ICEX España Exportación e Inversiones

FS FICHA SECTOR

AUSTRALIA

Ciberseguridad en Australia

A. CIFRAS CLAVE

El mercado de la ciberseguridad en Australia ha experimentado un crecimiento notable en los últimos años, alcanzando ingresos de 1.900 millones de dólares australianos en 2023, lo que representa un incremento del 9,5 % respecto al año anterior. Esta industria, que abarca 1.328 empresas, ha registrado un crecimiento en la demanda debido al aumento de las ciberamenazas, con un total de 87.400 ciberataques registrados en 2023. Este contexto ha impulsado la adopción de tecnologías de protección avanzada, incluyendo antivirus, redes privadas virtuales (VPN), y servicios de autenticación y cifrado de datos, que son los productos más destacados del sector. La expansión del teletrabajo, el aumento de la adopción de la tecnología 5G y la creciente concienciación sobre los riesgos cibernéticos representan importantes oportunidades para las empresas de ciberseguridad. A pesar de los retos, como las estrictas normativas de protección de datos y la alta demanda de personal especializado, el sector sigue en expansión, con una tasa de crecimiento anual compuesta proyectada del 3,7 % hasta 2029.

	2022	2023	Fuente
Población total de Australia (habs.)	26.312.201	26.821.557	Australian Bureau of Statistics
Porcentaje de usuarios con acceso a Internet	95,7 %	96,6 %	Statista
Clasificación de Australia en el Índice Global de Ciberseguridad (GCI)	-	43/194	International Telecommunications Union (UN)
Clasificación de Australia en el Índice de Conectividad (NRI)	14/131	14/134	Network Readiness Index
Número total de ciberataques	94.000	87.400	Australian Cyber Security Centre
Ingresos del mercado	1.700 MAUD	1.900 MAUD	IBIS World 2024
Número de empresas del sector	1.181	1.328	IBIS World 2024

B. CARACTERÍSTICAS DEL MERCADO

B.1. Definición precisa del sector estudiado

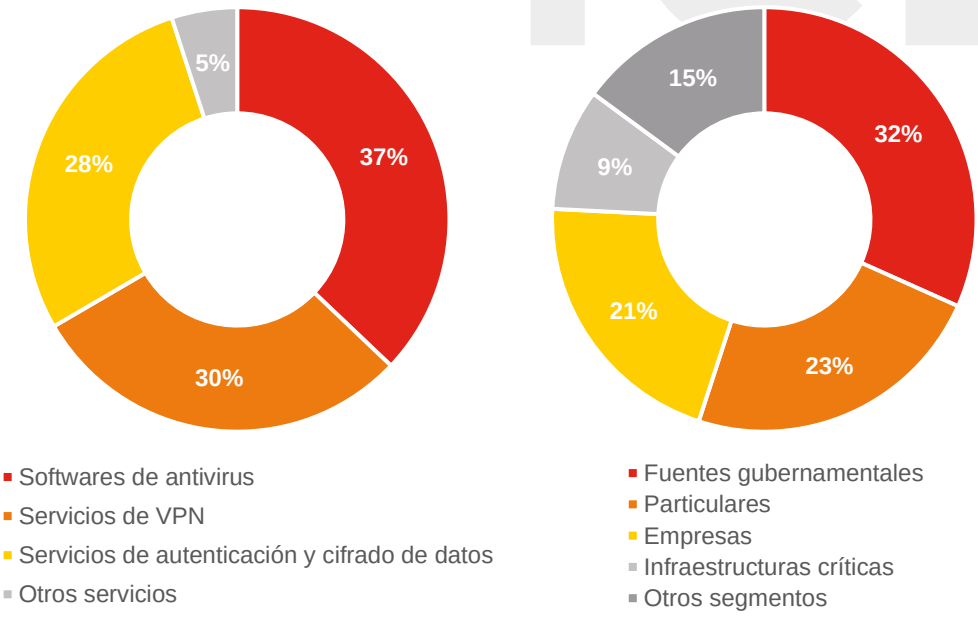
El sector de ciberseguridad en Australia abarca un conjunto de **actividades, tecnologías y servicios diseñados para proteger sistemas, redes y datos frente a ciberamenazas**, al tiempo que garantiza la privacidad y confianza en las interacciones digitales. Este sector es esencial para el funcionamiento de una economía moderna y digitalmente conectada, y su importancia se ha incrementado debido al aumento de los cibercrímenes con el paso de los años. La ciberseguridad en Australia comprende desde la **protección de infraestructuras críticas**, como telecomunicaciones y energía, hasta la **defensa de empresas y datos personales**.

