ICEX España Exportación e Inversiones

FS FICHA SECTOR

MÉXICO

Ciberseguridad en México

A. CIFRAS CLAVE

México es uno de los países del mundo que más crece anualmente en cuanto a digitalización y penetración de Internet, aunque se encuentra lejos de los niveles de países más desarrollados como España. Como consecuencia de este aumento de la digitalización en los últimos años, el nivel de ataques cibernéticos también ha crecido considerablemente, siendo el segundo país en América Latina con más incidentes de ciberseguridad en 2018.

El gasto en ciberseguridad es bajo comparado con el de otros países, pero se prevé que crezca a una media anual del 4,83 % entre 2020 y 2023, teniendo en cuenta el impacto negativo de la crisis sanitaria de este año.

TABLA 1. DATOS DEL MERCADO MEXICANO

		2019	2020	2021 (previsión)
Crecimiento PIB real	%	-0,3	-10,5	3,3
PIB per cápita	USD	10.118	n. d.	n. d.
Inflación	%	2,83	2,43	3,00
Cuenta Corriente	% PIB	-0,19	-0,28	-0,40
Déficit fiscal	% PIB	-2,3	-6	-4
Población	Millones habs.	125,93	127,09	128,23
Penetración de internet en México	%	70,1 %	76 %	n. d.
Gasto en Ciberseguridad	MUSD	944,82	975,81	1.023,62
Crecimiento del gasto	%	5,51 %	3,28 %	4,90 %

Fuente: FMI, World Economic Outlook Database (2020); INEGI, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (2019); INCIBE, *La Ciberseguridad en el mundo. Situación de España* (2020).

B. CARACTERÍSTICAS DEL MERCADO

B.1. Definición del sector estudiado

El ecosistema de la ciberseguridad comprende todo un conjunto de medidas susceptibles de ser implementadas para defenderse de ciberataques mediante legislación, políticas, herramientas, tecnologías y acciones que pueden ser utilizadas para proteger los activos informáticos de las administraciones, empresas y particulares.

La Corporación Internacional de Datos (IDC) divide el sector de ciberseguridad en **servicios, *software*, *hardware* y seguridad en la nube.** En la actualidad, el sector de los **servicios** es el que mayor peso tiene en el mercado a nivel mundial, con aproximadamente el 64 %, seguido de ***software*** con un 19 %, ***hardware*** con un 13 % y **seguridad en la nube** con un 4 %.

La ciberseguridad es un sector cada vez más esencial debido a la rápida evolución y desarrollo de la economía digital. En la medida en que cada vez más productos y servicios de todo tipo se conectan a Internet, aumenta la necesidad de abordar de forma proactiva su seguridad aumenta. En consecuencia, las organizaciones con visión de futuro están requiriendo nuevos modelos de ciberseguridad ágiles, capaces de actuar y adaptables a la evolución de riesgos y amenazas.

En el último reporte de riesgos globales elaborado por el Foro Económico Mundial, el **riesgo de ciberataques** ocupa el séptimo puesto en cuanto a probabilidad, y el octavo en impacto[1]. Este término apareció por primera vez en los informes de la organización en 2010, y ha ido ganando importancia desde entonces.

Cabe destacar que la ciberseguridad está cobrando cada vez mayor protagonismo en sectores de **infraestructuras críticas** para un país, cuya perturbación o destrucción tendrían un gran impacto en los servicios esenciales. La normativa española incluye dentro de estos sectores: energía, salud, transportes, comunicación, alimentación o agua[2].

B.2. Tamaño del mercado

México es un país con un largo camino por delante en materia de ciberseguridad, ya que cuenta con una elevada tasa de ataques de cibercrimen y, sin embargo, las medidas e iniciativas tanto públicas como privadas, no son suficientes.

B.2.1. Grado de digitalización de la economía mexicana

En México, las Tecnologías de la Información y la Comunicación (TIC) se encuentran en una fase de **acelerada adopción,** aún lejos de llegar al nivel de desarrollo de los países de Europa Occidental o América del Norte, pero su crecimiento es rápido. Actualmente, México es el segundo país con mayor penetración digital de América Latina, detrás de Brasil.

