CEOE Empresas Españolas

Liderar
Defender
Impulsar
Promover

Informe Internacional

Comparativa del estado de la seguridad económica en países seleccionados: EE.UU., Japón, Corea del Sur, Reino Unido, Australia, India, Canadá y Singapur

Mayo 2024

Contenido

1. CONTEXTO

La seguridad económica ha adquirido especial relevancia en la actualidad fruto de la creciente rivalidad competitiva entre los estados. Se trata de un concepto poco claro, que puede ser objeto de todo tipo de interpretaciones. Por ello, hemos considerado oportuno atenernos a la **Declaración del G7 de Hiroshima sobre la Resiliencia Económica y Seguridad Económica**, del 20 de mayo de 2023.

En esta declaración impulsada por Japón, por **seguridad económica puede** entenderse todas aquellas medidas orientadas a reforzar la resiliencia de las cadenas de suministro y las infraestructuras críticas, mejorar la respuesta a las prácticas nocivas que socavan las reglas internacionales e intensificar la cooperación internacional en cuanto a la estandarización.

Se trata de un documento que sirve de orientación a las políticas de seguridad económica de los países del G7 y de otros países cercanos, además de la Unión Europea, y que pone un especial acento en un **esfuerzo coordinado** entre los países afines.

El objetivo del presente documento consiste en analizar modelos de seguridad económica existentes fuera de la Unión Europea, poniendo especial énfasis en los modelos de seguridad económica de los países del G7 situados fuera de la UE (Estados Unidos, Canadá, Japón y Reino Unido), y de países afines (Australia, Corea del Sur, India y Singapur), con el fin de sacar conclusiones y ayudarnos en nuestros trabajos en materia de seguridad económica.

2. ESTADOS UNIDOS

2.1. Introducción

Estados Unidos **cuenta con una estrategia oficial** de seguridad económica bien definida. Dispone de un **conjunto de iniciativas** muy desarrolladas y actualizadas, que intentan dar una respuesta coherente y global a las vulnerabilidades que presentan ciertas interdependencias externas.

La primera mención importante de seguridad económica debe encontrarse en la **estrategia de seguridad nacional de 2017** publicada bajo la Presidencia Trump, donde se señala que "*la seguridad económica es la seguridad nacional".* Este primer paso, que dio lugar a los primeros cambios en materia legislativa, fue reforzado de manera contundente durante la Presidencia de Biden, como quedó bien reflejado en el documento de la Casa Blanca de 21 de **junio de 2021 "Building Supply Chains, Revitalizing American Manufacturing, and Fostering Broad- Based Growth".** Este documento elaborado por el Consejo de Seguridad Nacional, en coordinación con los Departamentos de Comercio, Energía, Defensa y Salud, pone especial énfasis en la producción y las cadenas de suministro de los semiconductores, las baterías de gran capacidad, los minerales críticos y las medicinas, además de sustancias e ingredientes.

Este enfoque adquirió aún más solidez a raíz de la publicación por la Casa Blanca de la **nueva Estrategia de Seguridad Nacional en octubre de 2022**, que, bajo una visión más global, hace hincapié en el desarrollo de una estrategia industrial y de innovación, en la seguridad climática y energética, el comercio y la economía, el control de armas y la proliferación, la ciberseguridad y la seguridad alimentaria, entre otros aspectos.

2.2. Marco institucional

Un signo distintivo del modelo estadounidense son los **poderes discrecionales concedidos al presidente** de los Estados Unidos en los ámbitos de la seguridad nacional y la seguridad económica, una tradición que tiene su origen en la legislación Trading With the Enemy Act (TWEA), promulgada en 1917, con ocasión de la entrada de los Estados Unidos en la Primera Guerra Mundial. El fuerte carácter presidencialista del sistema político estadounidense también explica el importante papel que despeña el **Consejo de Seguridad Nacional adscrito a la Oficina del presidente de Estados Unidos**, que tiene, entre sus principales objetivos, definir la estrategia de seguridad

nacional y coordinar los departamentos y agencias implicados. Destaca el papel que desempeñan en materia de seguridad económica tres departamentos, como son los de Comercio y Tesoro, por medio de sus agencias **Bureau of Industry and Security (BIS),** responsable del control de exportaciones, y **Office of Foreign Assets Control (OFAC)**, responsables de la aplicación del régimen de sanciones económicas. El Tesoro también regula control de inversiones extranjeras. Otra agencia relevante es la **Strategic Industries and Economic Security (SIES),** dependiente del Departamento de Interior, que apoya la seguridad nacional y el desarrollo de la base industrial estadounidense colaborando con otras agencias y en programas internacionales. Desempeña un importante papel el Comité de Inversión Extranjera (CFIUS) de cara a la identificación del peligro que pueda suponer una inversión extranjera en la seguridad nacional, en coordinación con BIS. SIES y BIS, además del Departamento de Defensa, asumen parte de las funciones recogidas en la legislación **Defense Production Act.**

2.3. Sanciones económicas

En este ámbito, tenemos que destacar la **Ley de Poderes Económicos de Emergencia Internacional (IEEPA),** de 1983, una ley federal, que otorga amplios poderes al Presidente de EE.UU., al permitirle declarar la emergencia nacional cuando estén amenazadas la seguridad nacional, la política exterior o la economía de los Estados Unidos, así como imponer sanciones, bloquear activos y restringir el comercio. Su funcionamiento destaca, a diferencia de otros modelos nacionales, por su rapidez, una vez declarada la emergencia nacional.

En la legislación IEEPA reside la facultad del presidente de Estados Unidos para **imponer sanciones económicas**. IEEPA sirvió también de base legal para la adopción de reglas de **control de exportaciones de doble uso** cuando expiraba en su vigencia la legislación **Export Administration Act (EAA).**

En la actualidad, sirve aún de base legal para la adopción de reglas de control de exportaciones en aquellos ámbitos normativos que no estuvieren en conflicto con la Ley de Reforma de Control de Exportaciones, de 2018. El régimen de sanciones es gestionado por la oficina dependiente del Departamento del Tesoro, **Office of Foreign Assets Control (OFAC)**.

2.4. Control de exportaciones

La Ley de Reforma de Control de Exportaciones (ECRA), de 2018, supone un hito importante en la regulación del control de las exportaciones. Ello es así, no

tanto por el hecho de que siga otorgando amplios poderes al presidente de los Estados Unidos, sino por la posibilidad de restringir la exportación de **tecnologías emergentes y fundamentales con potencial de uso dual**[1] **(tanto físicas como digitales)**.

Entre sus disposiciones se faculta al presidente a iniciar un **proceso interinstitucional para establecer nuevos controles sobre tecnologías emergentes y fundamentales**. También se prevé una revisión de los requisitos para **conceder licencias** a las exportaciones, las reexportaciones o las transferencias internas de artículos a países sujetos a un embargo de armas comprensivo de los Estados Unidos; procedimientos de licencias para evaluar el impacto de una exportación propuesta en la base industrial de defensa de EE. UU.; un examen de los intereses de propiedad extranjera del consignatario, una revisión y evaluación de los procedimientos de referencia.

En virtud de ello, la oficina dependiente del Departamento de Comercio, **Bureau of Industry and Security (BIS)** identificó en noviembre de 2018 las siguientes **tecnologías como emergentes**: fabricación aditiva, tecnología informática avanzada, materiales avanzados, tecnología de vigilancia avanzada, inteligencia artificial y aprendizaje automático, biotecnología, interfases cerebro-computadora, tecnología de análisis de datos, hipersónicos, tecnologías logísticas, microprocesadores, tecnologías de posición, navegación y cronometraje (PNT), computación cuántica y tecnología de reconocimiento y detección, robótica.

Partiendo de esta base de trabajo, **BIS aprobó controles sobre las siguientes tecnologías emergentes**: software especialmente diseñado para automatizar el análisis de imágenes geoespaciales, cámaras de cultivo de un solo uso con paredes rígidas que pueden utilizarse para manipular armas biológicas y precursores químicos, "software" capaz de utilizarse para operar ensambladores y sintetizadores de ácido nucleico con el fin de generar patógenos y toxinas sin necesidad de adquirir elementos y organismos genéticamente controlados (propuesto). Por otro lado, también agregó las tecnologías definidas por acuerdos multilaterales (Acuerdo de Wassenaar).

