismo el intercambio de tecnología y conocimientos técnicos conexos que puedan reforzar los objetivos de seguridad económica de la UE.

3.3. Apoyar una base industrial de defensa y espacial dinámica y otros sectores industriales de alto riesgo

El riesgo. La guerra de agresión de Rusia contra Ucrania, el aumento de las tensiones geopolíticas y las medidas políticas conducentes a utilizar las dependencias comerciales como arma ponen de relieve la importancia de invertir en una base industrial nacional dinámica — en particular en los sectores de la defensa y el espacio, así como en sectores estratégicos de doble uso, como el transporte (por ejemplo, la aviación, la aeronáutica, la construcción naval y los puertos)— que alimente la economía de la UE y apoye su autonomía estratégica. Los riesgos en este ámbito incluyen los siguientes: i) inversión (interna) insuficiente; ii) bajos volúmenes de producción, combinados con una adquisición insuficiente de tecnología nacional para infraestructuras institucionales; iii) políticas y prácticas no basadas en el mercado por parte de terceros países, que den lugar a distorsiones en los mercados mundiales y regionales; iv) controles injustificados o desproporcionados de las exportaciones procedentes de terceros países impuestos a los productos y tecnologías europeos (extraterritorialidad de los regímenes de exportación de terceros países); v) pérdida de propiedad y control debido a adquisiciones extranjeras, incluso en determinados casos a través de adquisiciones de cartera; vi) un marco regulador rígido y unos mercados de capitales fragmentados que no facilitan el flujo de fondos ni promueven la puesta en marcha y la

expansión de tecnologías de alto riesgo y rentabilidad elevada con capacidades de doble uso.

Ejemplo de aplicación: componentes clave para drones y sistemas antidrones

Riesgo: la dependencia de proveedores de terceros países en lo que respecta a los componentes clave de drones, a las baterías y a los sistemas antidrones; ciclo de innovación extremadamente corto (computado en meses y, a veces, en semanas) para lograr que los drones mantengan su eficacia operativa, sobre la base de la experiencia real en el campo de batalla.

Uso de herramientas: la Comisión utilizará sus herramientas en el marco de los programas industriales europeos de defensa para garantizar la capacidad de producción de la UE y la reducción de los ciclos de innovación para las tecnologías de drones sobre la base de la experiencia operativa real. Seguirá reforzando la cooperación y el intercambio de información con carácter voluntario entre los organismos pertinentes [por ejemplo, las agencias nacionales de contratación pública y las organizaciones internacionales de contratación pública, como la Organización Conjunta de Cooperación en Materia de Armamento (OCCAR), la Agencia Europea de Defensa (AED) y la Organización del Tratado del Atlántico Norte (OTAN)], así como en el marco de los instrumentos y acciones de los programas industriales de defensa europeos. Con el fin de garantizar la resiliencia de la cadena de suministro, elaborará un mapa selectivo de las cadenas de suministro de productos y equipos específicos, incluidos los productos de doble uso, y apoyará la producción mediante la coinversión.

Determinados componentes de sectores críticos como la defensa proceden de entidades de alto riesgo, que podrían impedir el acceso y el uso de **material de defensa, tecnologías de doble uso y vehículos militares** si surgiera una situación de tensión geopolítica. Además, es fundamental que la UE mantenga una mano de obra altamente cualificada y no se quede atrás en la curva de innovación en las tecnologías que sustentan los sectores estratégicos. Una mitigación eficaz de estos riesgos mediante la movilización rápida de herramientas específicas y eficaces es esencial para las capacidades militares y de defensa de la UE.

Objetivo. La Comisión utilizará sus herramientas para mantener y desarrollar las capacidades estratégicas de fabricación en la UE, en particular a

través de: i) la promoción de la **inversión** pública y privada y, cuando proceda, la reducción del riesgo de dichas inversiones; ii) el **apoyo a la demanda** (mediante incentivos), también a través de la agregación o de adquisiciones conjuntas; iii) la **prevención del traslado** de capacidades y sectores estratégicos; iv) la **eliminación progresiva de los agentes potencialmente hostiles** de las cadenas de suministro de defensa y otras cadenas de suministro críticas, incluida la limitación de la adquisición de tecnologías críticas de defensa y espaciales restringidas desde fuera de la Unión; v) la mitigación de las **amenazas que plantean las inversiones extranjeras directas** en empresas que suministran productos esenciales o tecnologías críticas, vi) el **apoyo al desarrollo de tecnologías, componentes y materiales críticos** en la Unión persiguiendo objetivos a largo plazo, así como su adquisición mediante la contratación pública nacional para infraestructuras institucionales; vii) la garantía de que **las empresas emergentes y los negocios** de la UE reúnen las condiciones necesarias para su expansión, por ejemplo, mediante financiación adecuada y un trato arancelario favorable para determinados insumos de forma temporal, así como a través de un ecosistema propicio para los mercados de capitales.

