ICEX España Exportación e Inversiones

FS FICHA SECTOR

BRASIL

Ciberseguridad en Brasil

A. CIFRAS CLAVE

Brasil ocupa el 18.º lugar del mundo en el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones de 2022, con una población super conectada, y más del 83,3 % de hogares con acceso a Internet. El **gasto realizado en ciberseguridad en Brasil fue de 188.000 MUSD** en **2023**, lo que supone el **1,35 % del gasto mundial.** Las amenazas en ciberseguridad van en aumento, pues sólo en 2020 los ataques de *malware* y *ransomware* **aumentaron un 358 % y un 435 %** respecto al año anterior. Un factor limitante del mercado es la escasez de mano de obra cualificada, que incrementa los costes de contratación. Se espera que Brasil presente tasas de crecimiento de dos dígitos en los próximos años en el mercado de ciberseguridad.

Principales indicadores	2020	2021	2022	2023	2024
Ingresos en ciberseguridad en Brasil (MUSD)	4.710	5.120	5.560	n.d.	**n.d.**
N.º incidentes en ciberseguridad en Brasil (miles)	319	n.d.	n.d.		
Coste medio Brasil por brecha de seguridad (MUSD)	1,16	n.d.	1,38		
Coste medio mundial por brecha de seguridad (MUSD)	3,86	4,24	4,35		
Población (millones de habs.)	213,2	214,3	215,3	216,4	**217,6**
Crecimiento del PIB	-3,3 %	5 %	2,9 %		
PIB per cápita (USD)	6.923	7.697	8.918	9.185	
Inflación	3 %	10 %	9 %	5 %	**5 %***
SELIC (Tasa interés anual)	4,25 % - 2 %	2 % - 9,25 %	13,75 %	11,75 %	**10,75 %***
Redes móviles (millones)	155	162	n.d.		
Acceso a Internet (% población)	73 %	75 %	81 %	84 %	

Fuente: Elaboración propia a partir de Statista, LAFIS, Mordor Intelligence, Euromonitor, Banco Mundial, IBGE y Banco Central do Brasil.

B. CARACTERÍSTICAS DEL MERCADO

B.1. Definición precisa del sector estudiado

No existe un consenso global sobre la definición de ciberseguridad. Según normas como la ISO/IEC 27032/2012 el término se refiere a la preservación de la confidencialidad, la integridad y la disponibilidad de la información en el ciberespacio, es decir, los principios que guían las actividades de seguridad. En este caso, la seguridad no se dirige en última instancia a proteger el ciberespacio, sino a los sistemas, los usuarios y la información que se ven afectados por las amenazas y los ataques cibernéticos.

El número de amenazas es prácticamente ilimitado y se reproducen a una velocidad de vértigo. Algunos de los ciberincidentes más comunes en la actualidad son: ***phishing*** o ***spear-phishing***: En este tipo de ataque se suplanta la identidad de una entidad en sus comunicaciones electrónicas. ***Malware***: Define cualquier tipo de *software* malicioso diseñado para dañar cualquier dispositivo, servicio o red. ***Ransomware***: Tipo de *malware* que impide o limita el acceso a los sistemas informáticos que infecta. ***Advanced Persistent Threats* (APT):** Ocurre cuando una persona no autorizada gana acceso a la red y no es detectada durante un largo periodo de tiempo. **Denegación de Servicio Distribuida** (***Distributed Denial of Service*** (**DDoS**)): Se produce cuando un número elevado de sistemas comprometidos atacan a un único objetivo, causando una negación del servicio a los usuarios. ***Man-in-the-Middle***: Ocurre cuando las comunicaciones electrónicas entre dos usuarios son interceptadas. ***Fake news,*** o noticias falsas.

Es importante mencionar también que, según el reconocido analista tecnológico y asesor financiero Matthew Ball, la mayor amenaza **para las organizaciones desde una perspectiva operativa, financiera y de marca** en 2023 fue **el *ransomware*.** Sin embargo, el riesgo ha escalado considerablemente con la incorporación de ***modelos generativos de inteligencia artificial***, como ChatGPT. Estos modelos, que pueden crear contenido convincente y automatizado, han ampliado el potencial para ataques más sofisticados y difíciles de detectar, elevando así el nivel de amenaza en el panorama de ciberseguridad.