En una segunda etapa, concretamente el 27 de agosto de 2020, BIS emitió una **propuesta de regulación buscando orientación pública sobre el control de**

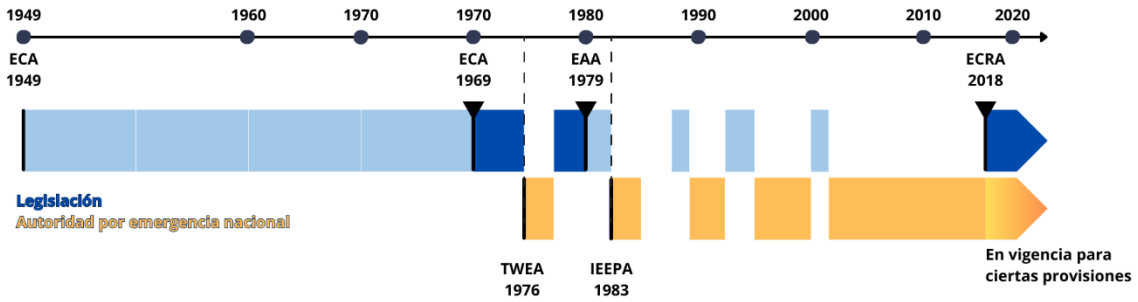
[1] Los bienes de doble uso son productos, software o tecnologías que tienen aplicaciones tanto civiles como militares.

"tecnologías fundamentales", las cuales describió como "aquellas que podrían requerir controles más estrictos si una aplicación o capacidad actual o potencial de esa tecnología representa una amenaza para la seguridad nacional de los Estados Unidos". Además, también sugirió algunas posibles categorías para el control, como elementos o tecnologías controladas para usos finales y usuarios finales militares, incluyendo elementos que podrían ayudar a la innovación militar en China, Rusia o Venezuela; utilizadas o necesarias para la innovación en el desarrollo de armas convencionales o armas de destrucción masiva, o para habilitar actividades de recolección de inteligencia militar extranjera o sujetas a actividades de adquisición ilícita.

Otro hito importante es la aprobación en octubre de **2022 de nuevas regulaciones por BIS para controlar la exportación de tecnología de computación avanzada y semiconductores.** Además, se han introducido requisitos de licencia y se ha ampliado el alcance de los reglamentos de exportación para proteger los intereses de seguridad nacional y política exterior de los Estados Unidos. Asimismo, se ha establecido una Licencia General Temporal para mitigar el impacto a corto plazo en la cadena de suministro de semiconductores.

BIS no es la única agencia que publica listados de tecnologías críticas y emergentes. Así, por ejemplo, la Casa Blanca publicó la **Estrategia Nacional de Tecnologías Críticas y Emergentes (National Strategy for Critical and Emerging Technologies),** que incluye en uno de sus anexos una lista de tecnologías críticas y emergentes. En 2020, 2022 y 2024, la Casa Blanca ha publicado **listas actualizadas de tecnologías críticas y emergentes**. Estas listas, que son consistentes con la lista de BIS de 2018, intentan reflejar un entorno tecnológico cambiante, y servir de guía y orientación.

A modo de resumen para entender esta legislación, se adjunta el siguiente gráfico:



Fuente: elaboración propia mediante datos de Congressional Research Service, 2021.

Por último, cabe mencionar que EE. UU., junto con otros países, entre los que destacan Canadá, India, Australia, Japón y Corea del Sur, forma parte de los siguientes acuerdos internacionales referentes al control de exportaciones:

- Acuerdo de Wassenaar sobre controles de exportación de armas. convencionales y bienes y tecnologías de doble uso.
- Grupo de Australia.
- Grupo de Suministradores Nucleares.
- Régimen de control de tecnología de misiles.

2.5. Escrutinio de inversiones

El control de **inversiones entrantes** en Estados Unidos es competencia del **Comité de Inversión Extranjera (CFIUS** de ahora en adelante). CFIUS es un comité interinstitucional autorizado para revisar ciertas transacciones que involucran la inversión extranjera en los Estados Unidos, así como ciertas transacciones inmobiliarias realizadas por extranjeros, con el fin de determinar el efecto de dichas transacciones en la seguridad nacional de los Estados Unidos.

Las operaciones de este comité se realizan en conformidad con lo establecido en la sección 721 de la Ley de Producción de Defensa de 1950. Fue objeto de una primera revisión sustancial mediante la promulgación de la Ley de Inversión Extranjera y Seguridad Nacional de 2007 (FINSA), y de una posterior reforma por medio de la **Ley de Modernización de Revisión de Riesgos de Inversión Extranjera de 2018 (FIRMMA),** que otorgó más facultades a CFIUS.

De acuerdo con esta legislación:

- El Departamento del Tesoro promulgó directrices concernientes a la imposición de sanciones y otras medidas en relación con FIRMMA, facultando al CFIUS a **examinar, bloquear e incluso deshacer ciertas transacciones** que implican inversiones extranjeras en empresas u operaciones estadounidenses susceptibles de comprometer la seguridad nacional y afectar el liderazgo tecnológico de los Estados Unidos en áreas de relevancia para la seguridad nacional.
- Se amplía la competencia del comité para las **tecnologías emergentes,** se han incorporado nuevos criterios de seguridad nacional a ser considerados por el CFIUS y se ha fortalecido su capacidad para salvaguardar las **infraestructuras críticas**. Complementariamente, se ha incorporado el requisito de presentar una **declaración obligatoria** (en esencia, una notificación previa) al CFIUS para ciertas inversiones realizadas por entidades no estadounidenses en empresas del país

que se dediquen a la producción, diseño, prueba, fabricación o desarrollo de una o más tecnologías críticas.

- Asimismo, CFIUS está también facultado para imponer **sanciones pecuniarias y buscar otras formas de reparación** (tales como notificaciones dirigidas o planes de acción) por infracciones de la Sección 721, órdenes, imposición de requisitos o acuerdos de mitigación.

Mediante la **orden ejecutiva 14083 del 15 de septiembre de 2022**, se actualiza la lista de riesgos para la seguridad nacional y se enfatiza la necesidad de revisar las inversiones extranjeras en empresas estadounidenses para salvaguardar los intereses de seguridad nacional.

Por otro lado, respecto al control de **inversiones salientes**, el 9 de agosto de 2023, Joe Biden, emitió la **orden ejecutiva 14105** para regular ciertos tipos de inversiones salientes de Estados Unidos en **tecnología crítica, materiales e infraestructura críticos,** que tuvieran como destino una lista de "países o territorios preocupantes" *(countries of concern)*, donde esta inversión podría ser una amenaza para la seguridad nacional. Esta lista está compuesta por China, Hong Kong y Macao. Con ella, las inversiones salientes de los Estados Unidos en estas tecnologías o subconjuntos de estas que tengan como destino esos territorios, estarán sujetas a reglas de notificación (transacciones notificables) y, en casos extremos (que involucran entidades que son propiedad o están controladas por, o tienen vínculos estrechos con, adversarios extranjeros), prohibidas (transacciones prohibidas). El Departamento de Tesoro está aún trabajando en el desarrollo legal del decreto presidencial.

2.6. Política Industrial

En este ámbito, caben destacarse las siguientes iniciativas:

- **Defense Production Act,** promulgada durante la Guerra de Corea el 8 de septiembre de 1950, concede al presidente amplias facultades para exigir que las empresas prioricen la producción y contratación de equipos y materiales necesarios para la defensa nacional. Entre marzo de 2022 y diciembre de 2023, la Administración Biden ha hecho uso de esta legislación para impulsar la producción minera, de tecnologías verdes, de la base industrial hipersónica, la IA y el refuerzo de las cadenas de suministro de medicinas.