El porcentaje de usuarios de Internet en el país en 2019 fue del **70,1 %**, mientras que en España es de un 90,7 %. Como se puede observar en el Gráfico 1, el incremento de internautas en 2019 fue de un 4,3 % respecto a 2018 y un 12,7 % respecto a 2015. La media de crecimiento anual de los últimos 5 años ha sido de un **5,1 %**.

El uso de **dispositivos móviles**, específicamente de teléfonos inteligentes o *smartphones*, ha sido decisivo para la penetración de Internet en el país. En el Gráfico 2 se observa cómo, en 2019, el 95,3 % de las personas que se conectaron a Internet lo hicieron a través de este medio, y sólo un 62,1 % con un ordenador portátil o de escritorio.

[1] Foro Económico Mundial (2020) *The Global Risks Report, 2020*. Disponible en: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

[2] *BOE* (2011) Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Disponible en: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

Los principales motivos de conexión en 2019 fueron **entretenimiento, obtener información** y **comunicación,** mientras que las actividades que menos realizaron los usuarios fueron operaciones bancarias en línea, la compra de productos e interactuar con el Gobierno[3].

GRÁFICO 1. USUARIOS INTERNET EN MÉXICO, 2015-2019
(en porcentaje sobre el total)

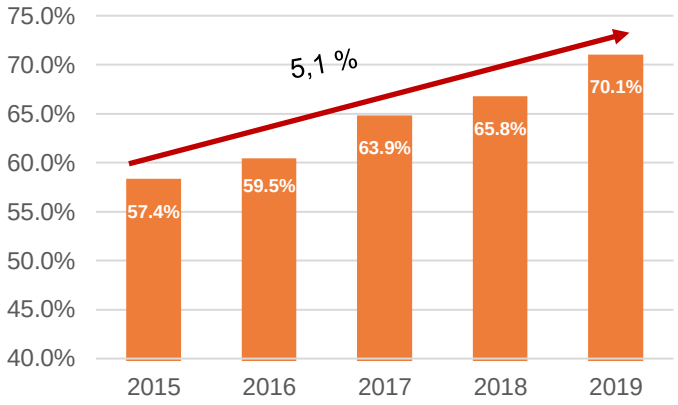
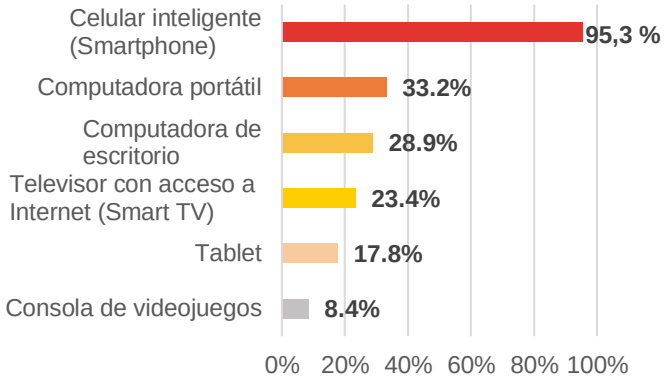


GRÁFICO 2. USUARIOS DE INTERNET SEGÚN DISPOSITIVOS DE CONEXIÓN, 2019
(en porcentaje)



Fuente: INEGI, 2020.

Es destacable la diferencia entre los usuarios de Internet en el entorno urbano y el rural: un 76,6 % de la población urbana mexicana es internauta y tan sólo un 47,7 % de la rural lo es.

Por último, el **comercio electrónico**, cuyo pilar fundamental es la seguridad en los pagos y la privacidad de los usuarios, ha experimentado un considerable desarrollo en los últimos años, creciendo un 28,6 % en 2019 respecto al año anterior, por encima de la media mundial, de un 20,7 %[4].

B.2.2. Ataques y coste del cibercrimen en México

Después de Brasil, México es el país que mayor número de ataques cibernéticos sufre en América Latina[5]. De acuerdo con un estudio de Willis Towers Watson, se estima que en **2018 el 83 % de las empresas mexicanas fueron víctima de algún tipo de ciberataque** al menos una vez en el año, con pérdidas en promedio de 1,5 millones de dólares, posicionando a México entre los 10 países con más ataques cibernéticos. Este mismo estudio afirma que tan sólo un 30 % de las empresas contaban con un plan de protección ese año[6].