CÓDIGOS NBS MÁS HABITUALES PARA SERVICIOS TIC

Código BS	Descripción
1.1501	Servicios de consultoría, de seguridad y de soporte en tecnología la de información
1.1501.10.00	Servicios de seguridad en tecnología de la información (TIC)
1.1501.20.00	Servicios de seguridad en tecnología de la información (TIC)
1.1501.30.00	Servicios de soporte en tecnología de la información (TIC)
1.1502	Servicios de proyectos, desarrollo e instalación de aplicativos y programas no personalizados (no estandarizado)
1.1502.10.00	Servicios de proyectos, desarrollo e instalación de aplicativos y programas no personalizados (no estandarizado)
1.1502.20.00	Servicios de proyectos, desarrollo, adaptación e instalación de aplicativos personalizados (estandarizados)
1.1502.30.00	Servicios de proyectos y desarrollo de estructuras de contenido de páginas electrónicas
1.1502.40.00	Servicios de proyectos y desarrollo de estructuras de contenido de bancos de datos

Fuente: Ministério da Fazenda de Brasil.

B.2. Tamaño del mercado

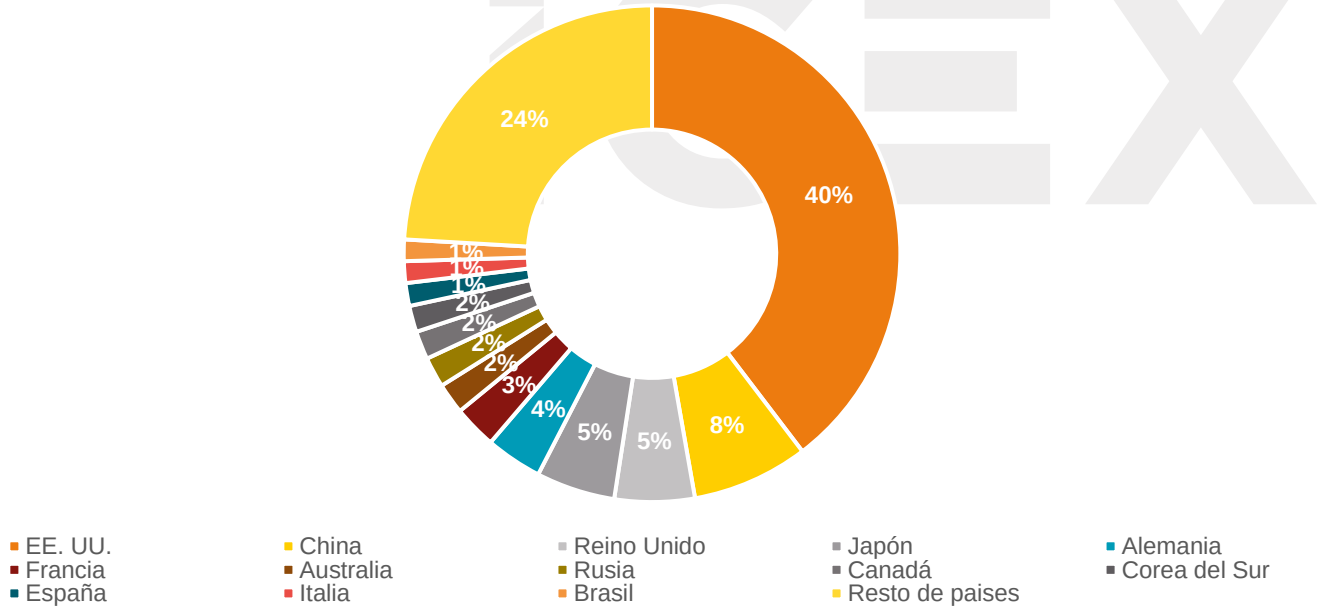
Brasil cuenta con una extensión favorable a la instalación de redes, ya que tiene una zona continental superconectada, con **tres puntos diferentes de llegada de cables submarinos de conexión de alta velocidad**: São Paulo, Río de Janeiro y Fortaleza, convirtiendo así al país en un destino atractivo de inversión en servicios de telecomunicaciones. Sólo **en Brasil, el 83 % de los domicilios cuentan con conexión a Internet, lo que se traduce en 175 millones de usuarios.** Según el informe de 2021 *Internet Organised Crime Threat Assessment – IOCTA,* de la Agencia de Cooperación Policial de la Unión Europea - Europol, "la falta de una legislación adecuada en materia de ciberdelincuencia ha convertido a Brasil en el objetivo número uno y la principal fuente de ataques en línea en América Latina; el 54 % de los ciberataques denunciados en Brasil se habrían originado en el país". El documento continúa diciendo que "al igual que Estados Unidos, Brasil es un importante anfitrión de sitios web de

phishing, y algunos informes sitúan a **Brasil como una de las diez principales fuentes de ciberataques del mundo**".