- **Infrastructure Investment and Jobs Act,** de 15 de noviembre de 2021, pretende, mejorar y extender las infraestructuras viarias, ferroviarias y de agua en el país.
- **Chips and Science Act**, del 9 de agosto de 2022, es una ley federal que pretende apoyar la investigación y desarrollo de tecnologías avanzadas, así como promover la educación en ciencias y tecnología.
- **Inflation Reduction Act (IRA)** del 16 de agosto de 2022, dirige nuevos gastos federales hacia la reducción de las emisiones de carbono, la disminución de los costos de atención médica, la financiación del Servicio de Impuestos Internos y la mejora del cumplimiento tributario. La ley tiene como objetivo catalizar inversiones en capacidad de fabricación nacional, fomentar la adquisición de suministros críticos de manera nacional o de socios comerciales de libre comercio, e impulsar la I + D y la comercialización de tecnologías de vanguardia como la captura y almacenamiento de carbono y el hidrógeno limpio.

2.7. Ciberseguridad

La regulación de ciberseguridad en los Estados Unidos está dividida entre leyes federales y estatales. La Comisión Federal de Comercio (FTC) es responsable de hacer cumplir las regulaciones y legislaciones de ciberseguridad a nivel federal. Además, el Departamento de Seguridad Nacional (DHS) y el Instituto Nacional de Normas y Tecnología (NIST) también tienen roles en la regulación de la ciberseguridad.

La ley principal que rige la ciberseguridad en los Estados Unidos es **la Ley de la Comisión Federal de Comercio FTCA (Federal Trade Commission Act)**. Esta ley prohíbe actos y prácticas engañosas en los negocios, incluidos los relacionados con la seguridad de datos. La FTC también hace cumplir **la Ley Gramm-Leach-Bliley (GLB),** que, desde 1999, requiere que las empresas protejan los datos de los clientes que recopilan.

2.8. Cooperación internacional

Estados Unidos ha optado por no ampliar su red de acuerdos comerciales, salvo algunos acuerdos sectoriales, entre los que deberíamos citar el de los **minerales críticos firmado con Japón en marzo de 2023,** con el fin de evitar que sus empresas queden excluidas de parte de las ayudas de la iniciativa IRA. Para otros acuerdos significativos hay que retrotraerse a la presidencia Trump, donde caben destacarse la modernización del **Tratado Estados Unidos-México y Canadá de Libre Comercio de América del Norte** (The United

States-Mexico-Canada Agreement o USMCA), de 1 de julio de 2020, y la primera fase de un acuerdo comercial con China, de 15 de enero de 2020, que no llegó a aplicarse.

Considerando lo expuesto, la estrategia de la **Administración Biden se estructura en torno a dos iniciativas** en las que se abordan con los países aliados aspectos de comercio, tecnología y de seguridad económica:

- El **Consejo de Comercio y Tecnología con la Unión Europea** (en sus siglas en inglés TTC). Entre los principales logros en materia de seguridad económica podríamos mencionar una mayor cooperación en nuevas tecnologías y en las cadenas de suministro resilientes, por ejemplo, en semiconductores, mediante un sistema de alerta temprana, y en minerales críticos, mediante el impulso de un Foro sobre minerales (Mineral Security Partnership) (MSP), entre otros.
- El **Marco Económico del Indo-Pacifico** (en sus siglas en inglés IPEF) con Australia, Brunéi, Corea del Sur, India, indonesia, Malasia, Nueva Zelanda, Singapur, Tailandia y Vietnam. Entre sus iniciativas, podemos mencionar el establecimiento de un mecanismo de alerta temprana ante interrupciones en las cadenas de suministro, un mapeo de suministro de minerales críticos, la mejora de la trazabilidad y mayores esfuerzos en diversificación.

Otras iniciativas más concretas, que merecen atención son:

- **Chips 4 Alliance**. Alianza constituida por EE. UU., Taiwán, Japón y Corea del Sur, con la intención de cooperar en la implementación de políticas que fomenten la fabricación sostenible de semiconductores en los países de origen de los Estados miembros.
- **Acuerdo con Países Bajos y Japón sobre control de exportación de tecnologías relacionadas con los semiconductores** a la R.P. China, tras la decisión adoptada por la Administración estadounidense de limitar las exportaciones de semiconductores de última generación a la R.P. China.
- **La Asociación para el Aseguramiento de Minerales (MSP**, por sus siglas en inglés) de abril de 2024. La UE, los Estados Unidos y otros socios de la Asociación, a los que se han unido Kazajistán, Namibia, Ucrania y Uzbekistán, anunciaron la puesta en marcha del Foro de la Asociación para el Aseguramiento de Minerales («Foro de la MSP»). El foro será una nueva plataforma para la cooperación en el ámbito de las materias primas fundamentales, vitales para las transiciones ecológica y digital

a escala mundial. El Club de Materias Primas Fundamentales anunciado por la Comisión Europea pasa a formar parte integrante del Foro de la MSP. Así se creará una iniciativa conjunta más amplia y ambiciosa, donde la UE está representada por la Comisión Europea. El Foro reunirá a países ricos en recursos y a países con una gran demanda de esos recursos.

3. JAPÓN

3.1. Introducción

El Gobierno de Fumio Kishida -accedió al puesto de primer ministro en octubre de 2021-ha seguido el legado dejado por el primer ministro Shinzo Abbe (2006-2007 y 2012-2020), quien dio un giro a la política exterior de su país y empezó a replantear ciertos aspectos relacionados con la seguridad y defensa en una sociedad muy pacifista, ante la creciente percepción de amenaza procedente de Corea del Norte, China y Rusia. Buenos ejemplos de ello fueron una política más asertiva del país en la región del Indo Pacifico, el liderazgo de Japón para sacar adelante el **acuerdo comercial regional TTP-ahora CPTTP-,** tras el anuncio de la retirada de Estados Unidos de este acuerdo, o el impuso de la iniciativa **Quality Investment Infrastructure Initiative** con ayuda de la OCDE y del Banco Asiático de Desarrollo, en respuesta a las iniciativas chinas de la Franja y la Ruta de la Seda y el Banco Asiático de Inversión e Infraestructuras. En el ámbito de seguridad, debemos mencionar el **Diálogo de Seguridad Cuadrilateral (QUAD),** impulsado primero en 2007 por Shinzo Abbe, junto a Estados Unidos, Australia e India, y reactivado después con ocasión de la Cumbre de la ASEAN, celebrada en Manila, con un fuerte enfoque en temas de defensa, seguridad, cadenas de suministro y cooperación tecnológica, entre otros aspectos.

El Gobierno de Fumio Kishida profundiza el camino trazado por Shinzo Abbe mediante un creciente abandono de la ambigüedad estratégica en la región y un **creciente alineamiento con Estados Unidos** en todos los ámbitos, incluyendo los de seguridad y defensa. Este reposicionamiento de Japón en el mundo y en la región del Indo-Pacífico se ponen de manifiesto en la **Estrategia Nacional de Seguridad** y el **Programa de Adquisiciones de Defensa**, presentados conjuntamente en diciembre de 2022, con un **fuerte énfasis en la seguridad económica.**

Todo ello a su vez ha dejado el camino expedito a un aumento del gasto miliar hasta un 2% del PIB hasta 2027 y a una posible adhesión de Japón a la iniciativa AUKUS, cuyo principal objetivo consiste en que Estados Unidos y el Reino compartan su tecnología de propulsión nuclear submarina con Australia. Una decisión de este calibre supondría un paso decisivo hacia un alineamiento definitivo con Estados Unidos y el resto de sus aliados. Japón es invitado desde hace varios años a las reuniones de la OTAN.