El 56 % de las empresas mexicanas encuestadas por PWC en 2018, declararon haber sido víctimas de ataques por *malware* y *phishing* a lo largo del año. Además, un 27 % de los mexicanos fueron víctimas de un robo de identidad en medios digitales y un 21 % de fraudes financieros[7]. En los gráficos 3 y 4, se puede observar que el principal ataque en México en 2018 fue *malware* (35 %), seguido de *phishing* (21 %), y que los tipos de fraude más habituales fueron la disrupción del proceso de negocio (25 %) y la extorsión (19 %).

[3] Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares, ENDUTIH (2019). Realizada por el Instituto Nacional de Estadística y Geografía (INEGI), la Secretaría de Comunicaciones y Transportes (SCT) y el Instituto Federal de Telecomunicaciones (IFT). Disponible en: https://www.inegi.org.mx/programas/dutih/2019/
[4] Asociación Mexicana de Venta Online (2020). *Impacto del COVID-19 en Venta Online en México*: https://www.amvo.org.mx/estudios/reporte-1-impacto-covid-19-en-venta-online-mexico/
[5] CSIS, McAfee (2018). *Economic Impact of Cybercrime*: https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email
McKinsey & Company (2018) Perspectiva de Ciberseguridad en México: https://consejomexicano.org/multimedia/1528987628-817.pdf
PWC (2018) Global State of Information Security Survey
[6] Willis Towers Watson (2018). *Riesgo Cibernético México*: https://www.willistowerswatson.com/es-MX/Insights/2018/12/riesgo-cibernetico-mexico-2018
[7] Secretaría de Comunicaciones y Transporte (2019). *Hábitos de los usuarios en ciberseguridad en México*: https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf

GRÁFICO 3. TÉCNICAS MÁS USADAS EN CIBERATAQUES EN 2018

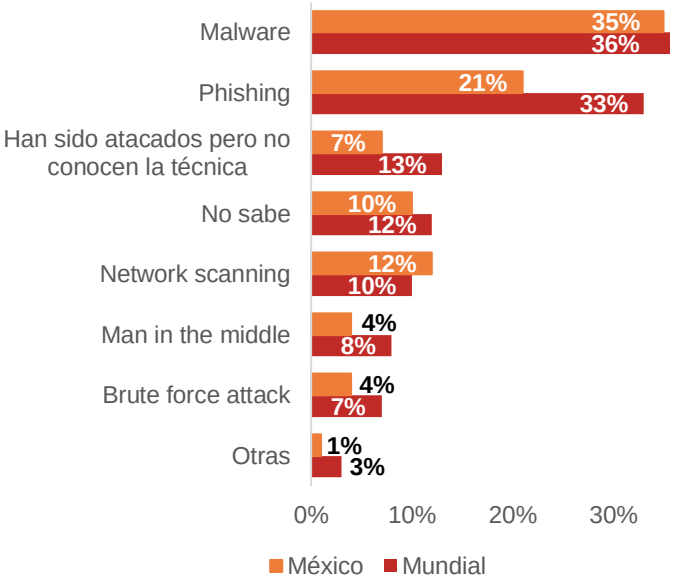


GRÁFICO 4. TIPO DE FRAUDE MÁS HABITUAL EN 2018

Fuente: PWC, Encuesta de Delitos Económicos, 2018.

Con la **crisis de la COVID-19** y la aceleración de la digitalización en 2020, el número de ataques ha aumentado considerablemente. Según el último informe del Banco de México, durante los meses de contingencia sanitaria, el número de ciberataques a empresas, instituciones gubernamentales y personas se ha incrementado en todo el mundo hasta un 400 %[8].

B.2.3. Inversión

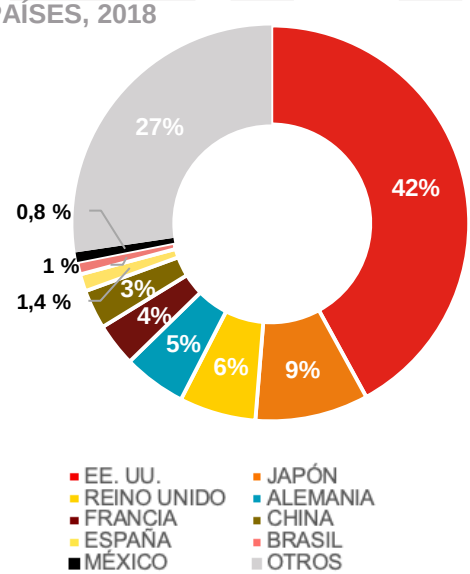
Según el estudio de Gartner de 2019, el **gasto mundial** en ciberseguridad en 2018 fue de 112.667,85 millones de dólares, un 11,15 % más que en 2017.