La prioridad será apoyar la **base industrial de la defensa y el espacio**. Si bien la atención se

Ejemplo de aplicación: tecnologías cuánticas

Riesgo: diversas entidades extranjeras de alto riesgo o respaldadas por Estados buscan obtener acceso a la computación cuántica, la comunicación y los conocimientos técnicos e infraestructuras de detección de la UE a través de inversiones, adquisiciones o asociaciones de I+D, acelerando los usos militares o de inteligencia sensibles en el extranjero y erosionando la soberanía tecnológica de la UE.

Uso de herramientas: la Comisión seguirá elaborando un mapa de los principales agentes e infraestructuras cuánticos de la UE y llevando a cabo un seguimiento de las inversiones extranjeras, las asociaciones y los flujos de propiedad intelectual e industrial para alimentar el control de las inversiones extranjeras directas (IED), el control de las exportaciones y las evaluaciones de riesgos para la seguridad de la investigación. Utilizará sus herramientas para investigar las inversiones que planteen riesgos y trabajar con los Estados miembros para coordinar respuestas rápidas a los intentos de adquisiciones hostiles o a los casos de filtraciones. Con el fin de apoyar los objetivos de seguridad económica, dará prioridad a la financiación y a los proveedores de la UE y afines para los componentes y servicios cuánticos esenciales, y limitará la dependencia de proveedores cuánticos o en la nube de alto riesgo en sectores sensibles. Además, tratará de garantizar que las entidades bajo influencia extranjera indebida no puedan acceder a proyectos cuánticos sensibles.

centrará inmediatamente en las situaciones específicas de alto riesgo determinadas en el proceso de evaluación de riesgos, la Comisión vigilará de cerca, desde la perspectiva de la seguridad económica, todas las industrias clave, como las tecnologías limpias, la energía y las industrias de gran consumo de energía y circulares, el sector agroalimentario, la industria digital y electrónica, la aviación (incluida la aeronáutica), la construcción naval, la automoción y la salud.

3.4. Desarrollar y mantener el liderazgo en tecnologías críticas

El riesgo. Algunos terceros países y empresas han demostrado su interés en adquirir el control de la tecnología y los conocimientos técnicos incipientes o avanzados de la UE. En algunos casos, estas acciones han tenido por objeto poner en peligro la capacidad de la Unión para competir en el terreno de la tecnología. Persiguen este objetivo, por ejemplo, mediante adquisiciones, cooperación en materia de investigación

y desarrollo (I+D), ingeniería inversa o espionaje industrial, pero también mediante la reducción artificial de la cuota de mercado de otras empresas más innovadoras, lo que a su vez se traduce en una menor disponibilidad de ingresos por parte de estas últimas para invertir en I+D de vanguardia. A largo plazo, los resultados económicos, la seguridad y el peso geopolítico de la UE dependerán de nuestra capacidad para mantener y desarrollar nuestras capacidades tecnológicas. Por lo tanto, la conservación de las capacidades de la UE en todas estas tecnologías, mejorando las herramientas de financiación específicas de la UE y abordando la seguridad tecnológica y las fugas de tecnología, reviste una importancia estratégica. Al mismo tiempo, debe prestarse especial atención a la aplicación y el cumplimiento cada vez más fragmentados de los controles de las exportaciones de productos de doble uso.

Objetivo. La Comisión utilizará sus herramientas para apoyar un entorno marco positivo para el desarrollo de tecnologías críticas en la UE y evitar acciones que socaven los esfuerzos de la UE al abordar las distorsiones. Llevará a cabo un seguimiento de la evolución del mercado y prestará un mayor apoyo a la investigación y la innovación en la UE por parte de las empresas emergentes y en expansión, las empresas ya consolidadas, las organizaciones de investigación e innovación y las instituciones académicas. Se centrará en garantizar el despliegue industrial y la puesta en valor de los logros en el campo de la investigación, el desarrollo y la innovación (I+D+i) en la base industrial del mercado interior. El 28.º régimen, que proporciona a las empresas un conjunto único y armonizado de normas a escala de la UE para la constitución de sociedades, su gobernanza, su movilidad y su acceso a la financiación, fortalecerá la resiliencia económica de la UE al permitir operaciones transfronterizas más seguras y cadenas de suministro más sólidas y diversificadas.

