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 2022 de la Unión Internacional de Telecomunicaciones, con una población muy conectada de más del 83,3 % de hogares con acceso a Internet. Además, se estima que el **gasto realizado en ciberseguridad mundial será de alrededor de 172.000 millones de USD en 2022**, y Brasil representó un **peso relativo del 1,02 % del gasto mundial en 2018 (995 MEUR).** Las amenazas en ciberseguridad van en aumento, pues sólo en 2020, los ataques de *malware* y *ransomware* **aumentaron un 358 % y un 435 %**, respectivamente, frente al año anterior. Un factor limitante del mercado es la escasez de mano de obra cualificada, incrementando los costes de contratación. Se espera que Brasil presente crecimientos de dos dígitos en los próximos años en el mercado de ciberseguridad.

Principales indicadores	2018	2019	2020	2021	2022
Ingresos en ciberseguridad Brasil (miles de millones USD)	3,99	4,33	4,71	5,12	5,56
N.º incidentes en ciberseguridad en Brasil (miles)	676,51	875,33	318,70	-	-
Coste medio en Brasil por brecha de seguridad (MUSD)	-	-	1,16	-	1,38
Coste medio mundial por brecha de seguridad (MUSD)	3,86	3,92	3,86	4,24	4,35
Población (millones habs.)	210,00	211,00	212,60	213,3	213,3*
Crecimiento del PIB	1,80 %	1,40 %	-4,10 %	4,6 %	2,76 %
PIB per cápita (USD)	9.151	8.898	6.797	7.541	-
Tasa de inflación	3,7 %	3,7 %	3,2 %	10,06 %	5,91 %
SELIC (Tasa de interés anual)	6,75 % - 6,5 %	6,5 % - 5 %	4,25 % - 2 %	2 % - 9,25 %	13,75 %
Redes móviles (millones)	140,30	148,40	155,40	161,80	-
Acceso a Internet (% población)	67,00 %	70,40 %	73,20 %	75,70 %	-

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 los sistemas, los usuarios y la información que lo componen, actúan y se ven afectados por las amenazas y los ataques cibernéticos.

El número de amenazas es prácticamente ilimitado, 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***: 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.

CÓDIGOS NBS* MÁS HABITUALES PARA SERVICIOS TIC

Código NBS	Descripción
1.1501	Servicios de consultoría, de seguridad y de soporte en tecnología de la 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 estandarizados)
1.1502.10.00	Servicios de proyectos, desarrollo e instalación de aplicativos y programas no personalizados (no estandarizados)
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

* Nomenclatura Brasileira de Serviços.

Fuente: *Ministério da Fazenda* de Brasil.

B.2. Tamaño del mercado

Brasil cuenta con una extensión favorable para la instalación de redes, ya que cuenta con 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. **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 primer objetivo 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 *Global Digital Trust Insights*, **en 2022 el gasto mundial en ciberseguridad ascenderá a 172.000 MUSD**. En 2018, este gasto fue de 97.500 MEUR, por lo que, teniendo en cuenta el tipo de cambio 1 EUR = 1,16 USD, el gasto mundial ha aumentado más de un 50 % en 4 años. Brasil ocupa la decimoquinta posición por **gasto**

realizado en ciberseguridad, con 995 MEUR en 2018, es decir, un peso relativo del 1,02 % mundial, cifra muy baja en comparación con los países lideres, EE. UU., Japón y Reino Unido, con un 42,03 %, 9,25 % y 6,26 % respectivamente. Según estimaciones realizadas en 2017, la ciberdelincuencia provoca **pérdidas anuales en Brasil por valor de 20.000 MEUR**, lo que lo sitúa como el **segundo país del mundo con más pérdidas por ciberataques**, sólo por 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 19,2 % 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.