El gasto en Norteamérica y Europa Occidental representa el 70,72 %, mientras que América Latina sólo supone un 2,74 % del total. Como se puede observar en el Gráfico 6, el gasto de Estados Unidos es casi la mitad del gasto mundial, llegando al 42 %.

El **gasto de México** en 2018 fue de 895,49 millones de dólares, es decir, un 0,79 % del gasto mundial, creciendo un 7,95 % respecto a 2017. El país ocupa el puesto 18.º, siendo el segundo país por gasto de América Latina después de Brasil con un 1,02 %.

El **gasto de España** fue algo mayor, llegando a los 1.594,01 millones de dólares, es decir, un 1,41 % del gasto mundial. Esto supone un aumento del 15,78 % respecto a 2017, por encima de la media mundial, ocupando el puesto 14.º en el *ranking* por países[9].

GRÁFICO 6. REPARTO DEL GASTO MUNDIAL EN CIBERSEGURIDAD POR PAÍSES, 2018



Fuente: Gartner, 2019.

[8] Banco de México (2020). *Reporte de Estabilidad Financiera, Junio 2020*. Disponible en: https://www.banxico.org.mx/publicaciones-y-prensa/reportes-sobre-el-sistema-financiero/ %7BA66FA96C-EC89-D558-3342-F303E53042D5 %7D.pdf

[9] Gartner (2019). *Forecast: Information Security and Risk Management, Worldwide, 2017-2023, 4Q2019 Update*: https://www.gartner.com/en/documents/3978569/forecast-information-security-and-risk-management-worldw ;INCIBE (2020) *La Ciberseguridad en el mundo. Situación de España.*

TABLA 2. GASTO EN CIBERSEGURIDAD, 2018
(En millones USD)

	Mundial	España	México
	112.667,85	1.594,01	895,49
Porcentaje	100 %	1,41 %	0,79 %
Posición en *ranking* mundial	-	14.º	18.º
Crecimiento 2018 respecto a 2017	11,15 %	15,78 %	7,95 %

Fuente: Gartner, 2019.

En este mismo estudio se estima que las previsiones de crecimiento del gasto, teniendo en cuenta los efectos de la crisis de la COVID-19 entre 2020 y 2023, son de 4,83 % para México y 5,78 % para el mundo.

TABLA 3. PREVISIONES DE CRECIMIENTO DEL GASTO ANUAL EN CIBERSEGURIDAD, 2020-2023

México, en millones USD

	2019	2020	2021	2022	2023	CAGR 2020-2023
Gasto	944,82	975,81	1.023,62	1.077,36	1.140,82	**4,83 %**
Crecimiento anual	5,51 %	3,28 %	4,90 %	5,25 %	5,89 %	

Mundial, en millones USD

	2019	2020	2021	2022	2023	CAGR 2020-2023
Gasto	120.877,16	125.736,42	133.657,81	141.944,60	151.312,94	**5,78 %**
Crecimiento anual	7,28 %	4,02 %	6,30 %	6,20 %	6,60 %	

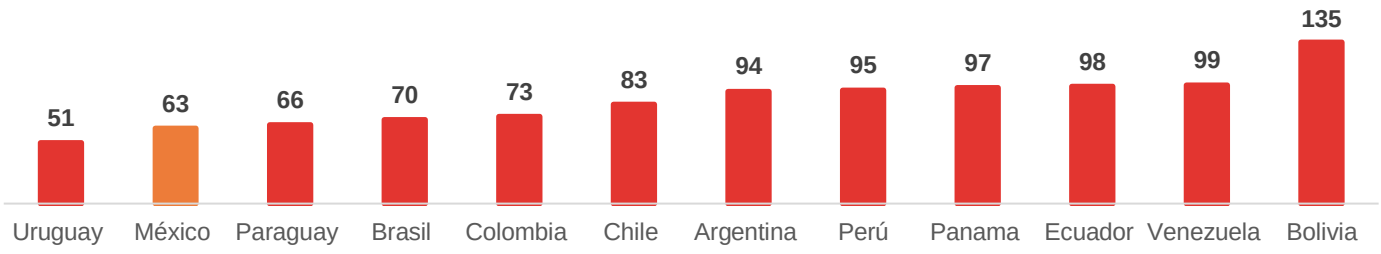
Fuente: elaboración propia con datos de Gartner, 2019.