La Comisión impulsará la seguridad de la investigación y la innovación, y adoptará las medidas de acompañamiento necesarias para mitigar el riesgo de fuga de tecnología o de conocimientos técnicos, por ejemplo mediante adquisiciones predatorias, la cooperación en materia de I+D y la inversión en mercados estratégicos y emergentes de la UE en destinos o sectores sensibles, al tiempo que seguirá promoviendo asociaciones internacionales de investigación e innovación de confianza, que son vitales para los objetivos de seguridad económica de la Unión. Asimismo, la Comisión estudiará cómo garantizar que las empresas y las organizaciones de investigación e innovación de la UE puedan expandirse y evitar las adquisiciones o transferencias de propiedad impulsadas exclusivamente por la insuficiencia de oportunidades de financiación procedentes de fuentes de confianza. Al mismo tiempo, la Comisión tratará de impedir el acceso de las entidades de alto riesgo a las acciones apoyadas por la Unión en el ámbito de las tecnologías críticas, que pueden utilizarse como arma contra la UE.

3.5. Impedir el acceso a información y datos sensibles que puedan socavar la seguridad económica de la UE

El riesgo. Terceros países podrían obtener acceso a información o datos sensibles de la UE o de sus Estados miembros, ya sea como resultado del espionaje industrial, del suministro por su parte de hardware o software utilizados en determinados productos (por ejemplo, vehículos conectados, 5G u otros sistemas de telecomunicaciones, infraestructura de red eléctrica, plataformas de secuenciación de ADN) o a través de la propiedad y el control de determinadas empresas que posean información o datos sensibles (por ejemplo, operadores portuarios, aeroportuarios y de tráfico, redes financieras, modelos de IA, portales de datos, telecomunicaciones, datos personales o información sensible del mercado). Existen claras implicaciones para la seguridad y el orden público, agravadas por las posibles repercusiones económicas, por ejemplo, relacionadas con la fragmentación de las cadenas de suministro. En el sector de la energía, por ejemplo, este riesgo se extiende a la adquisición por parte de inversores de fuera de la UE de empresas de la Unión que posean tecnologías avanzadas para el seguimiento y el tratamiento de datos operativos procedentes de infraestructuras energéticas críticas.

Objetivo. Reducir y, cuando sea posible, eliminar el riesgo de acceso por parte de entidades de alto riesgo y entidades conexas a información o datos sensibles de la UE o de sus Estados miembros, para limitar así los posibles efectos negativos en la economía y la seguridad de la UE. También se prestará atención al riesgo que pueden plantear los trabajadores extranjeros en sectores estratégicos y los estudiantes extranjeros de educación superior, en particular en los ámbitos de la ciencia, la tecnología, la ingeniería y las matemáticas (CTIM), en consonancia con los procedimientos pertinentes.

3.6. Prevenir y mitigar las perturbaciones en las infraestructuras críticas de la UE que afecten a la economía de la Unión

El riesgo. Las infraestructuras críticas de la UE —incluidas las infraestructuras críticas de transporte, sistemas espaciales, infraestructuras energéticas y de comunicaciones, en particular las consideradas estratégicas para la movilidad militar— se ven perturbadas por agentes

Ejemplo: equipo de detección en las fronteras de la UE (puertos, aeropuertos, fronteras terrestres, etc.)

Riesgo: ausencia de prácticas comunes en toda la UE, dependencia de un solo proveedor o de un número limitado de proveedores, acceso no autorizado (también a través de canales autorizados, por ejemplo, mantenimiento) que afecta al rendimiento del equipo de detección y a la integridad o confidencialidad de la información sensible relacionada, vulnerabilidad a programas maliciosos que podrían comprometer o distorsionar la información, los sistemas o las redes conexas a través del equipo.