Brasil ocupa el tercer lugar del mundo por el aumento del número de ciberataques en 2021 (78 %), por detrás de Turquía (82 %) y Suecia (80 %). El 53 % considera que los ataques son actualmente demasiado avanzados para que sus equipos informáticos puedan bloquearlos por sí mismos. En caso de ataque, el 93 % de las empresas recuperan sus datos, un 22 % pagando un rescate, el 67 % con copias de seguridad y otro 4 % a través de otros medios.

En 2021, **Brasil tenía la mayor proporción de usuarios únicos atacados con *ransomware* en América Latina**, con casi el **46,7 % de los usuarios de ordenador infectados** (Kaspersky Lab. (2021). Latin America: internet users attacked by malware 2021. Statista). En cuanto a los usuarios de móviles atacados por ***malware***, Argentina fue el país más atacado, con un 9 %. Mientras tanto, el 7,04 % 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 al 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 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 la Copa 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 de 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 e 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)). En la tabla se presentan los competidores en el territorio brasileño según el estudio *ISG Provider Lens™ – Cybersecurity – Solutions and Services*:

ANÁLISIS DE COMPETIDORES EN BRASIL

	Gestión de identidades y accesos (IAM)	Prevención de fugas y pérdidas de datos (DLP) y seguridad de los datos	Protección, detección y respuesta avanzadas a las amenazas a los puntos finales (ETPDR avanzadas)	Servicios técnicos de seguridad	Servicios estratégicos de seguridad	Servicios de seguridad gestionados
Absolute Software		●	●			
Accenture					●	●
Agility Networks				●	●	●
Ativy				●	●	●

	Gestión de identidades y accesos (IAM)	Prevención de fugas y pérdidas de datos (DLP) y seguridad de los datos	Protección, detección y respuesta avanzadas a las amenazas a los puntos finales (ETPDR avanzadas)	Servicios técnicos de seguridad	Servicios estratégicos de seguridad	Servicios de seguridad gestionados
Broadcom	●	●	●			
Capgemini				●	●	●
Check Point	●	●	●			
Cipher			●		●	●
Claranet				●	●	●
Compasso UOL						
Compugraf				●		
Deloitte				●	●	
DXC				●	●	●
E-TRUST	●					
EY					●	
FastHelp				●		●
FireEye			●			
Forcepoint		●				
Forgerock	●					
Fortinet	●	●	●			
GBS		●				
Google DLP		●				
HelpSystems		●				
IBM	●	●	●	●	●	●
ISH Tecnologia				●	●	●
Kaspersky			●			
Kryptus					●	
Logicalis				●	●	●
Lumen						●
McAfee		●	●			
Micro Focus	●					
Microsoft	●	●	●			
NEC				●	●	●
Netskope		●				
Nextios				●		
NTT Data (Everis)				●	●	
Okta	●					
One Identity	●					
OneLogin	●					
OpenText		●	●			
Oracle	●					
Ping Identity	●					
PwC					●	
RSA	●					
SailPoint	●					
SAP	●					
senhasegura	●					
Sonda				●		●
Sophos		●	●			
Stefanini Rafael				●	●	●
TDeC				●		
Thales	●					
TIVIT	●					●
Trend Micro		●	●			
T-Systems				●		
Unisys					●	●
Varonis		●	●			
VMware Carbon Black			●			
Watchguard		●				

	Gestión de identidades y accesos (IAM)	Prevención de fugas y pérdidas de datos (DLP) y seguridad de los datos	Protección, detección y respuesta avanzadas a las amenazas a los puntos finales (ETPDR avanzadas)	Servicios técnicos de seguridad	Servicios estratégicos de seguridad	Servicios de seguridad gestionados
Wipro				●	●	●
Zscaler		●				

Leyenda: Competidor *Product/Market challenger* Líder Actor emergente

Fuente: Information Services Group, Inc. (2021) Brito. P. (2021). *ISG Provider Lens – Cybersecurity – Soultions and Services - Brazil 2020*. Information Services Group.