En conclusión, se prevé que el mercado de la ciberseguridad siga experimentado un incremento continuo en los próximos años en México. A pesar del impacto negativo de la crisis económica de 2020, las perspectivas de crecimiento del sector siguen siendo muy optimistas. De hecho, las restricciones a la movilidad impuestas para combatir la COVID-19 estarían acelerando el tráfico de datos y, por tanto, aumentando la demanda de protección.

B.2.4. Índice de Ciberseguridad Global

El **Índice de Ciberseguridad Global** monitorea el compromiso con la ciberseguridad de los 194 Estados miembros de la Unión Internacional de Telecomunicaciones (UIT).

GRÁFICO 7. *RANKING* DE PAÍSES DE AMÉRICA LATINA EN EL ÍNDICE DE CIBERSEGURIDAD GLOBAL 2018



Fuente: Unión Internacional de Telecomunicaciones, 2019.

México ocupó el puesto **63.º** en 2018, siendo el segundo país de América Latina y el cuarto en la región de América, sólo por detrás de Estados Unidos, Canadá y Uruguay.

A nivel global, México ha pasado del puesto 72.º al 63.º en 5 años y en América Latina del puesto 10.º al 4.º, lo que refleja la progresiva mejora del país en este índice[10].

B.3. Principales actores

B.3.1. Actores públicos y asociaciones

Los principales organismos públicos en México en materia de Ciberseguridad son:

- **Secretaría de Seguridad Pública y Protección Ciudadana:** responsable de diseñar, planear, ejecutar y coordinar las políticas gubernamentales en materia de seguridad pública. De esta dependen:
  - **Dirección General Científica de la Guardia Nacional:** se ocupa, entre otros, de la prevención de delitos, incluyendo los delitos cibernéticos.
    Dentro de esta se encuentra el **Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX),** encargado de prevenir y mitigar las amenazas de seguridad informática.
  - **Centro Nacional de Inteligencia**: se encarga de obtener información y tomar decisiones relacionadas con el diseño y ejecución de la estrategia, políticas y acciones de Seguridad Nacional.
- **Consejo Nacional de Seguridad Pública**: presidido por el presidente de la República, se encarga de tomar decisiones en materia de seguridad pública, así como de desarrollar la política de seguridad, y aprobar los programas y subprogramas de prioridad nacional.

El Gobierno de México elaboró en 2017 la **Estrategia Nacional de Ciberseguridad**[11] con el objetivo de fortalecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político, y de definir objetivos estratégicos para los diferentes actores implicados.

No obstante, el país sigue teniendo por delante un largo camino en materia de regulación de ciberseguridad, ya que la legislación al respecto es escasa y uno de los problemas a los que se enfrenta el sistema es la limitada coordinación entre organismos públicos y privados. Hoy en día, no existen exigencias en cuanto a medidas de seguridad cibernética, ni las organizaciones están obligadas a informar sobre incidentes a las autoridades, lo que hace que la recolección de estadísticas sobre ciberataques sea muy difícil[12].

Algunas de las principales **asociaciones** en el sector son la Asociación Mexicana de Ciberseguridad (AMECI), la Asociación Latinoamericana de Seguridad (ALAS), la Asociación Mexicana de la Industria de Tecnologías de Información (AMITI) y la Asociación de Internet de México (AIMX).

En el país también existen varios **CERT** (Equipos de Respuesta ante Emergencias Informáticas), privados y públicos. Algunos de los públicos destacables son: el de la Universidad Nacional Autónoma de México (CERT UNAM), de la Policía Federal (CERT MX), de la Universidad Autónoma de Chihuahua (CERT UACH) o el del Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (CERT Infotec). Y entre los privados están: el de IQSec (IQSec CERT), Total Sec (CERTDSI Totalsec), Scitum (Scitum CERT) o Mnemo (Mnemo CERT).