Según el estudio *Information Security and Risk Management*, publicado por Gartner, el gasto mundial en seguridad de la información ha crecido de 2017 a 2023, pasando de algo menos de 100.000 MUSD en 2017 a casi 200.000 MUSD en 2023. La mayor parte del gasto se ha concentrado en servicios de seguridad, protección de infraestructuras y equipos de seguridad de redes. Se espera que el gasto en servicios de seguridad **alcance casi los 250.000 MUSD en 2027.**

Brasil se encuentra en la decimoquinta posición por **gasto realizado en ciberseguridad, con 995 millones de euros en 2018**, es decir, un peso relativo del 1,02 % mundial, que aumentó a 1,35 % en 2023. Según estimaciones realizadas en 2017, la ciberdelincuencia provoca **pérdidas anuales en Brasil por valor de 20.000 millones de euros**, lo que lo sitúa como el **segundo país del mundo con más pérdidas por ciberataques**, sólo detrás de China (Norton Security. (2017). *Cyber safety insights report*, 2017). En 2021, Brasil revalidó su posición como **el país con mayor índice de víctimas de *phishing* en Internet** (Kaspersky. (2021). *Spam and phishing* 2021). Según un estudio de PSafe de 2018, en total, **el 57,4 % de los ataques se realizaron mediante *phishing***, y en segundo lugar se encontraban las estafas con publicidad sospechosa, que supusieron el 19 % de los casos. En Brasil son especialmente comunes los ataques a los usuarios finales a través de ***apps* de mensajería.** El país sufre la tendencia mundial de ataques a través de ***ransomware***, *malware* que explota una grieta en la seguridad y criptografía y que supusieron 3,4 billones de ataques de enero a septiembre de 2020.

GASTO MUNDIAL EN CIBERSEGURIDAD
Datos de 2023: países con cuota superior al 1 % (Total: 188.100 MEUR)



Fuente: *Information Security and Risk Management Worldwide*, Statista (2023).

En 2021, Brasil fue el segundo país del mundo con mayor número de ciberataques, convirtiéndose en el país con mayor proporción de usuarios atacados con *ransomware* en América Latina. Entre el 1 de enero y el 3 de agosto de 2021, Brasil sufrió más de 439.000 ataques cibernéticos, lo que representa el 7,1 % del total de 6,4 millones realizados en todo el mundo. Esto sitúa al país en segunda posición, detrás sólo de EE. UU., que encabeza la lista con más de 1,33 millones de ataques (21,7 %), según un informe de la empresa especializada Netscout. En tercer lugar está Corea del Sur, con 385.808 ataques (6,3 %), seguido por el Reino Unido, con 348.330 (5,7 %), y China, con 256.985 (4,2 %).

Según el informe titulado "Los ataques de *ransomware* son cada vez más sofisticados", la situación entre 2022 y 2023 es la siguiente: "En 2022, las soluciones de Kaspersky detectaron más de 74 millones de intentos de ataques

de *ransomware*, un aumento del 20 % con respecto a 2021 (61,7 millones). Ya a principios de 2023, vimos una ligera disminución en la cantidad de ataques de *ransomware*. Sin embargo, estos se han vuelto más sofisticados y específicos. Además, ha habido un cambio drástico entre los grupos de *ransomware* más influyentes y prolíficos. REvil y Conti, que ocuparon, respectivamente, el segundo y tercer lugar en cuanto a ataques en el primer trimestre de 2022, fueron reemplazados, en los primeros tres meses de 2023, por Vice Society y BlackCat. Dos de los otros grupos que están más activos ahora mismo son los Clop y los Royal".

En cuanto a los usuarios de móviles atacados por ***malware***, Argentina fue el país más atacado, con un 9 %. Mientras tanto, el 7 % de los usuarios de móviles en Brasil se enfrentaron al mismo problema *(Kaspersky Lab. (2021). Latin America: share of mobile users attacked by malware 2020, by country*. Statista). Brasil ha sido también el país con el mayor porcentaje de usuarios atacados por ***phishing***, con un 19,94 % *(Kaspersky Lab. (2021). Latin America & the Caribbean: share of users attacked by phishing 2020, by country*. Statista). En relación con ell coste medio de una violación de datos, en 2022, en Brasil la cifra fue de 1,36 MUSD, de las cifras más bajas de los países analizados (Ponemon Institute. (2022). *Average total cost per data breach worldwide 2022, by country or region.* Statista).