3.2. La nueva estrategia de seguridad económica

3.2.1. Estructura institucional

Varios cambios institucionales han elevado la seguridad económica dentro del gobierno japonés. La Secretaría de Seguridad Nacional lanzó en 2020 una **nueva división centrada en temas de seguridad económica**. En febrero de 2021, la Agencia de Inteligencia de Seguridad Pública de Japón (PSIA) también creó una nueva unidad para tratar las transferencias no deseados de tecnología. En este marco, el primer ministro Kishida subrayó la importancia que otorga al tema al constituir el 4 de octubre de 2021 una **Oficina de Seguridad Económica** en el gabinete del primer ministro y establecer un grupo asesor, el Consejo de Expertos en Legislación de Seguridad Económica, en julio de 2022.

Entre los primeros objetivos de esta nueva Oficina figuró la elaboración de la **Ley de Protección de la Seguridad Económica (ESPA), que fue aprobada el 11 de mayo de 2022** (Ley N.º 43 de 2022). Asimismo, la oficina tiene como principal misión coordinar los distintos ministerios y agencias concernidos por esta nueva legislación, incluyendo el Ministerio de Economía, Comercio e Industria, el Ministerio del Interior y el Ministerio de Comunicación.

La ESPA se estructura en torno a cuatro ejes:

- Garantizar el suministro estable de **materiales** críticos.
- Proteger las **infraestructuras** críticas.
- Apoyar el desarrollo de **tecnologías** críticas.
- Crear un sistema de **patentes** secretas.

El desarrollo de estas cuatro líneas fue encomendado al Consejo de Expertos en Legislación de Seguridad Económica, constituido en julio de 2022. Éste es dependiente de la ya mencionada división económica en la Secretaría de Seguridad Nacional y está formado, entre otros, por representantes de organizaciones empresariales, empresas, *think tanks* y universidades.

3.2.2. Cadenas de suministro

Se han fijado **cuatro condiciones** con el objeto de **calificar si un producto merece apoyo gubernamental**: debe ser esencial para la supervivencia de las personas, debe existir una excesiva dependencia del exterior, el suministro puede podría estar sujeto a interrupciones y se necesita asegurar un suministro estable.

Con arreglo a estos criterios, se han identificado **once productos esenciales**: semiconductores, tierras raras, suministros médicos, fertilizantes, piezas de barcos, gas natural licuado, piezas de aviones, aplicaciones en la nube, antimicrobianos, baterías de almacenamiento, robots industriales y máquinas herramienta.

Al mismo tiempo, cabe mencionar la creación en 2004 de **Japan Organization for Metals and Energy Security (JOGMEC).** Este organismo, que integra las funciones de Japan National Oil Corporation y de la Agencia de Minería de Metales, tiene entre sus principales objetivos asegurar el suministro de petróleo, gas y de materias primas. En **agosto de 2022** entró en vigor una **reforma de la legislación de JOGMEC**, que permite a este organismo conceder subvenciones para desarrollar proyectos que aseguren un suministro estable de petróleo, gas y de materias primas. Así pues, Japan Organization for Metals and Energy Security (JOGMEC) y Sojitz Corporation firmaron un acuerdo para invertir en una mina de tierras raras en Australia para suministrar el i65% de su producción del disprosio y el terbio a Japón.

3.2.3. Infraestructuras críticas

El 12 de junio de 2023, el gobierno presentó al Consejo de Expertos los criterios para realizar evaluaciones antes de que se desarrollen nuevas instalaciones en sectores bien definidos, con el fin de proteger la infraestructura crítica contra ciberataques y otras amenazas.

Los sectores concernidos son: distribución eléctrica; gasoductos; ferrocarriles y transporte de carga; transporte aéreo y aeropuertos; telecomunicaciones; radiodifusión terrestre; servicio postal; banca, transferencia de fondos.

3.2.4. Promoción de tecnologías críticas

En este ámbito hay que destacar dos iniciativas:

- En octubre de 2022, el gobierno identificó las siguientes **20 tecnologías críticas**: biotecnología; tecnología médica y de salud pública; inteligencia artificial y aprendizaje automático; informática avanzada; tecnología de microprocesadores y semiconductores; ciencia de datos, análisis, almacenamiento y gestión; tecnología de ingeniería y fabricación avanzada; robótica; ciencia de la información cuántica; tecnología de vigilancia, posicionamiento y detección avanzada; neuro computación y tecnología de interfaz cerebral; tecnología de energía avanzada y almacenamiento de energía; tecnología de información, comunicación y redes avanzada; ciberseguridad; tecnología espacial,

tecnología marina; tecnología de transporte; hipersónicos; tecnología química, biológica, radiológica y nuclear; y ciencia de materiales avanzada.

- En junio de 2023, el gobierno también anunció apoyo financiero y participación de capital público en empresas con tecnología avanzada.

3.2.5. Patentes secretas / No divulgación de patentes por razones de seguridad

El 12 de junio de 2023, el gobierno presentó al Consejo de Expertos el **sistema de no Divulgación para Solicitudes de Patente**, en el que proponen **25 ámbitos tecnológicos** que podrían utilizarse con fines militares y en los que, por lo tanto, las patentes deberían mantenerse en secreto. Estos incluyen ciertas tecnologías relacionados con submarinos y aeronaves no tripuladas, explosivos, etc.

3.2.6. Control de inversiones entrantes

La ley troncal que regula las inversiones extranjeras en Japón es la **Ley de Intercambio y Comercio Extranjero (FEFTA**, por sus siglas en inglés), es complementada mediante ciertos regímenes normativos específicos, como la aeronáutica, la radiodifusión, la aeronáutica, los fletes, la minería, las telecomunicaciones. Varios ministerios tienen jurisdicción en este ámbito, debiéndose presentar los informes y notificaciones a los ministerios a través del Banco de Japón.

Entre las recientes modificaciones normativas, deberíamos destacar las siguientes:

- El 5 de octubre de 2021, el Gobierno agregó a los sectores económicos principales **dos nuevas categorías dentro del sector minero** (incluida la minería en aguas profundas):
    - **Sectores empresariales relacionados con 34 minerales críticos**, incluidos los elementos de tierras raras:
        - Minería de metales de los minerales designados.
        - Fabricación, reparación, mantenimiento o software para dispositivos o productos utilizados para la minería de metales de minerales designados,
        - Servicios de análisis de componentes respecto a minerales designados.

- **Empresas de construcción que mejoran o mantienen las instalaciones portuarias en islas identificadas como importantes para las operaciones mineras de recursos minerales**, como Okino-Tori-Shima y Minami-Tori-Shima. Además, la exploración o medición para, o el diseño de, dicha construcción también está cubierta.

Ambas enmiendas parecen estar dirigidas no solo a proteger los recursos minerales estratégicos dentro del territorio japonés, sino también a mantener y asegurar las capacidades asociadas a la exploración y el resto de las actividades mineras en tierra como en aguas profundas y las actividades mineras. Esta enmienda se **aplica a las inversiones extranjeras directas desde el 4 de noviembre de 2021.**

Entre otras novedades, debemos destacar la promulgación de la **Ley de Revisión y Regulación del Uso de Bienes Raíces en junio de 2021,** que regula la transferencia y uso de propiedades inmobiliarias cercanas o dentro de ciertas instalaciones y lugares que son importantes desde una perspectiva de seguridad nacional.

Por último, la **Ley de Intercambio de Divisas y Comercio Exterior** fue revisada en **octubre de 2019** para permitir al gobierno japonés verificar las inversiones o compras de empresas japonesas por parte de empresas estatales chinas

3.2.7. Control de exportaciones

La **Ley de Intercambio y Comercio Extranjero (FEFTA,** por sus siglas en inglés) regula el control de exportaciones de bienes de doble uso. Una de las últimas modificaciones fue en julio de 2023, cuando se decidió reforzar el control en 32 productos específicos, incluyendo **semiconductores de última generación y sus equipos de fabricación**, como parte de los esfuerzos de alineación con Estados Unidos y los Países Bajos para restringir la exportación de semiconductores avanzados, máquinas litográficas y servicios asociados a China. Además, Japón forma parte de los **regímenes multilaterales de control de exportaciones**, junto con otros países entre los que destacan EE.UU., India, Australia, Corea del Sur y Canadá como son el Acuerdo Wassenaar (WA), el Grupo de Suministradores Nucleares (NSG), el Grupo de Australia (AG) y el Régimen de control de tecnología de misiles (MTCR).