B.3.2. Empresas

El mercado mexicano de ciberseguridad se encuentra altamente fragmentado. Las principales empresas son multinacionales de *hardware* y *software*, servicios de tecnología, consultoras y administradores de seguridad. Existe una elevada presencia de empresas extranjeras, principalmente estadounidenses.

- **Empresas extranjeras** con presencia en el mercado mexicano: Rockwell, Kaspersky, Paloalto Networks, Cisco Systems, Trend Micro, Belden Solutions, Broadcom, Attivo Networks, Primx,Trend Micro, Fortinet, Alestra, EY, IBM, Deloitte, KPMG, PWC o Thales.
- **Empresas mexicanas:** SCITUM (división de Telmex), Nordstern Technologies, Totalsec, IQSec, VdV Netwoks o CSI consultores.

[10] Unión Internacional de Telecomunicaciones (2019). *Global Cybersecurity Index, 2018.* Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
[11] Estrategia Nacional de Ciberseguridad (2017). Informe elaborado por el Gobierno. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
[12] Entrevista a Jorge Osorio, Consultor y Auditor en el área de Seguridad de la Información, fundador de CSI.

C. LA OFERTA ESPAÑOLA

Según el listado de empresas elaborado por Cybersecurity Ventures de las 500 mayores empresas del sector de la ciberseguridad mundial, los países que lideran la industria son Canadá, EE. UU., Reino Unido e Israel. En el listado figuran dos empresas españolas Panda Security (posición 315.ª) y Blueliv (posición 429.ª), ambas presentes en México[13].

La percepción del sector español de ciberseguridad en el país es buena. En cuanto colaboración interinstitucional, España es un país de referencia en este sector, gracias a la labor del Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI), y del Instituto Nacional de Ciberseguridad (INCIBE), que han desarrollado diversas actividades de formación y de consultoría en materia normativa con la administración mexicana.

Otras empresas españolas con presencia en México son Elevenpaths (división de ciberseguridad de Telefónica), Minsait (división de Indra), S21Sec, Electronic identification, Innotec System (grupo Entelgy), S2 GRUPO, Countercraft, Continuum Security, Mnemo, GMV, One Esecurity, Ondata Internacional Spamina, Everis, Enigmedia, Scati Labs, Ikusi, Prosegur, Innotech, OpenCloud o Buguroo[14].

D. OPORTUNIDADES DEL MERCADO

Existen dos principales factores generadores de oportunidades en el mercado mexicano:

- **Aceleración de la digitalización y aumento del cibercrimen:** a medida que las empresas y organismos sufren más ataques, la demanda de herramientas y soluciones de ciberseguridad aumenta.
- **Nuevas regulaciones:** el cumplimiento regulatorio es un factor decisorio clave para implantar soluciones de ciberseguridad. Se prevé que el marco regulatorio en todas las regiones se actualice y se incrementen los requisitos y exigencias.

  México tiene pendiente la publicación de normativa referente a la protección de **infraestructuras críticas** que debería aprobarse en los próximos años**,** pues ya estaba en proceso, pero se ha detenido hace unos meses**.** Muchos países, entre los que está España, ya cuentan con normativa al respecto, lo que ha conllevado un considerable aumento de la demanda de servicios de ciberseguridad por parte de las empresas de los sectores afectados. Existen presiones de los dos grandes socios económicos de México (EE. UU. y Canadá) para que se apruebe esta ley, ya que México es proveedor de muchos componentes para estos dos países, y para ser un proveedor de confianza se necesita una buena ciberseguridad.

  Se prevé por tanto que se multiplique la demanda de servicios de ciberseguridad en México desde el momento en que se apruebe normativa en este campo, tanto de consultoría como de proveedores de soluciones de *hardware* y *software*. Esto constituirá una oportunidad interesante para empresas españolas que tienen 12 años de experiencia en la aplicación práctica de este tipo de leyes[15].

Además, con la crisis generada por la COVID-19 han surgido nuevos **nichos** específicos de demanda de servicios de ciberseguridad en:

- **Sanidad:** protección para dispositivos médicos, información confidencial, etc.
- **Educación:** con la llegada masiva de la teleformación.
- **Teletrabajo:** con el aumento de las diferentes herramientas necesarias (plataformas de videoconferencias, servicios en la nube, etc.).
- **Comercio electrónico:** donde son fundamentales aspectos como la seguridad en el pago, lucha contra el fraude, etc.