Uso de herramientas: sobre la base de la evaluación de riesgos para la ciberseguridad en virtud de la Directiva SRI 2, la Comisión tratará de mitigar los riesgos detectados mediante la determinación de proveedores de alto riesgo, el uso de esquemas de certificación de la ciberseguridad, el refuerzo de las normas de ciberseguridad y la incorporación de requisitos de seguridad en las licitaciones de contratación pública. La Comisión evaluará el papel que pueden desempeñar las subvenciones extranjeras, en particular si otorgan una ventaja competitiva a determinados proveedores.

extranjeros, lo que podría tener efectos en cascada en la economía europea. La atención se centrará en garantizar la estabilidad de los servicios prestados. Las perturbaciones podrían producirse a través de ataques físicos, cibernéticos o híbridos, incluido el sabotaje de instalaciones enteras o de sus partes o subcomponentes. También podrían estar vinculadas a las cadenas de suministro de TIC, que sustentan componentes o servicios esenciales para infraestructuras críticas. Existe asimismo el riesgo de que terceros países y operadores de alto riesgo tomen posiciones en las infraestructuras críticas de la UE con vistas a adquirir la capacidad de perturbarlas (si lo necesitan y en el momento en que lo precisen). Además, existe un riesgo para la reputación y la credibilidad si determinadas infraestructuras están amenazadas o se ven realmente afectadas. Por último, existe el riesgo de que terceros países asuman un papel de liderazgo en el establecimiento de normas internacionales, lo que podría afectar a infraestructuras críticas.

Ejemplo: inversores solares

Riesgo: la dependencia creciente respecto de un único proveedor; riesgos cibernéticos (manipulación de los parámetros de producción de electricidad, impedimentos a la producción de electricidad, acceso a datos operativos, infiltración entre los agentes de la cadena de suministro).

Uso de herramientas: la Comisión seguirá evaluando los riesgos cibernéticos mediante una evaluación coordinada en el marco de la Directiva SRI 2 (que concluirá en 2026). Sobre esta base, aplicará medidas de mitigación centradas tanto en el fortalecimiento de la preparación (por ejemplo, el Reglamento sobre la preparación frente a los riesgos en el sector de la electricidad o la Directiva relativa a la resiliencia de las entidades críticas) como en el abordaje de las vulnerabilidades detectadas, recurriendo, por ejemplo, a las actuaciones siguientes: certificación y normalización en el marco del Reglamento de Ciberresiliencia y criterios no relacionados con los precios en el marco del Reglamento sobre la Industria de Cero Emisiones Netas. La Comisión llevará a cabo un seguimiento de la evolución del mercado y tratará de prevenir o mitigar las inversiones de alto riesgo. La Comisión seguirá evaluando el papel de las subvenciones extranjeras que puedan distorsionar la igualdad de condiciones en los mercados de la energía solar, principalmente a través de importaciones subvencionadas.

Objetivo. En consonancia con las estrategias pertinentes de la UE en materia de defensa, seguridad interior y preparación, hacer cumplir las normas existentes para reducir el riesgo de filtración o espionaje de datos y de perturbaciones físicas y cibernéticas, en particular a través de: i) **el establecimiento de límites a la propiedad, el control y la explotación** de infraestructuras europeas críticas **por parte de entidades de alto riesgo**; ii) el aumento de las medidas de **protección física**; iii) la **limitación de las cibervulnerabilidades**; y iv) la **limitación de la dependencia de proveedores únicos o de alto riesgo**, así como de las vulnerabilidades ocultas, las puertas traseras o las posibles perturbaciones sistémicas del suministro de tecnologías de la información y de las comunicaciones (TIC), en particular en casos de dependencia tecnológica o de proveedores; v) la **reserva de capacidades críticas de fabricación de la UE** con

posibilidades de expansión en tiempos de perturbaciones de las cadenas de suministro mundiales o de crisis sanitarias; vi) la Comisión **impedirá el acceso de las entidades de alto**

riesgo a las acciones apoyadas por la Unión, incluidas las apoyadas por entidades e instrumentos financieros públicos; vii) el apoyo al **desarrollo de proveedores fiables de subcomponentes críticos** en la UE y en terceros países de confianza, de modo que existan alternativas viables; viii) el apoyo a **iniciativas emblemáticas** en los ámbitos de la defensa y afines (guardia del flanco oriental, Iniciativa Europea de Defensa Antidrones).

4. Acciones dirigidas a reforzar la seguridad económica de la UE

El acceso a información de calidad y su análisis exhaustivo son el punto de partida para una política y una toma de decisiones eficaces y correctamente fundamentadas en lo relativo a la seguridad económica de la UE. El sistema de evaluación de riesgos puesto en marcha por la Estrategia de 2023 seguirá ocupando un lugar central en estos esfuerzos. Las evaluaciones existentes se actualizarán, profundizarán y complementarán con otras nuevas en todas las tecnologías y cadenas de suministro críticas.

La Comisión seguirá desarrollando su capacidad de recopilación de información sobre la seguridad económica. Acelerará la **cartografía de las dependencias estratégicas a lo largo de las cadenas de valor que dan lugar a vulnerabilidades en la economía de la Unión** y reforzará la **vigilancia y la anticipación de las acciones de terceros países** destinadas a crear nuevas dependencias o a mantener las existentes.