B.3. Principales actores

La ciberseguridad brasileña tradicionalmente se ha asociado a un grupo específico de organismos, como son el **Gabinete de Seguridad Institucional (GSI),** las **Fuerzas Armadas,** las **agencias de inteligencia,** la **Policía Federal** y los **centros de respuesta a incidentes.** El GSI y las Fuerzas Armadas (Comando de Ciberdefensa y Centro de Ciberdefensa) se erigen como el punto central de las responsabilidades y competencias asociadas a la ciberseguridad y la ciberdefensa, desde el punto de vista estratégico "macro" o público. Esto se debe en gran medida a la rápida institucionalización de las capacidades y responsabilidades cibernéticas en estos dos organismos durante las Olimpiadas de Rio de Janeiro de 2016 o el Mundial de Fútbol de 2014. Pero la responsabilidad práctica y la actuación en cuestiones relacionadas con la ciberseguridad en toda la economía dependen de un grupo más amplio de actores.

Algunos los servicios que conforman la cadena de ciberseguridad empiezan a ser *commodities*. Para estos servicios en el mercado de la ciberseguridad en Brasil son muy fuertes las ***Big Four*** (EY, PwC, Deloitte y KPMG), así como la multinacional de consultoría Accenture (Sêmola, M. (2021). Entrevista realizada por esta Oficina Económica y Comercial el 26 de julio de 2021 al Prof. Marcos Sêmola, experto en ciberseguridad de la Fundação Gentúlio Vargas (FGV)). Tras la publicación del estudio *ISG Provider Lens™ – Cybersecurity – Solutions and Services* es posible observar un análisis detallado de los competidores en servicios de soluciones del territorio brasileño, además de conocer los principales actores del mercado. El enlace para acceder a esta información es el siguiente: *Análisis de competidores y principales actores del mercado brasileño.*

C. LA OFERTA ESPAÑOLA

Hay una serie de empresas españolas con presencia en Brasil que trabajan en el sector de la ciberseguridad, como son **Indra, Panda, Eleven Paths** (Telefónica) o **Entelgy**. **Neoenergia** (Iberdrola), la mayor empresa eléctrica de Brasil, es reconocida por su sistema de protección de infraestructura crítica desarrollado internamente por la propia empresa, ya que la compañía utiliza sus propios recursos y conocimientos para diseñar e implementar medidas de seguridad adaptadas a sus necesidades específicas y entorno operativo. Este enfoque asegura que Neonergia mantenga el control total sobre los protocolos de seguridad y pueda adaptarse rápidamente a nuevas amenazas y avances tecnológicos. Con todo, y pese a que España se sitúa en el 7.° puesto de 193 países en el Global Cybersecurity Index, de la Unión Internacional de Telecomunicaciones, **en este sector el origen español no supone, *a priori*, una característica beneficiosa ni perjudicial a la hora de contratar un producto o servicio**. En todo caso, el **país de origen**, aquel donde la solución de ciberseguridad ha sido desarrollada, es visto como un **atributo poco relevante por los expertos del sector**. Son las características técnicas de la oferta y su precio los criterios que realmente importan a la hora de llevar a cabo la valoración de la solución de ciberseguridad**.**

D. OPORTUNIDADES DEL MERCADO

El elevado número de ataques recibidos y la falta de madurez de la ciberseguridad en el país, acelerada sólo recientemente a través de cambios legislativos y por los efectos de la COVID-19, hacen que las oportunidades en sector sean muy amplias. En general, la mayor parte de los sectores de la economía necesitarán crecer en medidas de ciberseguridad, más aún tras la aprobación de la Ley General de Protección de Datos (LGPD), de obligado cumplimiento. Con todo, hay sectores que tienen un fuerte componente de tratamiento de datos, y que por ello se exponen a más riesgos e invertirán más, como pueden ser los **B2C**, **banca y finanzas**, ***e-commerce*** o el sector de la **salud**. El más fuerte en capacidades de ciberseguridad es el financiero, mientras que los más débiles actualmente son el de salud que, por su naturaleza y en ocasiones, prioriza la atención ante la seguridad de la información, así como el sector del *retail* o venta minorista.