3.3. Ciberseguridad

Japón tiene una ley específica de ciberseguridad llamada **Ley Básica de Ciberseguridad,** que fue promulgada el 6 de noviembre de 2014 (y promulgada el 12 de noviembre de 2014). Fue la primera ley específica de ciberseguridad promulgada entre las naciones del G7.

Debido al aumento de las amenazas a la ciberseguridad, se modificó el 5 de diciembre de 2018 (y entró en vigor el 1 de abril de 2019), con miras a garantizar aún más la ciberseguridad en Japón y preparar a Japón para los Juegos Olímpicos y Paralímpicos de Tokio 2020.

En la actualidad, Japón tiene otras leyes sustantivas que cubren cuestiones de delitos cibernéticos, como el **Código Penal, la Ley de Prohibición de Acceso No Autorizado a Computadoras, la Ley de Prevención de la Competencia Desleal, la Ley de Derecho de Autor, la Ley de Protección de Secretos Especialmente Designados, la Ley Básica sobre la Formación de una Sociedad de Redes Avanzadas de Información y Telecomunicaciones, y la Ley de Empresas de Certificación y Firma Electrónica**. Además de la legislación sobre delitos cibernéticos, en 2003 se promulgó la **Ley de Protección de Información Personal** para proteger la información y la identidad personales.

3.4. Cooperación internacional

Japón cuanta con una **amplia red de acuerdos comerciales**. Gran parte de los acuerdos comerciales RCEP y CPTTP, tiene un acuerdo comercial con la Asociación de Países del Sueste Asiático (ANSA) y con la Unión Europea, entre otros. Sin embargo, no tiene un acuerdo comercial en vigor con Estados Unidos, país con el que ha tenido que negociar un acuerdo de minerales críticos con el fin de que las empresas japonesas no quedasen del todo excluidas de la iniciativa IRA. Asimismo, forma parte, junto a Estados Unidos y otros 11 países de la región, del **Marco Económico del Indo-Pacífico (IPEF).** Con Estados Unidos estableció en noviembre de 2023 el **Consejo Consultivo de Política Económica** (Economic Policy Consultative Committee, EPCC), también conocido como 2+2, que tiene por objeto un diálogo estructurado sobre diálogo, economía y seguridad.

La **cooperación entre la Unión Europea y Japón** se ha fortalecido significativamente, en áreas como las inversiones entrantes o la conectividad digital y verde, debido a la convergencia de los enfoques de seguridad económica de ambos bloques.

Debido a ello, ambas partes han anunciado medidas para mejorar el escrutinio de **inversiones entrantes y los controles de exportación**, así como **esfuerzos conjuntos contra la coerción económica** extranjera. Además, en la primera reunión del **Consejo de Asociación Digital UE-Japón**, celebrado en julio de 2023 en Tokio, se firmó un memorando de cooperación sobre cables submarinos para garantizar una conectividad global segura, resiliente y sostenible. En octubre de ese año, se firmó un acuerdo sobre los flujos transfronterizos de datos digitales.

Finalmente, Japón se ha unido recientemente a nuevas asociaciones para diversificar sus cadenas de suministro, como en abril de 2021 a la **Iniciativa de Resiliencia de la Cadena de Suministro (SCRI), un grupo trilateral con Australia e India**, que tiene como objetivo compartir mejores prácticas en resiliencia de la cadena de suministro y fomentar la diversificación de las cadenas de suministro a través de inversiones.

4. REPÚBLICA DE COREA (COREA DEL SUR)

4.1. Introducción

Desde que Moon Jae-in a Yoon Suk Yeol accediese el cargo de primer ministro de Corea del Sur en mayo de 2022, su gobierno ha emprendido un firme **desarrollo de su estrategia de seguridad económica en el marco de una redefinición más amplia de su seguridad nacional**, poniendo énfasis en la promoción de las industrias estratégicas, mediante ventajas fiscales, en la resiliencia de las cadenas de suministro y en la prevención de fugas de conocimientos tecnológicos y de talento. Se trata de una decisión de gran trascendencia para un país, cuya economía presenta un **elevado grado de internacionalización** y una fuerte **vinculación con China**. Este nueva estrategia de seguridad económica es, en parte, resultado de las lecciones sacadas a raíz de las amenazas de retorsión económica por parte de China con motivo del anuncio para el despliegue en Corea del Sur del sistema antimisiles estadounidense THAAD (Terminal High Altitude Area Defense) en 2017 y las vulnerabilidades externas identificadas durante la pandemia de la Covid-19; pero también del impacto que han tenidas iniciativas estadounidenses, como IRA y las restricciones a la exportación de semiconductores avanzados y sus equipos de fabricación, en las industrias de automoción y de semiconductores coreanas.

Sin embargo, este cambio no se entendería del todo si no se relacionase, a su vez, con el nuevo rumbo dado a la política exterior, en la que la ambigüedad estratégica cede el paso a una **mayor alineación con Estos Unidos y Japón,** en los ámbitos económico y tecnológico, y a una **implicación** decidida del país **en la región del Indo Pacífico**, sin por ello perder de vista la fuerte interdependencia económica con la R.P. China. Todo ello se pone de manifiesto con:

- La visita del presidente surcoreano a Japón en marzo de 2023 y la **Cumbre de Camp David entre Estados Unidos, Corea del Sur y Japón en agosto de 2023**, cuya declaración conjunta menciona, entre otros aspectos, la cooperación en tecnología, incluidas las cadenas de suministro de semiconductores y baterías.
- La publicación por el Gobierno surcoreano de dos documentos, que definen este nuevo paradigma:
    - **National Security Strategy. Global Pivotal State for Freedom, Peace and Stability, de junio de 2023**, entre cuyos ejes figura la seguridad

económica, a su vez inspirada en torno a los siguientes principios: un sistema de respuesta integrado y multinivel, estructurado en torno a la colaboración público-privada, la conformación de reglas internacionales con otros países y un desempeño activo en las agendas de las organizaciones internacionales.

- **Strategy for a free, peaceful and prosperous Indo Pacific Region**, de diciembre de 2022, entre cuyos objetivos figuran el establecimiento de redes de seguridad económica y la cooperación científica y tecnología en dominios estratégicos.

4.2. Marco institucional

Como resultado de este cambio rumbo en la política exterior y en la estrategia de seguridad nacional, se producen varios cambios importantes:

- El viceprimer ministro se responsabiliza de coordinar el Ministerio de Comercio y Energía (MOTIE) el Ministerio de Tierras, Infraestructura y Transporte (MOLIT), el Ministerio de PYMES y Empresas Emergentes, el Ministerio de Ciencia y TIC (MSIT), el Ministerio de Educación (MOE), el Ministerio de Agricultura, Alimentación y Asuntos Rurales (MAFRA), el Ministerio de Medio Ambiente (MOE), la Comisión de Servicios Financieros (FSC) y la Oficina de Coordinación de Políticas del Gobierno están involucrados en la planificación de una política industrial para industrias futuras. Entre estos ministerios, debemos subrayar el Ministerio de Industria, Comercio y Energía, el más próximo a las empresas, como quedó evidenciado a raíz de sus gestiones realizadas con la Administración estadounidense para **mitigar los efectos negativos de las iniciativas estadounidenses** IRA y de semiconductores en las industrias coreanas (por ejemplo, obtención de "waivers" para los fabricantes de semiconductores surcoreanos en la R.P. China), y el Ministerio de Ciencia y TIC (MSIT), responsable de establecer la hoja de ruta concerniente a las tecnologías estratégicas.
- En octubre de 2022 se constituyó también **un Consejo Asesor Nacional de Ciencia y Tecnología (National Science Technology Advisory Board)** presidido por el primer ministro coreano. Este órgano consultivo tiene como principal objetivo asesorar en ciencia y tecnología, incluyendo la dirección política, la revisión de políticas de innovación y ciencia, así como las inversiones en investigación y desarrollo. De él forman parte diecinueve representantes del sector privado y representantes de los ministerios implicados.