Además, el éxito de la política de seguridad económica de la UE dependerá de una **mayor coordinación tanto a escala de la UE como con los Estados miembros**. Esto incluye la creación de un entendimiento común de las amenazas para la seguridad económica, la determinación de riesgos concretos y el desarrollo de medidas de mitigación. Todo ello debería estar respaldado por mejores flujos de información, una comprensión plena de los costes y beneficios de la acción de la UE, y la voluntad de actuar conjuntamente cuando sea necesario, situando a la UE en una posición de fuerza. La Comisión ha adoptado las medidas organizativas internas necesarias, pero esto también requiere una nueva forma de trabajar con los Estados miembros, y cada vez más entre los propios Estados miembros y dentro de ellos, especialmente en lo que se refiere a ámbitos de actuación cada vez más estratégicos pero tradicionalmente descentralizados, como la investigación y la innovación.

La UE seguirá colaborando estrechamente con la **industria** para garantizar un intercambio de información seguro y un compromiso más estructurado. La industria está en primera línea de la seguridad económica de la UE. Las empresas deben ser más resilientes y diversificar sus cadenas de suministro críticas, en particular mediante la eliminación de la dependencia total de un único proveedor de alto riesgo. También es fundamental integrar en sus modelos de negocio los costes que conlleva una mayor diversificación, reconociendo el beneficio que aporta la resiliencia frente a los riesgos geopolíticos. Este proceso debe ser **bidireccional** y constituir una **responsabilidad compartida entre el sector público y el sector privado**, de manera que permita a los responsables de la formulación de políticas mejorar la capacidad de evaluación de amenazas y de inteligencia empresarial de la UE y prepararla para la acción, ayudando al mismo tiempo a la industria a aplicar medidas de mitigación a nivel de empresa.

La Comisión, con el apoyo de la alta representante:

→ Mejorará su **capacidad de recopilación y análisis** de información; para ello, agilizará las

evaluaciones de riesgos sobre determinadas cadenas de suministro, infraestructuras y tecnologías críticas, y pondrá en marcha **convocatorias periódicas de datos** para obtener aportaciones de la industria y las partes interesadas sobre las vulnerabilidades de la cadena de suministro y la exposición a la presión externa.

- Promoverá una **coordinación y un intercambio de información mayores a través de su red de seguridad económica con los Estados miembros**. La Comisión utilizará dicha red para fomentar el desarrollo de escenarios, armonizar la comprensión de las amenazas, los riesgos y las posibilidades de mitigación, facilitar el intercambio de información y apoyar la aplicación, en particular en lo que se refiere al uso de herramientas que son competencia de los Estados miembros. En este contexto, la Comisión velará por que se disponga de sistemas de información adecuados para apoyar el **intercambio rápido y seguro de información clasificada entre los Estados miembros y con ellos** sobre cuestiones de seguridad económica, incluidas las evaluaciones de riesgos, las entidades críticas y de alto riesgo y las transacciones que puedan suscitar preocupación. Esto complementará la labor de la red de almacenamiento de reservas de la UE, que se centra en garantizar el suministro de artículos esenciales en situaciones de crisis.
- Creará un **Centro de Información sobre Seguridad Económica** en el que, con el apoyo del Servicio Europeo de Acción Exterior (SEAE), el SITCEN/SIAC³, la red de delegaciones de la UE y los Estados miembros, así como de las herramientas existentes para el seguimiento del mercado interior, como la metodología SCAN («Notificación de alerta de la cadena de suministro»); cartografiará y consolidará la información disponible en el marco de los mecanismos existentes y coordinará la recopilación de información adicional pertinente para la seguridad económica. Esto incluirá un **mecanismo de seguimiento del mercado** para recopilar información sobre la evolución en ámbitos de alto riesgo, incluida información rápida sobre los flujos comerciales en sectores sujetos a diversificación para garantizar que la acción de la UE no se vea socavada. Además, consolidará la información **sobre las entidades de alto riesgo** para apoyar el proceso de evaluación de la admisibilidad para recibir financiación de la UE y la participación en un proceso de inversión o contratación pública de la UE. Por otro lado, la Autoridad Aduanera de la Unión Europea y el Centro Aduanero de Datos de la UE permitirían **apoyar y hacer cumplir eficazmente la aplicación de las iniciativas conexas de seguridad económica de la UE**, facilitando también el intercambio de información pertinente.
- Intensificará la **colaboración estructurada de las delegaciones de la UE**, mediante el mantenimiento de contactos con las misiones de los Estados miembros, otros organismos de la UE y la comunidad empresarial de la UE presente en terceros países con el fin de