B.2. Tamaño del mercado

De acuerdo con datos de IBIS World 2024, la industria de la ciberseguridad en Australia generó ingresos de **1.900 millones de dólares australianos** en 2023, registrando un **crecimiento del 9,5 %** respecto al año anterior. Este sector está compuesto por **1.396 empresas** que emplean a **6.775 personas**. Además, se proyecta que la industria mantenga un **crecimiento anual compuesto del 3,7 % hasta 2029.**

Los servicios de ciberseguridad en Australia están experimentando una **fase de crecimiento**, superando incluso el ritmo del PIB del país. Este auge se debe, en parte, al incremento del trabajo remoto y a las nuevas ciberamenazas que surgieron tras la pandemia de COVID-19. Además, muchos proveedores de ciberseguridad se especializan en un solo servicio, lo que ha dado lugar a la aparición de nuevas empresas a medida que la tecnología y las comunicaciones se han vuelto más complejas, impulsando aún más el crecimiento del sector.

PRINCIPALES PRODUCTOS Y SEGMENTOS DEL SECTOR
Año 2024



Fuente: *Cybersecurity Software Services in Australia* - IBIS World 2024.

Los principales productos de este sector, según fuentes de IBIS World, 2024 son:

- ***Softwares* de antivirus** – 37,1 %
- **Servicios de redes privadas virtuales (VPN)** – 29,5 %
- **Servicios de autenticación y cifrado de datos** – 28,4 %

Estos productos y servicios destacan por ofrecer soporte posventa de alta calidad, incluyendo actualizaciones regulares y un apoyo continuo que incrementan la satisfacción del cliente. Además, la adopción temprana de nuevas tecnologías permite a las empresas adelantarse a las amenazas emergentes, convirtiendo sus servicios en indispensables y consolidando su éxito comercial.

Por otro lado, los principales segmentos de esta industria son:

- **Fuentes gubernamentales**, con ingresos por encima de los 610 MAUD.
- **Particulares**, que suponen más de 450 MAUD.
- **Empresas privadas**, con un total de 402 MAUD.
- **Infraestructuras críticas** que generan 180 MAUD para la industria.

B.3. Principales actores

En Australia, son varios los organismos gubernamentales que desempeñan un papel clave en la ciberseguridad nacional.

- **Australian Cyber Security Centre (ACSC):** Es la principal agencia de ciberseguridad del país, responsable de liderar la respuesta a amenazas cibernéticas y colaborar con sectores gubernamentales, empresas y ciudadanos para mejorar la seguridad cibernética a nivel nacional.
- **Department of Home Affairs:** Desarrolla políticas de ciberseguridad y lidera la implementación de la *2023-2030 Australian Cyber Security Strategy*, abordando tanto amenazas como oportunidades en el ámbito de tecnologías críticas y emergentes.
- **Critical Infrastructure Centre:** También bajo el Department of Home Affairs, se centra en proteger las infraestructuras críticas de ciberataques y otras amenazas relacionadas con la tecnología.
- **Department of Foreign Affairs and Trade (DFAT):** Gestiona el impacto de las tecnologías críticas y la ciberseguridad en las relaciones internacionales, promoviendo políticas que integran la seguridad nacional y la prosperidad económica global.

En el ámbito privado, el sector de la ciberseguridad se encuentra concentrado, con cuatro empresas que tienen el control del 52,9 % del mercado, según datos de IBIS World 2024. Estas empresas son:

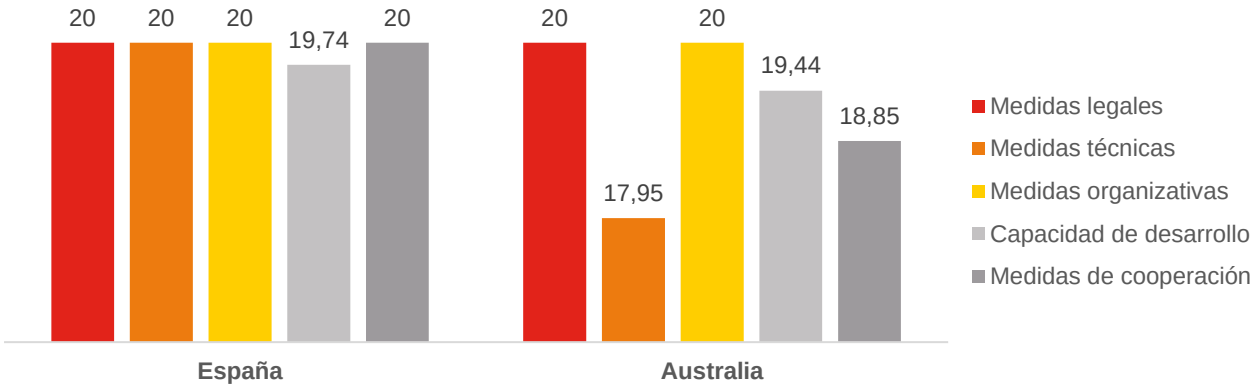
- **Data#3**, especializada en soluciones tecnológicas y servicios de TI, generó ingresos de 423 MAUD en 2024, con una cuota de mercado del 21,9 %.
- **Trend Micro Australia**, líder en ciberseguridad, alcanzó una cuota de mercado del 10,8 % y obtuvo ingresos de 209 MAUD en 2024.
- **Accenture Australia**, consultora global en estrategia y tecnología, tiene una cuota del 10,6 % y sus ingresos suman 205 MAUD.
- **Cisco Systems**, reconocida por su liderazgo en redes y telecomunicaciones, generó ingresos superiores a los 185 MAUD, con una cuota de mercado del 9,6 %.

C. LA OFERTA ESPAÑOLA

España ha emergido como un referente en ciberseguridad, un ámbito que se ha convertido en una prioridad estratégica para empresas, autoridades y la sociedad en general. Según datos del Instituto Nacional de Ciberseguridad (INCIBE), en 2023 se registraron en España más de 83.500 incidentes de ciberseguridad, lo que representa un aumento del 24 % respecto al año anterior. Estos incidentes afectaron a más de 22.000 empresas y 58.000 ciudadanos, reflejando el creciente desafío que supone proteger la infraestructura digital en todos los niveles.

En este contexto, no sorprende que el sector de la ciberseguridad en España alcance un valor de 2.150 millones de euros y se proyecte un crecimiento anual compuesto del 7,16 % hasta 2029, según la consultora Mordor Intelligence. Este desarrollo está respaldado por una posición destacada en el Índice Global de Ciberseguridad 2024 de la Unión Internacional de Telecomunicaciones (UIT). España ha logrado la máxima puntuación en cuatro de los cinco pilares evaluados por esta organización, consolidándose como uno de los líderes mundiales en este ámbito.

PUNTUACIÓN DE ESPAÑA Y AUSTRALIA EN EL ÍNDICE GLOBAL DE CIBERSEGURIDAD 2024
Sobre un total de 20 puntos



Fuente: Índice Global de Ciberseguridad 2024 elaborado por la UIT.

A pesar de que España es uno de los países más avanzados del mundo en materia de ciberseguridad, la distancia con Australia representa una gran barrera para las empresas españolas. A pesar de ello, la compañía **Indra**, a través de su filial en Sídney, ofrece servicios de ciberseguridad que incluyen consultoría estratégica, sistemas avanzados de ciberdefensa, y soluciones de simulación y formación para fortalecer la prevención, detección y respuesta frente a ciberataques en el ámbito militar y civil. Por otro lado, la consultora **NTT Data** también tiene presencia en el país, aunque actualmente su enfoque se centra en servicios de consultoría, soluciones SAP y servicios en la nube, sin ofrecer aún servicios específicos de ciberseguridad.

D. OPORTUNIDADES DEL MERCADO

A pesar de la distancia geográfica, el mercado de la ciberseguridad en Australia presenta varias oportunidades clave, especialmente prometedoras para la oferta española, en áreas como la integración de soluciones basadas en IA, la educación sobre ciberseguridad y la protección de infraestructuras críticas.

- **Teletrabajo y avances tecnológicos:** La adopción del teletrabajo, impulsada por la pandemia, ha generado una creciente necesidad de proteger los datos y redes corporativas. Esto crea oportunidades para empresas españolas que ofrecen **soluciones de seguridad avanzadas**, como redes privadas virtuales (VPN) y sistemas de autenticación sofisticados, ideales para empresas que buscan proteger sus infraestructuras digitales en un entorno remoto.