- Se ha creado un **grupo de trabajo intergubernamental** (ministerios, agencias y embajadas, entre otros) para implantar un sistema de **alerta temprana en la detección de interrupción en las cadenas de suministro**. Se han establecido **nuevos organismos** como Korea Center for Global Value Chain y el Center for Economic Security and Foreign Affairs (CESFA) para la identificación y prevención de cortes en las cadenas de suministro.
- La responsabilidad de la contrainteligencia y la investigación de casos de espionaje son transferidas al **Servicio de Seguridad Nacional (NIS).** Esta medida busca mejorar la eficiencia y la coordinación entre diferentes agencias de seguridad. Pero, a su vez, asume también **competencias en materia de seguridad económica**. Además, la NIS se centrará en fortalecer la coordinación con otros organismos gubernamentales, como el Ministerio de Defensa Nacional y el Servicio Nacional de Inteligencia, para garantizar una respuesta integrada a las amenazas a la seguridad nacional.
- A finales de junio de 2024 se constituirá un **comité sobre cadenas de suministro**, presidido por el ministro de Finanzas, e integrado por 25 expertos económicos y de seguridad.

4.3. Industrias estratégicas

- En octubre de 2022, Corea dio a conocer su **Plan Estratégico Nacional de Tecnologías (National Strategic Nurture Plan)** en el que se identifican doce tecnologías críticas, con sus respectivas hojas de ruta.
- Bajo la **Ley de Industrias Avanzadas, promulgada el 10 de julio de 2023,** el gobierno **designó 17 tecnologías** diferentes, en las áreas de semiconductores, pantallas, baterías y biofarmacéuticos como industrias futuras en las que el país se esforzará por fomentar y desarrollar estratégicamente la estabilidad de las cadenas de suministro y la seguridad nacional y económica. Entre las tecnologías identificadas cabe destacar los semiconductores y pantallas, baterías, movilidad de vanguardia, energía nuclear de próxima generación, biotecnología de alta tecnología, aeroespacial y aeronáutica, ciberseguridad, inteligencia artificial, telecomunicaciones de próxima generación, robótica y fabricación de última generación, y tecnología cuántica. La Ley de Industrias Avanzadas especifica, a su vez, ocho tecnologías específicas relacionadas con semiconductores, así como cuatro tecnologías en pantallas, tres tecnologías en baterías y dos

tecnologías en biofarmacéuticos. Asimismo, se seguirá poniendo un fuerte énfasis político en las baterías y la movilidad futura (es decir, vehículos autónomos y K-UAM, o movilidad aérea urbana: taxis voladores).

4.4. Promoción de la industria de semiconductores

- **Aprobada el** 30 de marzo de 2023, la "Ley K-Chips" o Ley sobre Restricción en Casos Especiales Concernientes a la Tributación **establece ventajas fiscales para dar un nuevo impulso al desarrollo de la industria nacional de semiconductores.**

4.5. Prevención de fuga de conocimientos y de talento

- Desde su entrada en vigor **en 2007, el Decreto de Aplicación de la Ley de Prevención de Divulgación y Protección de la Tecnología Industrial o ITA** tiene como objetivo proteger las industrias futuras contra transferencias de tecnología no deseadas o la pérdida de talento. Bajo la ITA, se cubren **75 tecnologías en industrias futuras** -automóviles, ferrocarriles, acero, construcción naval, energía nuclear, telecomunicaciones, espacio, maquinaria, robótica e hidrógeno-. A diferencia de la **Ley de Industrias Avanzadas**, que tiene por objeto garantizar el funcionamiento de ciertas cadenas de suministro, ITA persigue objetivos más generales asociados a la seguridad nacional y el bienestar económico de los surcoreanos. La legislación ha sido emendada varias veces. Las últimas fueron en 2022, y 2023 para permitir ampliar el ámbito de tecnologías cubiertas y reforzar los procedimientos de control y autorización para la exportación de tecnologías críticas. Otras enmiendas están siendo tramitadas en el Parlamento surcoreano.

4.6. Promoción de cadenas de suministro resilientes

- El Ministerio de Comercio, Industria y Energía publicó en diciembre de 2023 **la Estrategia 3050** (Supply Chains Act), que identifica 185 componentes, cuyos suministros merecen ser estabilizadas como parte de la iniciativa destinada a reducir las dependencias del exterior por debajo del 50% hasta 2030. Los 185 componentes son claves para las industrias de alta tecnología (semiconductores, baterías, displays, así como productos eléctricos y electrónicos), las mayores y nuevas industrias (automoción, construcción naval, máquinas herramienta, robots y aeronáutica) e industrias de materiales (metales, fibras, cerámicas y química).

- En febrero de 2023, MOTIE publicó una actualización de **33 minerales elegibles** para recibir apoyo público, entre los que se **priorizan 10,** incluyendo **5 elementos de tierras raras**: litio, níquel, cobalto, manganeso y grafito, así como lantano, cerio, neodimio, terbio, disprosio, entre las tierras raras.

  Como parte de sus esfuerzos destinados a diversificar las cadenas de suministro, Corea creó en **agosto de 2021 Korea Mine Rehabilitation and Mineral Resources Corporation (Komir).** Esta agencia pública apoya proyectos mineros en el exterior. En febrero de 2023, el Gobierno decidió reforzar la capacidad de Komir y de otras agencias para conceder créditos, garantías y seguros a empresas coreanas, que inviertan en minas o en el procesado de minerales, o facilitar contratos de suministro a largo plazo. Así, en octubre de 2023 la agencia concedió 3 millones de USD para la financiación de un proyecto de exploración de litio en Australia para una empresa tecnológica coreana.

- En diciembre de 2023, se promulgó **the Framework Act on Supply Chain Stabilization Support for Economic Security (Framework Act on Supply Chain"),** que entrará en vigor en junio de 2024. Esta nueva legislación prevé la creación de un **Comité de cadenas de suministro y un Fondo de estabilización de cadenas de suministro**. Mediante la constitución del comité se quiere dar mejor seguimiento a las estrategias y políticas intergubernamentales, como el **Plan básico de estabilización de cadenas de suministros**, que tiene una vigencia de tres años. Mediante el fondo se pretende impulsar la diversificación de las cadenas de suministro, mediante el desarrollo de tecnologías y el desarrollo de proyectos en el exterior.

4.7. Control de inversiones entrantes

En **agosto de 2022** entró en vigor la legislación **Regulation on Operation of Security Review Procedures for Foreign Investments**. La nueva legislación no altera el sistema vigente; sin embargo, todo inversor extranjero tendrá que declarar en su petición si la transacción propuesta atañe a la seguridad nacional y si la transacción incurre en uno de los siguientes supuestos: impedimento de la producción de material y equipos defensa, productos que están sometidos al control de exportaciones o que vayan a ser destinados a propósitos de naturaleza militar, peligro de revelación de secretos de Estado, riesgo de divulgación de tecnologías criticas o riesgo en los esfuerzos de

Naciones Unidas y de otras organizaciones de preservar la paz. El Ministerio de Industria, Comercio y Energía podrá remitir la propuesta a un Comité de Expertos para que analice la propuesta y adopte una decisión.

4.8. Ciberseguridad

Las principales leyes y regulaciones relacionadas con la protección de datos y la ciberseguridad son la **Ley de Protección de Información Personal** de 2011 (modificada en 2020) ('PIPA') y sus regulaciones de implementación, que regulan la recopilación, el uso, la divulgación y otro procesamiento de datos personales por parte del gobierno. y entidades privadas.

El propósito de esta Ley es crear infraestructura para la industria de seguridad de la información proporcionando los recursos necesarios para promover la industria de seguridad de la información; y contribuir a crear un entorno en el que las personas puedan utilizar la información y las comunicaciones de forma segura, y a desarrollar sólidamente la economía nacional mediante el fortalecimiento de la competitividad de la industria de la seguridad de la información.