C. LA OFERTA ESPAÑOLA

En Brasil, existe una serie de empresas españolas con presencia en el país que trabajan en el sector de ciberseguridad como son **Indra, Panda, Eleven Paths** (Telefónica) o **Entelgy**. **Neoenergia** (Iberdrola), la mayor empresa eléctrica de Brasil cuenta con una buena reputación en su sistema de protección de la infraestructura crítica. Con todo, y pese a que España se sitúa en el 7.° puesto de 193 países del *Global Cybersecurity Index*, de la Unión Internacional de Telecomunicaciones (UIT), **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**, el dónde ha sido desarrollada la solución de ciberseguridad, 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, impulsada sólo recientemente a través de cambios legislativos y por los efectos de la COVID-19, hacen que las oportunidades en el sector sean muy amplias. En general, la mayor parte de los sectores de la economía necesitan ampliar medidas de ciberseguridad, más aún tras la aprobación de la 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 ciberseguridad es el sector financiero, mientras que los más débiles actualmente son el de salud que, por su naturaleza y en ocasiones, prioriza la atención a la seguridad de la información, así como el sector de la venta minorista. La visibilidad y la protección de los datos están ganando atención, por el reciente aumento de los ataques o por las necesidades planteadas por la LGPD. La seguridad digital ha de ser una estrategia empresarial, pues ser víctima de un incidente puede arruinar la reputación y causar importantes pérdidas económicas.

E. CLAVES DE ACCESO AL MERCADO

E.1. Distribución

E.1.1. Cliente público

El cliente público en general utiliza el método de la **licitación pública** para satisfacer sus necesidades de equipamiento y soluciones de ciberseguridad. De este modo, los concursos públicos establecidos por los distintos niveles del Gobierno brasileño, tanto federal como estatal, constituyen una primera vía de acceso al mercado. En Brasil, las compras públicas son reguladas por la Ley 8.666 de 1993, más conocida como la “Ley de Licitaciones”. Esta Ley otorga a las empresas extranjeras la posibilidad de participar en licitaciones, siempre que se cumplan los requisitos para su habilitación. Pueden participar las empresas extranjeras, con o sin operaciones 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 aconseja consultar la Ley indicada. El principal sistema en el que 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.

E.1.2. Cliente privado

En cuanto al cliente empresarial, se puede trazar una línea divisoria entre la gran empresa y la pyme. Las **grandes empresas**, por lo general, solicitan cotizaciones a diferentes empresas del sector. Las relaciones previas que la compañía tenga con su proveedor de confianza pueden constituir otra posible vía para conseguir contratos. En cuanto a las **pymes**, en función de los recursos que tengan y la sensibilidad de la información con la que trabajen, dedicarán una proporción mayor o menor de sus presupuestos a cubrir sus necesidades de ciberseguridad. Dicho esfuerzo presupuestario se destinará principalmente a *software* antivirus/cortafuegos y soluciones básicas de protección de equipos y comunicaciones. Por lo general, este tipo de compañías hará uso de su distribuidor de confianza (tanto en grandes superficies como tiendas de carácter local) para adquirir la solución que más se ajuste a sus necesidades. En Brasil, los canales de distribución se dividen en tres tipos de empresas:

- **Distribuidores**. Son mayoristas de grandes dimensiones, con gran conocimiento del mercado y de los revendedores existentes. Normalmente, distribuyen todo tipo de *software* y *hardware*, y suelen tener una cartera de productos muy amplia: sistemas operativos, antivirus, etc.
- **Revendedores** (*resellers*). Distribuidores de menor envergadura. Su función consiste en distribuir los productos de la empresa fabricante entre minoristas, con acceso al cliente final.
- **Integradores**. Los integradores se encargan de realizar un proyecto para el cliente, en el que proveen el *software* necesario para satisfacer sus demandas. Una de las ventajas de lanzar nuevos productos a través de este canal es la reducción del tiempo de lanzamiento al mercado y los costes de distribución.