La visibilidad y la protección de los datos están ganando atención, ya sea por el reciente aumento de los ataques o por las necesidades planteadas por la LGPD. La seguridad digital debe formar parte de las estrategias empresariales. Los casos de filtración de datos, por ejemplo, ya no son una noticia infrecuente, y ser víctima de un incidente puede poner en riesgo toda la planificación de una empresa, arruinar su reputación y causar importantes pérdidas económicas.

E. CLAVES DE ACCESO AL MERCADO

E.1. Distribución

E.1.1. Administración pública

La administración pública brasileña debe satisfacer sus necesidades de equipamiento y soluciones de ciberseguridad a través de procesos competitivos. Normalmente, a través de **licitaciones públicas**. De este modo, los concursos públicos publicados por los distintos niveles del Gobierno brasileño, federal, estatal y municipal constituyen una primera vía de acceso al mercado.

En Brasil, las compras públicas están reguladas por la Ley 14.133/2021, sobre licitaciones y contratos administrativos, que fue aprobada en abril de 2021 y entró en vigor en enero de 2024, tras un período de convivencia con el anterior marco regulatorio. Esta ley otorga a las empresas extranjeras la posibilidad de participar en licitaciones, siempre que cumplan los requisitos para su habilitación. Pueden participar las empresas extranjeras, con o sin funcionamiento en territorio brasileño, en licitaciones que tengan o no recursos internacionales, siempre siguiendo las condiciones especiales que pueden surgir en las convocatorias. Para más información se recomienda consultar el documento *El mercado de las licitaciones en Brasil 2022*, disponible en el portal de ICEX.

El principal sistema para obtener más información sobre el mundo de las licitaciones públicas es el Portal de Compras del Gobierno Federal (https://www.gov.br/compras/), cuya gestión está a cargo del Ministerio de Planificación, Presupuesto y Gestión. Asimismo, el art. 54 de la Nueva Ley de Licitaciones y Contratos establece que, para agilizar los procesos de licitación, todos los documentos relacionados con nuevas licitaciones deberán publicarse en una página web creada específicamente para centralizar esta actividad, el Portal Nacional de Contratación Pública (PNCP).

E.2. Barreras reglamentarias y no reglamentarias

E.2.1. Aspectos tributarios

Uno de los principales retos en Brasil es su complejo sistema tributario, que involucra impuestos en los niveles federal, estatal y municipal, con tasas a menudo elevadas. Esta complejidad se acentúa en la prestación de servicios desde el extranjero, que se enfrentan a una carga fiscal mayor, comparada con los servicios ofrecidos por empresas locales.

Además, es importante considerar los diferentes contratos de *software*, lo que puede influir, de nuevo, en los tributos aplicables.

E.2.2. Tributación aplicable a importación de servicios

La carga fiscal sobre la importación de servicios varía según su naturaleza y recae sobre los pagos dirigidos a residentes o domiciliados en el extranjero. Para consultar los tributos que existen actualmente en Brasil sobre la importación de servicios haga clic en el siguiente enlace: Tributación aplicable a la importación de servicios.

E.2.3. Contratos relativos a *software*

En primer lugar, debe tenerse en cuenta que las reglas para la aplicación de tributos a la importación están conformadas por la legislación tributaria, diferentes sentencias del Supremo Tribunal Federal, y las orientaciones proporcionadas por las "resoluciones de consultas" de la Receita Federal (equivalente a la Agencia Tributaria española). La Receita Federal distingue diferentes tipos de contratos relativos a *software*:

1. Acuerdo de **licencia de uso**.
2. Acuerdo de **licencia de derechos de distribución y comercialización** de *software* producido en el extranjero. Los pagos efectuados al extranjero como contraprestación por esta licencia se tratarían como una remuneración por derechos de autor (*royalties*).
3. Acuerdo para la **prestación de servicios** relacionados con programas informáticos (instalación, mantenimiento y soporte técnico), sin transferencia de tecnología.
4. Acuerdo de licencia de uso de programas informáticos o acuerdos de distribución y comercialización de programas informáticos y servicios conexos que impliquen la **transferencia de tecnología** (que implicaría la cesión del código fuente y conocimientos para su modificación).