- **Regulación y legislación:** Leyes como la ***Security of Critical Infrastructure Act 2018*** obligan a las empresas australianas a aumentar sus inversiones en ciberseguridad. Esto presenta una oportunidad para las empresas españolas especializadas en ***software* de ciberseguridad de alta calidad** y soluciones para la protección de infraestructuras críticas. A pesar de que algunas empresas prefieren mantener equipos internos, la necesidad de cumplir con regulaciones y prevenir ciberataques cada vez más sofisticados favorece a los proveedores externos que ofrecen soluciones especializadas y escalables.

- **Evolución hacia *softwares* de ciberseguridad avanzados:** La expansión de la tecnología 5G en Australia está aumentando la exposición de dispositivos inteligentes a ciberataques. Esto crea una oportunidad para las

empresas españolas que desarrollan **soluciones de ciberseguridad avanzadas**, como sistemas de seguridad gestionados y técnicas avanzadas de encriptación de datos, para proteger sistemas más complejos en un entorno digitalizado.

- **Concienciación y educación sobre ciberseguridad:** La creciente concienciación sobre las amenazas cibernéticas ha impulsado programas educativos como la iniciativa **Cyber Smart Challenge** del Gobierno australiano. Las empresas españolas que ofrecen **formación en ciberseguridad**, centrándose en temas como ataques de *phishing* y comportamiento seguro en línea, pueden aprovechar esta tendencia para proporcionar servicios de educación y concienciación, un área crucial para reducir el riesgo de ciberataques.

Estas tendencias indican un fuerte crecimiento del mercado australiano de ciberseguridad, lo que ofrece oportunidades significativas para empresas españolas que puedan proporcionar soluciones innovadoras y servicios especializados en ciberseguridad.

E. CLAVES DE ACCESO AL MERCADO

E.1. Distribución

El acceso a servicios de ciberseguridad en Australia varía según el tipo de cliente, diferenciando entre grandes corporaciones, pequeñas y medianas empresas, y organismos públicos. En todos los casos, las relaciones comerciales entre los actores y los proveedores de servicios suelen ser de largo plazo, con contratos que se mantienen durante varios años con el mismo proveedor. Por este motivo, resulta fundamental realizar un análisis exhaustivo de las distintas opciones disponibles en el mercado. Además, el Gobierno australiano publica guías y recomendaciones para facilitar la contratación de estos servicios. En ellas incide en la importancia de contratar empresas que hayan demostrado un compromiso con la seguridad y transparencia de sus productos.

De esta manera, los principales canales a través de los cuales se accede a estos servicios son:

- Pequeñas y medianas empresas – distribuidores mayoristas como Exclusive Networks o Dicker Data.
- Grandes empresas – contratación directa o integradores de sistemas como CyberCX o DXC Technology.
- Organismos públicos – licitaciones y acuerdos marco a través de la plataforma Digital Marketplace que ofrece el Gobierno australiano.

E.2. Barreras de entrada

El sector de la ciberseguridad en Australia presenta varias barreras significativas. En el **ámbito legal**, los proveedores deben cumplir con estrictas normativas de protección y seguridad de datos, como el *Notifiable Data Breaches Scheme* o la futura normativa *Cyber Security Bill 2024*, ya que su incumplimiento puede conllevar graves sanciones económicas. Además, aunque los costes iniciales en infraestructura y equipos son moderados, la contratación de personal altamente cualificado, que a menudo cuenta con titulaciones universitarias, representa un desafío debido a los **elevados salarios** que hay en el país. La fuerte dependencia del sector de la mano de obra especializada también incrementa los gastos operativos. Por otro lado, la **diferenciación** es crucial en un mercado donde los clientes priorizan proveedores con buena reputación y experiencia comprobada, **lo que dificulta la entrada de nuevas empresas** que deben competir ofreciendo alternativas más económicas o innovadoras para ganar terreno.