E.2. Barreras reglamentarias y no reglamentarias

E.2.1. Aspectos tributarios

La ciberseguridad corresponde mayoritariamente a la prestación de servicios, puesto que la venta de *software* en formato digital se enmarca en la tributación por servicios. Por ello, las empresas extranjeras prestadoras de servicios en Brasil pueden estar sujetas a los siguientes tipos de impuestos:

- **IOF** - Impuesto sobre las Transacciones Financieras. El tipo impositivo es del 0,38 % sobre el importe pagado.
- **ISS o ISSQN** - Impuesto sobre los servicios de cualquier naturaleza, a partir del 2 % y con un máximo del 5 %.
- **PIS y COFINS/**Importación. Su incidencia oscila entre el 1,65 % para el PIS y el 7,60 % para el COFINS.
- **CIDE** - Contribución para la Intervención en el Ámbito Económico.
- **IRRF** - Retención del impuesto sobre la renta, el tipo aplicable es del 15 %.
- Existe un **Convenio de Doble Imposición** (CDI) España–Brasil
- **Ley de Programas Informáticos n.° 9.609/98 y Derecho de Autor n.° 9.610/98,** que regulan los temas de propiedad intelectual y comercialización de *software*.
- **Ley n.º 116, de 31 de julio de 2003,** que regula la tasa de servicios de cualquier tipo y la competencia de los municipios.
- **Normativa MCTI n.º 721, de 10 de octubre de 2012,** por la que se establece el programa de aceleración de empresas de *software* y servicios informáticos.
- **Normativa n.º 181, de 28 de septiembre de 1989,** por la que se regula la tributación de los derechos de autor en la adquisición de programas informáticos, a favor de los beneficiarios residentes o domiciliados en el extranjero.

E.2.2. Aspectos legislativos del sector de la ciberseguridad

La legislación en materia de nuevas tecnologías se modifica continuamente en función de los nuevos problemas y necesidades que van surgiendo. Por esto, **se recomienda a los empresarios contar con la ayuda de asesorías y despachos especializados para definir con precisión desde el primer momento el marco legislativo que van a tener que aplicar**. La legislación sobre ciberseguridad en Brasil todavía está en vías de desarrollo, ya que no existe una normativa nacional que trate explícitamente la seguridad cibernética en el país. Sin embargo, sí que existen marcos legislativos y directrices que están relacionados con el sector de Internet en Brasil. El marco de los **Derechos Civiles de Brasil para Internet** viene recogido en la Ley n.° 12.965/2014. La **Ley de Delitos**

Cibernéticos (Ley n.° 12.737/2012), tipifica formalmente el delito cibernético. En julio de 2018 Brasil aprobó la **Ley General de Protección de Datos (LGPD)** (Ley n.º 13.709/2018), **inspirada en el Reglamento General de Protección de Datos (GDPR) de la Unión Europea**, pero no entró en vigor hasta el 18 de septiembre de 2020. Existe un Proyecto de Ley, PL 2630/2020, que instituye la **Ley Brasileña de Libertad, Responsabilidad y Transparencia en Internet**, conocida como la Ley de las *Fake News.*

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 2023**: https://www.cybersecuritysummit.com.br/
- **Mind the Sec**: https://www.mindthesec.com.br
- **Gartner Security Summit**: https://www.gartner.com/en/conferences/na/security-risk-management-us
- **ISC Brasil** - Feira e Conferência Internacional de Segurança: https://www.iscbrasil.com.br/
- **Exposec 2023**– Feria Internacional de Segurança: http://exposec.tmp.br/16/
- **Congreso Security Leaders Brasil:** http://www.securityleaders.com.br/
- **IT Forum 2023**: https://itforum.com.br/foruns/participe/

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
Email: 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

AUTOR
Marco Bernabé Lang

Oficina Económica y Comercial
de España en São Paulo
saopaulo@comercio.mineco.es
Fecha: 25/11/2022

NIPO: 114-22-016-9