4.9. Cooperación internacional

Corea cuenta con una **red de acuerdos comerciales**. Es de los pocos países del mundo que tiene acuerdos comerciales con las tres grandes economías del mundo: **Estados Unidos, China y la Unión Europea, así como ASEAN**. Forma parte del acuerdo comercial **RCEP** y ha solicitado su adhesión al acuerdo comercial **CPTTP**, del que también forma parte Japón. Asimismo, forma parte de la **Chips 4 Alliance**, junto a Estados Unidos, Japón y Países Bajos y de la iniciativa **Indo-Pacific Economic Forum** (IPEF), liderada por Estados Unidos. Asimismo, ha firmado **alianzas estratégicas** con países, como **Australia, Canadá, Ecuador, Mongolia, Estados Unidos y Kazajstán**. Asimismo, se ha adherido en 2022 a la iniciativa estadounidense **Minerals Security Partnership (MSP),** mencionada anteriormente, que tiene por objeto garantizar inversiones públicas y privadas en las cadenas de suministro estratégicas. A su vez, mantiene un **diálogo de alto nivel con Estados Unidos en tecnologías emergentes** (Next Generation Critical and Emerging Technologies Dialogue).

Por último, cabe mencionar que Corea, junto con otros países entre los que destacan EE. UU., India, Australia, Japón y Canadá, forma parte de los siguientes acuerdos internacionales referentes al control de exportaciones:

- Acuerdo de Wassenaar sobre controles de exportación de armas. convencionales y bienes y tecnologías de doble uso.
- Grupo de Australia.
- Grupo de Suministradores Nucleares.
- Régimen de control de tecnología de misiles.

5. REINO UNIDO

5.1. Introducción

El enfoque de la estrategia de seguridad económica del Reino Unido consiste en una combinación de legislación, estrategias y adaptación organizativa, incluida la creación de organismos dedicados a temas específicos, como es el caso de Centro Nacional de Seguridad Cibernética en el Reino Unido (NCSC).

Sin contar con una estrategia global como la japonesa o surcoreana, la seguridad económica adquiere especial relevancia desde la publicación en marzo de 2023 de la **Revisión Integrada del Gobierno (IRR23),** un documento orientativo que analiza los retos que afronta el Reino Unido en un nuevo contexto internacional de rivalidad estratégica, y en el que se expresa la necesidad de adoptar medidas más sólidas para fortalecer la seguridad económica del Reino Unido.

5.2. Marco institucional

Prueba de la importancia concedida a la seguridad económico, el Reino Unidos es junto con Japón, el único país del G7 con un cargo ministerial dedicado a este tema. El Ministerio de Economía y de Seguridad Económica coordina la estrategia de seguridad económica del país y entiende del escrutinio de inversiones y del control de las exportaciones., en este último caso a través de la Unidad Conjunta de Control de Exportaciones (ECJU).

Además, en el marco de su nueva estrategia de seguridad económica, se prevé la creación de un foro público-privado de seguridad económica con el fin de abordar junto a las empresas, las políticas y medidas de seguridad económica.

5.3. Desarrollo de la estrategia de seguridad económica

En el marco de la IRR23, hay reuniones de expertos públicos y privados, en un esfuerzo por ayudar a crear condiciones regulatorias, económicas y de mercado coherentes propicias para el suministro seguro y sostenible de materiales críticos. En el pilar de **"resiliencia" de la IRR23**, el Gobierno está trabajando en los ámbitos de los minerales críticos, las cadenas de suministro, los controles de exportación, disuasión y los delitos económicos, junto con la priorización de "ventaja estratégica" en ciencia y tecnología. Como resultado de los trabajos realizados, se han identificado como críticos los siguientes sectores de actividad económica: manufactura avanzada,

sector automotriz, aeroespacial, sostenibilidad e infraestructura, materiales y minerales críticos, construcción naval, servicios profesionales y empresariales y cadenas de suministro globales.

5.4. Cadenas de suministro

Entre las medidas concretas, debemos destacar la estrategia de Reino Unido para impulsar el sector de semiconductores conocida como **National Semiconductor Strategy,** que fue presentada por la Secretaría de Estado de Ciencia, Innovación y Tecnología en mayo de 2023. Ésta tiene un triple objetivo: apoyar la industria de semiconductores nacional, mitigar el riesgo de las disrupciones de la cadena de suministro de este sector, y proteger los intereses de la seguridad nacional británica. Para lograr este objetivo, se estableció un **Panel Asesor de Semiconductores** (UK Semiconductor Advisory Panel) en el que participan representantes de la industria, el gobierno y la academia. Se prevén, entre otras medidas, invertir hasta £200 millones entre 2023-2025, así como alcanzar los £1 mil millones en la próxima década. Asimismo, se están explorando opciones para respaldar la investigación y el desarrollo comercial del sector.

5.5. Escrutinio de inversiones

En enero de 2022, entró en vigor la **Ley de Seguridad Nacional e Inversiones**, que otorga al gobierno poderes para examinar las inversiones y tomar medidas para proteger los activos vitales para la seguridad nacional del Reino Unido en algunos sectores económicos. Posteriormente, y para dotar de mayor poder a esta ley, se publicó, en marzo de 2023, la ya mencionada **Revisión Integrada del Gobierno (IRR23),** que estableció el enfoque para abordar las amenazas a la seguridad económica, más allá del ámbito de las inversiones entrantes.

Por otro lado, el secretario de Estado del Departamento de Cultura, Medios de Comunicación y Deporte en ese momento, Oliver Dowden, desempeñó un papel destacado en la decisión del gobierno de **prohibir a Huawei en las redes 5G del Reino Unido** e introdujo la **Ley de Seguridad de las Telecomunicaciones.**

En relación las inversiones salientes, el **Departamento de Negocios y Comercio o DBT (Department for Business and Trade**) lidera la evaluación, junto con otros departamentos relevantes y en colaboración con el sector privado, de los posibles riesgos para la seguridad nacional que plantea la inversión directa extranjera. Esta iniciativa responde a la **declaración conjunta entre el Reino Unido y Estados Unidos el 8 de junio de 2023**, en la que se

manifestó el objetivo compartido de ambos países para evitar la fuga indeseada de capital y el *know-how* de las empresas nacionales al exterior, que pudieran contribuir al desarrollo de las capacidades militares y de inteligencia de países hostiles o considerados como preocupantes.

5.6. Ciberseguridad

Aunque no existe una ley nacional de ciberseguridad primaria y general en el Reino Unido, hay **cuatro esquemas legislativos críticos** que rigen la ciberseguridad, la privacidad de datos y la protección de datos: DPA (Data Protection Act 2018), UK-GDPR (UK General Data Protection Regulation), NIS Regulations (Network and Information Security Regulations 2018) y la Computer Misuse Act de 1990. Asimismo, también destacan **tres legislaciones complementarias de importancia:** Ley de Telecomunicaciones (Seguridad) de 2021, la UK eIDAS (Reglamentos de Identificación Electrónica y Servicios de Confianza para Transacciones Electrónicas de 2016) y la PECR (Reglamentos de Privacidad y Comunicaciones Electrónicas).

5.7. Cooperación internacional

Como parte del desarrollo de la Revisión Integrada del Gobierno (IRR23), el gobierno británico ha reforzado su colaboración con Estados Unidos y Japón estableciendo acuerdos internacionales con Estados Unidos y Japón, después de la Declaración del Atlántico, que fue una declaración conjunta entre el Reino Unido y Estados Unidos el 8 de junio de 2023.

6. OTROS PAÍSES

En este apartado hemos incluido una serie de países que aún no disponen de un marco institucional seguridad económica centralizado o de una estrategia económica cohesionada y desarrollada en sus vertientes de protección, promoción y de alianzas.