Otros **sectores** de especial interés son:

- **Administraciones públicas:** debido a una mayor vulnerabilidad y un aumento de los ciberataques.

[13] Cybersecurity Ventures (2018). *Cybersecurity 500 List, 2018 Edition.* Disponible en: https://cybersecurityventures.com/cybersecurity-500-list/
[14] INCIBE (2020). *La Ciberseguridad en el mundo*. Situación de España.
[15] Entrevista a Félix Antonio Barrio Juárez, Director del *Hub* de Ciberseguridad en el Tecnológico de Monterrey.

- **Sectores relacionados con infraestructuras críticas o estratégicas:** como se mencionó anteriormente, sectores como el energético, telecomunicaciones, agua, etc.
- **Sector financiero:** uno de los sectores que más ataques ha sufrido en los últimos años.
- **Industrias con infraestructura física:** actualmente, la ciberseguridad no sólo es TIC, sino que muchos de los vectores de ataque llegan a través de tecnología operativa, por lo que los proveedores de infraestructuras físicas tienen que contar con protección de ciberseguridad en sectores como automoción, energético, etc.[16].

Según el último informe de INCIBE, los **tipos de soluciones de ciberseguridad** en los que más se invirtió en México en 2018 fueron: servicios de seguridad (47,36 %), protección de infraestructuras (17,52 %) y equipamiento de seguridad de red (13,23 %), gestiones de acceso de identidad (8,86 %) y *software* de seguridad para el consumidor (5,06 %)[17]. Las empresas de servicios de **"seguridad híbrida"**, es decir, que además de los servicios tradicionales de seguridad física incluyen en su cartera servicios de ciberseguridad, están cobrando un papel importante.

Por otro lado, el **T-MEC,** tratado entre México, Canadá y EE. UU. que entró en vigor el 1 de julio, trae nuevas oportunidades, como una mayor seguridad de la información, o la incorporación de "medidas tecnológicas efectivas" para empresas de *software*.

Por último, una ventaja que no han de olvidar las empresas españolas es el **factor idioma**, ya que muchas empresas de menor tamaño prefieren tratar con un proveedor en su mismo idioma.

E. CLAVES DE ACCESO AL MERCADO

E.1. Distribución

La cadena de distribución de ciberseguridad comprende tres tipos de actores en general[18]:

- **Fabricantes:** de *hardware*, desarrolladores de *software* y mixtos.
- **Distribuidores:**
  - Mayoristas: compran y venden productos a consultoras, integradores o proveedores de servicios.
  - Distribuidores: venden directamente a empresas de ciberseguridad o a cliente final.
  - Minoristas: puntos de venta físicos, grandes superficies y pequeñas consultoras, centradas en la venta de productos y servicios de ciberseguridad a pymes y particulares.
- **Prestadores de servicios:** proveedores locales de servicios especializados, revendedores de valor añadido (VAR), consultoras tecnológicas (EY, KPMG, Deloitte, PWC), integradores y proveedores de servicios gestionados de seguridad (MSSP).

En el mercado mexicano es recomendable buscar alianzas con socios **colaboradores TIC** locales que cuentan con estructuras de distribución y clientes. Se recomienda por lo tanto la entrada a través de un distribuidor, colaborar mediante transferencia de tecnología o alianzas estratégicas con líderes en el mercado[19].

Se recomienda a las empresas españolas registrar **la marca en México**, así como los **derechos de autor** para *software* propio. Pueden encontrar los requisitos y procedimientos en el Instituto Mexicano de Propiedad Industrial.

E.2. Barreras reglamentarias y no reglamentarias

Algunos de los factores que pueden suponer una barrera de entrada al país son:

- **La brecha digital:** como se ha mencionado anteriormente, el grado de digitalización varia enormemente entre las áreas rurales y urbanas, además de las considerables diferencias entre pymes y grandes empresas.

[16] Entrevista a Félix Antonio Barrio Juárez, director del *Hub* de Ciberseguridad en el Tecnológico de Monterrey.
[17] INCIBE (2020) *La Ciberseguridad en el mundo*. Situación de España.
[18] ONTSI - INCIBE (2015). *Caracterización del subsector y el mercado de la ciberseguridad*. Disponible en: https://www.ontsi.red.es/sites/ontsi/files/caracterizacion_del_subsector_y_el_mercado_de_la_ciberseguridad.pdf.
[19] Entrevista a Félix Antonio Barrio Juárez, director del *Hub* de Ciberseguridad en el Tecnológico de Monterrey.