³ El Centro de Inteligencia y de Situación de la Unión Europea (INTCEN) del Servicio Europeo de Acción Exterior forma parte de la Capacidad Única de Análisis de Inteligencia (SIAC) de la UE y es el centro de inteligencia civil de la UE, que proporciona análisis en profundidad a los responsables de la toma de decisiones en todas las instituciones de la Unión.

garantizar contribuciones eficaces a las evaluaciones, el seguimiento y la mitigación de los riesgos relacionados con la seguridad económica, en particular mediante la facilitación de intercambios entre empresas y entre estas y las administraciones públicas.

- Evaluará, a más tardar en el tercer trimestre de 2026, en qué medida el Reglamento de Emergencia y Resiliencia del Mercado Interior permite recopilar información a nivel de empresa sobre la cadena de suministro de las empresas pertenecientes a sectores de alto riesgo. A la luz de este análisis, la Comisión evaluará la necesidad de adoptar nuevas medidas.
- Recomendará que los Estados miembros designen **asesores nacionales de seguridad económica** de alto nivel y les encomienden la responsabilidad de coordinar en sus respectivas administraciones la evaluación y mitigación de los riesgos para la seguridad económica. La Comisión promoverá una mayor coordinación de las políticas y acciones conjuntas **reuniendo periódicamente a estos asesores**. Asimismo, invita al Consejo de la UE a que considere la posibilidad de convocar periódicamente a las formaciones pertinentes del Consejo para celebrar debates políticos.
- Creará un **grupo de asesores de confianza compuesto por representantes de empresas de la UE** para, entre otras cosas, prestar asesoramiento sobre riesgos específicos y posibles respuestas, así como para debatir acerca de estrategias de reducción del riesgo. La Comisión invitará periódicamente a representantes de la industria a participar en los debates sectoriales de la red de seguridad económica y, cuando proceda, a informar a los comisarios europeos.
- Creará un **portal de información sobre resiliencia comercial** para proporcionar a las empresas de la UE información actualizada, como parte del portal de acceso a los mercados (A2M), sobre las restricciones a la exportación y otras medidas restrictivas impuestas por terceros países, así como sobre los posibles riesgos relacionados con la necesidad de reforzar la resiliencia de la UE.
- Ampliará el **Observatorio de Tecnologías Críticas** para identificar, supervisar y analizar la industria espacial y de defensa y las cadenas de suministro conexas, así como para abarcar las tecnologías emergentes y apoyar la aplicación a escala nacional y de la UE de las hojas de ruta tecnológicas resultantes de la UE.
- Utilizará el futuro **Centro de Asesoramiento sobre Seguridad de la Investigación** para promover la seguridad de la investigación y aumentar la resiliencia de la comunidad investigadora, en particular mediante el desarrollo de una plataforma de diligencia debida para ayudar a las universidades a elegir a sus socios internacionales.
- Explorará formas de alinear e **integrar a los países candidatos con nuestro enfoque de seguridad económica**, especialmente en aquellos ámbitos en los que sus vulnerabilidades en materia de seguridad económica puedan suponer un riesgo para la seguridad de la UE.

Sobre la base de un análisis y una gobernanza reforzados, la UE puede perseguir mejor sus objetivos de seguridad económica i) aclarando y mejorando el despliegue de las herramientas existentes y ii) desarrollando nuevas herramientas cuando sea necesario.

En primer lugar, **la Comisión adaptará el modo en que utiliza algunas de sus herramientas** para hacerlas más eficaces en la gestión de los riesgos para la seguridad económica y tratará de mejorar la coordinación entre esas herramientas.

La Comisión adoptará las medidas siguientes para mejorar el uso de las herramientas:

→ Financiación de la Unión:

- En adelante, la Comisión **incentivará en sus actividades de financiación proyectos que apoyen la seguridad económica de la UE.**
- En particular, deberá movilizar un nivel suficiente de financiación para reducir las dependencias de tecnologías, componentes y materiales críticos, especialmente en sectores estratégicos como el espacio y la defensa, en particular para aplicar plenamente las hojas de ruta tecnológicas del Observatorio de Tecnologías Críticas.
- La Comisión, los Estados miembros y las entidades gestoras asociadas deberán tratar de impedir el acceso de las entidades de alto riesgo a las acciones sensibles apoyadas por la Unión. El artículo 136 del Reglamento Financiero proporciona una base jurídica horizontal para proteger la seguridad y el orden público de la UE cuando la Comisión y las entidades gestoras asociadas ejecutan el presupuesto de la UE. Esto permite impedir que las entidades de alto riesgo se beneficien de los fondos de la UE, así como restringir el acceso a los fondos de la UE en sectores estratégicos y en los ámbitos de la tecnología y las infraestructuras críticas por parte de entidades procedentes de terceros países que socavan los intereses de la UE en materia de seguridad económica. Para evitar dudas, las entidades gestoras asociadas deben abstenerse de apoyar proyectos que contradigan lo anterior, incluso en las operaciones que realicen por su cuenta y riesgo. A tal fin, y para garantizar una mejor armonización de las políticas entre los programas de la UE y los objetivos de seguridad económica, se proporcionarán orientaciones en el primer trimestre de 2026, apoyando así el desarrollo de un enfoque más cohesionado y eficaz. Asimismo, la Comisión animará a los Estados miembros, al **Grupo Banco Europeo de Inversiones (Grupo BEI) y a otras instituciones financieras internacionales, bancos e instituciones nacionales de fomento que estén ejecutando presupuestos nacionales o de la UE** a priorizar el apoyo a las empresas de la UE que reduzcan las dependencias respecto del extranjero en sectores críticos, especialmente en proyectos específicos, tecnologías críticas e infraestructuras críticas identificadas como de alto riesgo. Del mismo modo, debe impedirse que los proveedores de alto riesgo de terceros países accedan a financiación nacional y de la Unión cuando se determine, sobre la base de criterios específicos, que dichos terceros países socavan los intereses de la Unión en materia de seguridad económica.

→ Control de las IED:

- La Comisión elaborará **directrices** basadas en la experiencia adquirida con la aplicación del actual Reglamento para el control de las inversiones extranjeras directas a fin de garantizar que las autoridades nacionales de control aborden el control de manera coherente, incluso en sectores estratégicos. En las directrices se explicaría además cómo tener en cuenta el riesgo acumulativo potencial de las múltiples inversiones. Esto se complementará con orientaciones sobre la interacción entre cualquier requisito a escala de la UE y la aplicación de mecanismos nacionales de control en el sector financiero.

→ Controles de las exportaciones de productos de doble uso:

- La Comisión llevará a cabo una **evaluación global** del Reglamento sobre el control de las exportaciones de productos de doble uso. Como parte de esta evaluación, la Comisión valorará si el Reglamento alcanza sus objetivos en el contexto de las nuevas realidades geopolíticas y geoeconómicas, incluidas las repercusiones del creciente recurso a controles unilaterales que también pueden afectar al mercado interior. Seguirá explorando con los Estados miembros la manera de adoptar eficazmente controles europeos en ámbitos tecnológicos emergentes en este nuevo contexto. Durante el proceso de evaluación, la Comisión garantizará un acercamiento activo a las partes interesadas de los Estados miembros, la industria, los institutos de investigación y el mundo académico.

→ Instrumentos de defensa comercial:

- Cuando se inicie un caso de relevancia para la seguridad económica de la UE, **esta se reflejará en el desarrollo de la investigación y en el diseño de posibles medidas.**

→ Herramientas en el ámbito del mercado interior, las aduanas y la defensa de la competencia:

- Se hará pleno uso del **Reglamento sobre subvenciones extranjeras** para mantener la competencia leal en ámbitos en los que las subvenciones extranjeras den lugar a distorsiones que planteen riesgos para la seguridad económica.
- Se animará a los Estados miembros a que hagan pleno uso de las posibilidades que ofrecen las ayudas estatales existentes, como el marco de ayudas estatales para una industria limpia, las Directrices sobre ayudas regionales, el marco de investigación, desarrollo e innovación, el Reglamento general de exención por categorías y los proyectos importantes de interés común europeo, como instrumentos para aumentar la resiliencia.
- **Se revisará el uso de instrumentos aduaneros estratégicos (suspensiones arancelarias, contingentes autónomos) para insumos clave** con vistas a apoyar la competitividad de las empresas de la Unión.

En segundo lugar, la Comisión **desarrollará nuevas medidas** para promover la seguridad económica de la UE.