6.1. Australia

Mantiene una fuerte interdependencia económica con la R.P. China y ha sido objeto de medidas de retorsión económica, al igual que Corea del Sur y Japón. El anuncio de la **iniciativa AUKUS** el 15 de septiembre de 2021, por la que Estados Unidos y el Reino Unido se comprometen a ayudar a Australia a desarrollar una flota de submarinos nucleares, como parte del esfuerzo del Gobierno australiano de potenciar su armada, refuerza el proceso de alineamiento gradual de Australia con Estados Unidos en seguridad y defensa. Australia también es invitada junto a Corea del Sur y Japón a las reuniones de la OTAN, y también, junto a Corea del Sur, a las reuniones del G7. Australia ha intensificado en los últimos años maniobras militares con Estados, Japón, India y Filipinas, entre otros.

El país cuenta con una oficina de seguridad nacional y una estrategia de defensa nacional. En el ámbito económico cuenta con una **estrategia económica para el sudeste asiático,** que fue dada a conocer en noviembre de 2021.

El país está implicado en **varias iniciativas internacionales** en las que se abordan aspectos de seguridad económica, como el **Marco Económico del Indo-Pacífico (IPEF) y el Diálogo de seguridad Cuadrilateral (QUAD).** Asimismo, hay que destacar la **Iniciativa de Resiliencia de la Cadena de Suministro (SCRI),** junto a India y Japón, dos países con los que trabaja también en las iniciativas IPEF y QUAD. Asimismo, Australia está colaborando en este ámbito con el Reino Unido. **El AUKUS** con Estados Unidos y el Reino Unido para al desarrollo de submarinos de propulsión nuclear para la Armada australiana, también tiene, además del militar, implicaciones económicas y tecnológicas para el país.

El Gobierno también ha creado una **Oficina de Resiliencia de la Cadena de Suministro (Office of Supply Chain Resilience),** que depende del Ministerio de Industria, Ciencia y Recursos. Su objetivo consiste en identificar las vulnerabilidades críticas en la cadena de suministro, con el objetivo de garantizar la salud, seguridad, bienestar, estabilidad económica, y seguridad

nacional tanto de Australia como de sus socios internacionales. La Oficina colabora con las empresas para comprender los riesgos específicos de la cadena de suministro de Australia, y proporcionar alertas tempranas sobre posibles interrupciones en las cadenas de suministro críticas.

En tecnologías críticas, el Gobierno australiano publicó el 19 de mayo de 2023 (revisada el 23 de mayo) una **Declaración sobre tecnologías críticas**, que puedan influir en la seguridad nacional y en la prosperidad económica del país. En ella se fija una lista de tecnologías críticas en los siguientes sectores: fabricación avanzada y nuevos materiales, tecnologías de inteligencia artificial, tecnologías de la información y de las telecomunicaciones, tecnología cuántica, sistemas autónomos y robótica, tecnologías de posicionamiento y de temporización, sensores, biotecnología, generación de energía limpia y almacenamiento. Cuenta con una plataforma de tecnologías críticas, dependiente del Ministerio del Ministerio de Industria, Ciencia y Recursos, que asesora al Gobierno sobre las oportunidades y riesgos que plantean las tecnologías críticas. Asimismo, se cuenta también con un Grupo de trabajo de tecnología digital, encarga de coordinar toda la política económica digital.

Por otro lado, respecto a **ciberseguridad**, Australia cuenta con un sólido marco legal para la prevención y persecución de una amplia gama de ciberdelitos. Esto incluye un conjunto integral de delitos informáticos y de telecomunicaciones en las Partes 7.3, 10.6 y 10.7 de la **Ley de Código Penal de la Commonwealth de 1995.** El **Centro de Ciberseguridad Australiano (ACSC)** lidera los esfuerzos del Gobierno Australiano en materia de ciberseguridad. Asimismo, cada Estado y territorio en Australia tiene legislaciones complementarias a las de la Commonwealth.

En materia de infraestructuras, debemos hacer mencionar la enmienda en 2021 (SLACI Act) de la legislación de infraestructuras críticas, **Security of Critical Infrastructure Act 2018,** por la que se obliga a los propietarios y operadores de infraestructuras críticas a adoptar medidas para mejorar el grado de protección de las infraestructuras. En febrero de 2023, el gobierno australiano publicó su visión sobre las infraestructuras críticas, **Critical Infrastructure Resilience Strategy**.

Por último, el Gobierno australiano acaba de anunciar el desarrollo de la ley **"Future Made in Australia Act",** que persigue establecer un marco para respaldar el desarrollo de la industria nacional.

6.2. India

El país está implicado en varias iniciativas ya mencionadas, como pueden ser el **Marco Económico del Indo Pacífico (IPEF), el Diálogo de Seguridad Cuadrilateral (QUAD), la Iniciativa de Resiliencia de la Cadena de Suministro (SCRI).** Cuenta con un régimen de control de inversiones con numerosas prohibiciones y restricciones en sectores económicos sensibles y la Alianza por la Competitividad industrial con Japón.

El control de inversiones se ha tornado más exigente desde 2020 para los inversores de los países vecinos en virtud de la seguridad nacional, además de Pakistán y Bangladesh que ya estaban sometidos antes del cambio legislativo a un régimen de control más duro. También se han endurecido en 2020 las condiciones para que una empresa de un país vecino pueda licitar en un concurso público en India, teniendo que registrarse previamente y obtener una autorización por parte del Gobierno para concurrir a la licitación. Por otro lado, India ha reforzado su control de exportaciones. Apoyándose en la **Ley de Tecnologías de la Información** (Information Technology Act), el Gobierno decretó en junio de 2020 la prohibición a la comercialización y uso de 59 aplicaciones de los gigantes tecnológicos, habiendo aumentado mientras tanto hasta 321. Asimismo, se ha impuesto la prohibición de facto a la importación de equipos de generación eléctrica por razones de ciberseguridad. También se muestra recitente a permitir que las empresas de telecomunicaciones chinas participen en el desarrollo de la red 5G. India en 2020 revisó en 2020 su **Política Nacional de Ciberseguridad**. En el plano de la promoción industrial, hay que mencionar el **Plan Make in India**, ha anunciado en 2014, y actualizado en mayo de 2020 - Self-Reliant India Scheme-, que tiene por objeto impulsar el desarrollo industrial en India.

6.3. Singapur

El 9 de enero de 2024, el gobierno de Singapur aprobó el **Proyecto de Ley de Revisión de Inversiones Significativas**, con el fin de reforzar el escrutinio de inversiones en entidades críticas que puedan suponer un riesgo para la seguridad nacional. Esta legislación concede amplios poderes discrecionales al ministro de Comercio e Industria. Además, se establecerá una **Oficina de Revisión de Inversiones Significativas**.

Aunque la ley no define explícitamente el alcance de la seguridad nacional, se entiende que abarca aspectos como la soberanía y la seguridad económica. Es importante destacar que esta legislación **no reemplaza las**

leyes sectoriales existentes, sino que las complementa, centrándose específicamente en los intereses de seguridad nacional de Singapur.

6.4. Canadá

El país cuenta con varias estrategias. La **Estrategia Canadiense de Minerales Críticos, la Estrategia Nacional para Infraestructuras Críticas, la Estrategia en el Indo-Pacífico de Canadá y las Directrices de Seguridad Nacional para Asociaciones de Investigación**. En materia de control de inversiones entrantes, el **Proyecto de Ley C-34** representa una oportunidad significativa para modernizar la Ley de Inversiones de Canadá y fortalecer su capacidad para gestionar las amenazas asociadas con las inversiones extranjeras.

En lo referente a la **ciberseguridad**, el marco legal está regido por varias leyes que incluyen privacidad, antispam, responsabilidad penal y propiedad intelectual. A nivel federal, la más importante es **Personal Information Protection and Electronic Documents Act (PIPEDA)** del año 2005. En junio de 2022, se presentó el Proyecto de Ley C-27, para incorporar una nueva **Consumer Privacy Protection Act**, una nueva **Personal Information and Data Protection Tribunal Act** (crearía un tribunal administrativo para escuchar apelaciones de órdenes emitidas por el Comisionado Federal de Privacidad y aplicaría un nuevo régimen de sanciones pecuniarias administrativas creado bajo la Ley de Protección de la Privacidad del Consumidor) y una nueva **Artificial Intelligence and Data Act (AIDA).**