De manera resumida, en los acuerdos de licencia de derechos de distribución y comercialización de *software* producido en el extranjero (caso 2), y en los acuerdos para la prestación de servicios relacionados con programas informáticos (caso 3), serían de aplicación:

- Impuesto sobre la Renta (IR).
- Programa de Integración Social – Importación (PIS).
- Aportación para la Financiación de la Seguridad Social – Importación (COFINS).
- Impuesto sobre los Servicios de Cualquier Naturaleza (ISS).
- Impuesto sobre Operaciones de crédito, cambio y seguro (IOF).

Si el *software* objeto del acuerdo de licencia de derechos de distribución y comercialización es revendido en formato SaaS, o en caso de existir una transferencia de tecnología que implique la cesión y modificación del código fuente (caso 4), sería de aplicación también:

- Contribuciones para la intervención en el ámbito económico, por el pago de *royalties* (CIDE - *royalties*).

E.2.4. Aspectos legislativos del sector de la ciberseguridad

La legislación sobre ciberseguridad en Brasil aún está en desarrollo, ya que no existe una normativa nacional que aborde explícitamente la seguridad cibernética. No obstante, existen varios marcos legislativos y directrices relacionados con el sector de Internet. Entre ellos:

- El Marco Civil de Internet, establecido por la Ley n.° 12.965/2014 y modificado por el Proyecto de Ley n.º 428/2024.
- La Ley de Delitos Cibernéticos (Ley n.° 12.737/2012), que tipifica formalmente los delitos cibernéticos.
- En 2018, Brasil aprobó la Ley General de Protección de Datos (LGPD, Ley n.º 13.709/2018), inspirada en el RGPD de la Unión Europea y modificada en 2019 por la Ley n.º 13.853/2019.
- Además, el Proyecto de Ley PL 2630/2020 propone la Ley Brasileña de Libertad, Responsabilidad y Transparencia en Internet, conocida como la Ley de *Fake News*.

- En diciembre de 2023, se publicó el Decreto n.º 11.856/2023 en el *Diario Oficial de la Unión*, que establece los principios, objetivos e instrumentos de la Política Nacional de Ciberseguridad y define la competencia y composición del Comité Nacional de Ciberseguridad.

Por último, cabe destacar la Ley de Propiedad Industrial (Ley 9.279 de 1996). Regula aspectos generales de patentes y marcas, incluyendo la licencia y transferencia de tecnología. Esta ley también contiene disposiciones para la protección de derechos de autor y patentes de *software* en ciberseguridad, ofreciendo protección bajo la ley de derechos de autor y estableciendo criterios para la patentabilidad de *software*, siempre que cumpla con los requisitos de novedad, actividad inventiva y aplicación industrial.

E.3. Ayudas

INCIBE (el **Instituto Nacional de Ciberseguridad** español) e ICEX España Exportación e Inversiones han firmado un acuerdo de colaboración en febrero de 2020, que tiene como objetivo mejorar la competitividad del sector de la ciberseguridad en España mediante la aceleración de empresas emergentes y apoyando la expansión internacional de la industria. Ambos organismos desarrollan conjuntamente **misiones comerciales directas o inversas** para la apertura o consolidación de la presencia española en mercados internacionales, participan en **ferias internacionales** de referencia en el sector, así como en el **Encuentro Internacional de Seguridad de la Información (ENISE).**

E.4. Ferias

- **Cyber Security Summit 2024:** Cyber Security Summit 2024 Brasil
- **Mind the Sec 2024:** https://www.mindthesec.com.br
- **ISC Brasil 2024,** Feira e Conferência Internacional de Segurança: https://www.iscbrasil.com.br/
- **Exposec 2024,** Feria Internacional de Segurança: http://exposec.tmp.br/16/
- **Futurecom 2024:** https://www.futurecom.com.br
- **Congreso Security Leaders Brasil 2024:** http://www.securityleaders.com.br/

F. CONTACTO

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

Entre otros, ofrece una serie de **Servicios Personalizados** de consultoría internacional con los que facilitar a dichas empresas: el acceso al mercado de Brasil, 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:

Plaza Praça General Gentil Falcão,
108 - 8º andar conjunto 82 Brooklin Novo,
São Paulo 04571-150, Brasil

Teléfono: +55 (11) 5105 4378
Correo electrónico: saopaulo@comercio.mineco.es
http://Brasil.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

AUTORA
Sara Cabezuelo Ayuso

Oficina Económica y Comercial
de España en São Paulo
saopaulo@comercio.mineco.es
Fecha: 10/08/2024

NIPO: 22424012X