La Comisión:

- Estudiará la posibilidad de implantar con carácter piloto un **mecanismo de supervisión de las empresas emergentes a escala de la UE** destinado a **identificar las empresas emergentes en ámbitos tecnológicos críticos que sean vulnerables al riesgo de adquisiciones hostiles por parte de entidades extranjeras**, reorientándolas hacia alternativas de inversión de la UE y otras formas de apoyo (por ejemplo, asesoramiento, desarrollo de capacidades, establecimiento de contactos con inversores). Este mecanismo funcionaría en paralelo a las iniciativas existentes, como la Estrategia de la UE para las Empresas Emergentes y en Expansión.
- Trabajará con las autoridades de supervisión para vigilar las **inversiones de cartera** (que quedan fuera del ámbito de aplicación del mecanismo de coordinación de las IED) en ámbitos considerados de alto riesgo a efectos de seguridad económica.
- Incluirá un componente de seguridad económica para sectores estratégicos clave en la próxima **herramienta de coordinación de la competitividad**.
- Reforzará la base industrial y la resiliencia de las cadenas de suministro de la UE a través de la **Ley de Aceleración Industrial**.
- Como se indica en ResourceEU, seguirá desarrollando **mercados secundarios** para las materias primas fundamentales, también a través de la Ley de Economía Circular, para facilitar la financiación de proyectos estratégicos relacionados con las materias primas fundamentales en ámbitos considerados de alto riesgo con fines de seguridad económica.
- Evaluará, a más tardar en el tercer trimestre de 2026, las formas de **reforzar la protección de la industria frente a las políticas comerciales desleales y la evolución negativa del mercado mundial, como el exceso de capacidad**. En este caso, la Comisión evaluará la eficacia y la adecuación de las herramientas existentes y considerará la necesidad de posibles nuevas medidas.
- Revisará el **estatuto de bloqueo** para simplificar su aplicación y reducir los costes de cumplimiento para las personas y las empresas de la UE, así como para crear un elemento disuasorio creíble contra la aplicación extraterritorial de sanciones de terceros países. Esto reforzará la seguridad económica europea al proteger mejor a los operadores de la UE frente a medidas opuestas de terceros países y al garantizar un marco más previsible, eficaz y asertivo.
- Estudiará las modalidades para alentar a las empresas de sectores específicos de alto riesgo a garantizar que **los suministros procedan de al menos dos proveedores diferentes** y limitar la exposición a un único proveedor dominante.
- Explorará la posibilidad de prestar **apoyo financiero a las empresas sujetas a decisiones de control de las IED** en situaciones en las que su viabilidad financiera pueda estar en peligro en ausencia de inversiones, sin perjuicio de las normas sobre ayudas estatales.

- Como parte de la revisión de las Directivas sobre contratación pública, **propondrá criterios de preferencia europea en sectores estratégicos específicos** en los que la contratación pública de la UE estimule la demanda de liderazgo industrial europeo, aumente nuestra resiliencia y mitigue los riesgos para la seguridad.
- Incentivará a las empresas para que **reduzcan las dependencias en ámbitos tecnológicos emergentes** como parte del próximo Reglamento de Chips 2.0, el Reglamento Cuántico, la Ley de desarrollo de la computación en la nube y la inteligencia artificial y la estrategia de software de código abierto de la Comisión.
- Utilizará la próxima revisión del **Reglamento sobre la Ciberseguridad** para imponer a escala de la UE restricciones de acceso a las infraestructuras críticas para los proveedores de alto riesgo.

5. Conclusión

La UE mantiene su firme compromiso con el comercio abierto y basado en normas, las relaciones en materia de inversión y la cooperación internacional. Por lo tanto, seguirá apoyando el comercio abierto y la inversión con socios de todo el mundo y beneficiándose de ellos. Al mismo tiempo, en el entorno geopolítico actual, es imperativo salvaguardar la seguridad económica de la UE. Para proteger a la UE, así como para nuestra seguridad en general y para la competitividad de nuestra industria, es fundamental hacer frente a los riesgos que conlleva la apertura.

La UE ya dispone de numerosos instrumentos para perseguir este objetivo. Estos instrumentos deben utilizarse ahora de manera estratégica y, en caso necesario, perfeccionarse aún más, tanto para disuadir de forma creíble las amenazas a la seguridad económica de la UE antes de que se produzcan como para responder eficazmente a ellas cuando surjan. Para lograrlo, es necesario que la Comisión, el Parlamento Europeo y los Estados miembros trabajen al unísono y cooperen estrechamente con la industria en pos de una toma de decisiones eficiente y fundamentada.

La UE está decidida a hacer un uso más proactivo, estratégico y coordinado de todas las herramientas disponibles para construir una economía fuerte, segura y resiliente a largo plazo, así como a operar eficazmente en las nuevas condiciones geopolíticas y geoeconómicas que configuran el comercio mundial.