E.3. Legislación aplicable y otros requisitos

A principios de octubre de 2024, el Gobierno australiano introdujo un borrador para la primera legislación específica para temas de ciberseguridad en el país, la ***Cyber Security Bill 2024***. Esta normativa parte de la ***2023-2030 Australian Cyber Security Strategy*** y busca reforzar la protección digital mediante medidas clave. Entre estas, se incluye la implementación de estándares de seguridad obligatorios para dispositivos inteligentes y la obligación para ciertas empresas de reportar pagos relacionados con *ransomware* y extorsión cibernética. Además, establece

restricciones sobre el uso de información de ciberseguridad proporcionada voluntariamente al National Cyber Security Coordinator, limitando su uso y divulgación. Finalmente, se propone la creación de una **Junta de Revisión de Incidentes Cibernéticos**, encargada de realizar evaluaciones posteriores a incidentes significativos.

De forma adicional, las empresas de ciberseguridad también tienen que cumplir con las siguientes normas:

- ***Notifiable Data Breaches Scheme***. Obliga a los proveedores de software de ciberseguridad a notificar de inmediato cualquier brecha o pérdida de datos a la Office of the Australian Information Commissioner y a notificar a los clientes afectados de inmediato.
- ***General Data Protection Regulation* (GDPR)**. Introducida por la Unión Europea en 2018, afecta a las empresas australianas que operan o tienen acceso desde la UE. Requiere el consentimiento de los consumidores para el uso de datos personales y obliga a garantizar su seguridad, incluyendo el uso por terceros.
- ***Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018***. Permite a las autoridades acceder a canales de comunicación, incluidos aquellos con cifrado de extremo a extremo, mediante *software* o *hardware*, y obliga a las empresas a crear "puertas traseras" para facilitar este acceso bajo solicitud gubernamental.
- ***The Security of Critical Infrastructure Act 2018* (SOCI)**. Obliga a los propietarios de infraestructura crítica a gestionar riesgos, incluidos los cibernéticos, aumentando la demanda de servicios de ciberseguridad. Además, introduce la **Positive Security Obligation (PSO)**, que exige la gestión de riesgos de infraestructura crítica, y permite la intervención gubernamental ante riesgos significativos.

E.4. Ayudas

E.4.1. Ayudas en España

- **Colaboración INCIBE e ICEX:** Desde 2020, INCIBE e ICEX trabajan juntos para impulsar la competitividad de la ciberseguridad en España, mediante la aceleración de *startups* y el apoyo a su internacionalización. Esta colaboración incluye misiones comerciales, participación en ferias internacionales y eventos como el **ENISE**.
- **Programas ICEX y Cámaras de Comercio:** Apoyo a la internacionalización mediante ayudas económicas y herramientas como el Plan Cameral de Exportaciones.
- **Centro para el Desarrollo Tecnológico Industrial (CDTI):** Financia proyectos de I+D+i tecnológicos, incluyendo cooperación internacional a través de iniciativas multilaterales (como IBEROEKA) y acuerdos bilaterales.
- **Plan Estratégico 2021-2025 de INCIBE**: Centrado en fortalecer la industria de ciberseguridad española, facilita la internacionalización de empresas y mejora su competitividad global.

E.4.2. Ayudas en Australia

Desde el Gobierno de Australia, son varias las propuestas que buscan incentivar la innovación en el sector de la ciberseguridad:

- **Incentivo fiscal para I+D** a través de un crédito fiscal reembolsable para empresas que promuevan la inversión en innovación y desarrollo.
- **Programa REDSPICE**. Cinco millones de dólares australianos destinados a un programa que busca triplicar la capacidad de ciberseguridad de la Australian Signals Directorate y duplicar sus actividades en la intercepción de amenazas cibernéticas.
- **Cyber Security Skills Partnership Innovation Fund**. Fondo de 70 MAUD destinados a mejorar las competencias y diversificar el personal en ciberseguridad.
- **Australian Defence Force Cyber Gap Program**. Programa de 41 MAUD que ofrece apoyo financiero, mentorías y oportunidades de experiencia laboral en defensa para estudiantes de ciberseguridad.
- **Australian Cyber Security Strategy Challenge.** Programa que ofrece financiación a pequeñas y medianas empresas para desarrollar soluciones innovadoras a retos relacionados con políticas y servicios gubernamentales.