- **Menor concienciación:** Las ciberamenazas son percibidas de manera diferente en cada región o industria. Por ejemplo, en Estados Unidos y Canadá, representan la mayor preocupación entre los CEO, de acuerdo con el informe de PwC *21th CEO Survey*. En Europa Occidental y Asia Pacífico se colocan en cuarto lugar, mientras que en América Latina no aparecen entre las 10 primeras amenazas, a pesar de ser regiones que reciben un número considerable de ataques[20].

E.3 Ferias

INFOSECURITY MÉXICO

Punto de encuentro anual de los profesionales de la ciberseguridad y tecnologías de la información más importante en México. En 2019 contó con más de 2.000 asistentes, 80 expositores y múltiples salas educativas para discutir tendencias en ciberseguridad https://www.infosecuritymexico.com/es.html
Última edición (virtual): 22-24 de septiembre de 2020

EXPO SEGURIDAD MÉXICO

La mayor exhibición anual del sector de la seguridad en América Latina. Reúne fabricantes, distribuidores, integradores y usuarios nacionales e internacionales para tratar sobre tecnología, soluciones y conocimiento del sector. https://www.exposeguridadmexico.com/es-mx.html
Próxima edición: 13-15 de abril de 2021, Ciudad de México

XIV CONGRESO INTERNACIONAL DE CIBERSEGURIDAD INDUSTRIAL EN LATINOAMÉRICA

Evento organizado anualmente por el Centro de Ciberseguridad Industrial (CCI) que se celebra en 2020 en México, como punto de referencia para el mercado hispanoamericano. Los diferentes actores del sector compartirán conocimiento y experiencias sobre la actualidad de la ciberseguridad.
https://www.cci-es.org/web/cci/detalle-congreso/-/journal_content/56/10694/1000826
Próxima edición (virtual): 27-29 de octubre de 2020.

ESHOW MÉXICO

Uno de los principales puntos de encuentro de carácter anual para el conjunto de profesionales del mundo *online* en América Latina, en el que los profesionales del sector crean sinergias, comparten conocimientos y presentan las estrategias y soluciones innovadoras. https://www.the-eshow.mx
Próxima edición: 2021, Ciudad de México.

IT SOLUTIONS DAY

Aborda temas como seguridad y desempeño, centros de datos, la nube e inteligencia artificial. Este evento cuenta con más de 1,000 asistentes, 40 stands de fabricantes, 4 foros, más de 30 conferencias, y la presencia de 800 empresas. https://www.itsolutionsday.mx/
Última edición (virtual): 2-3 de septiembre de 2020, Ciudad de México.

F. INFORMACIÓN ADICIONAL

- CANIETI - Cámara Nacional de la Industria Electrónica de Telecomunicaciones y de Tecnologías de la Información
- CIMECS - Consejo Mexicano de Ciberseguridad
- CSOFTMTY - Clúster de Tecnologías de la Información y Comunicaciones en Nuevo León
- Publicaciones y revistas: Revista Más Seguridad, Forbes México, Segurilatam, ITU Cybersecurity Activities, Usecim.net, Mundoti.net

[20] PWC (2018). *Global State of Information Security Survey*.

CONTACTO

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

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

Av. Pdte. Masaryk 473,
Polanco II Secc, Miguel Hidalgo
Ciudad de México 11550 – México
Teléfono: +55 9138 6040
Email: mexico@comercio.mineco.es
http://mexico.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

INFORMACIÓN LEGAL: Este documento tiene carácter exclusivamente informativo y su contenido no podrá ser invocado en apoyo de ninguna reclamación o recurso.

ICEX España Exportación e Inversiones no asume la responsabilidad de la información, opinión o acción basada en dicho contenido, con independencia de que haya realizado todos los esfuerzos posibles para asegurar la exactitud de la información que contienen sus páginas.

AUTORA
Yanilda Lucie Reynaud

Oficina Económica y Comercial
de España en México
Buzón oficial de la Oficina: mexico@comercio.mineco.es
Fecha: 05/10/2020

NIPO: 114-20-022-X