E.5. Ferias

En Australia, el tamaño de las ferias suele ser reducido en comparación con el de los eventos que se organizan en España, aun así, estos son algunos de los acontecimientos que se deben marcar en el calendario en el sector de la ciberseguridad:

- **Australian Cyber Conference**. Organizada por la Asociación Australiana de Seguridad de la Información (AISA), se celebra en Canberra del 17 al 19 de marzo de 2025. Este evento reúne a líderes, expertos y profesionales de diversas industrias para explorar estrategias innovadoras en ciberseguridad, con un enfoque en adaptar y transformar prácticas frente a un panorama digital en constante evolución.
- **Cyber Security Summit**. Evento exclusivo por invitación, dirigido a líderes en ciberseguridad de empresas, instituciones y entidades gubernamentales de Australia. La próxima edición tendrá lugar en Melbourne en septiembre de 2025.
- **Security and Government Expo**. Programado para el 21 de noviembre de 2025 en Canberra, ofrece a gerentes de seguridad gubernamentales, instaladores, integradores y consultores de seguridad la oportunidad de conocer las últimas tecnologías de seguridad. El evento servirá como un punto de encuentro clave para el sector de la seguridad en el ámbito gubernamental.
- **Security Edge**. El evento se celebrará el 8 de octubre de 2025 en el Grand Hyatt de Melbourne y reunirá a 150 CISO y CSO de empresas y organismos gubernamentales de Australia. Ofrecerá un día de *networking* exclusivo y análisis basado en datos, centrado en mejorar planteamientos de seguridad, mitigar riesgos y afrontar los desafíos de papeles complejos.

F. INFORMACIÓN ADICIONAL

- **Australian Cyber Collaboration Centre**. Organización sin fines de lucro que reúne los sectores de educación, industria y empresa, promoviendo colaboraciones y sinergias. Su equipo está formado por expertos en defensa, asuntos gubernamentales, gestión de riesgos y tecnología. Además, trabaja con una extensa red de asociaciones nacionales e internacionales en ciberseguridad y espacio.
- ***Australian Cibersecurity Magazine***. Revista especializada en ciberseguridad en Australia. Su objetivo es proporcionar noticias, análisis y artículos de expertos sobre las últimas tendencias, amenazas y soluciones en el campo de la ciberseguridad.
- **Australian Computer Emergency Response Team (AUSCERT)**. Organización nacional de respuesta ante incidentes de ciberseguridad en Australia. Su principal objetivo es ofrecer apoyo, asesoramiento y asistencia a empresas, instituciones y organismos gubernamentales para gestionar y mitigar los incidentes relacionados con la ciberseguridad.
- **Australian Information Security Association (AISA)**. Organización sin ánimo de lucro dedicada a promover la ciberseguridad en Australia. Fundada en 1999, AISA agrupa a profesionales de la seguridad de la información de diversas industrias para fomentar el intercambio de conocimientos, el desarrollo profesional y la colaboración en temas de ciberseguridad.
- **Australian Security Industry Association (ASIAL)**. Es el organismo nacional de referencia para organizaciones y profesionales de la seguridad en Australia. Los miembros de ASIAL representan aproximadamente el 85 % de la industria de la seguridad.

G. CONTACTO

La ***Oficina Económica y Comercial de España en Sídney*** está especializada en ayudar a la internacionalización de la economía española y la asistencia a empresas y emprendedores en **Australia.**

Entre otros, ofrece una serie de **Servicios Personalizados** de consultoría internacional con los que facilitar a dichas empresas: el acceso al mercado de Australia, la búsqueda de posibles socios comerciales (clientes, importadores/distribuidores, proveedores), la organización de agendas de negocios en destino, y estudios de mercado ajustados a las necesidades de la empresa. Para cualquier información adicional sobre este sector contacte con:

Centro Edgecliff, Oficina 408, 4º Piso, 203 New South Head Rd, Edgecliff.
Sídney 2026 – Australia
Teléfono: +61 2 9362 4212
Correo electrónico: sydney@comercio.mineco.es
http://Australia.oficinascomerciales.es

Si desea conocer todos los servicios que ofrece ICEX España Exportación e Inversiones para impulsar la internacionalización de su empresa contacte con:

Ventana Global
913 497 100 (L-J 9 a 17 h; V 9 a 15 h)
informacion@icex.es

Para buscar más información sobre mercados exteriores siga el enlace

AUTOR
Javier Sagüés de la Maza

Oficina Económica y Comercial
de España en Sídney
sidney@comercio.mineco.es
Fecha: 02/12/2024

NIPO: 22424012X