

Ciberseguridad en México

A. CIFRAS CLAVE

Los efectos de la digitalización en la sociedad mexicana, la permanencia del trabajo remoto y la irrupción de la inteligencia artificial han enfatizado la necesidad de contar con una estrategia nacional de ciberseguridad y la importancia de este sector en la sociedad, tanto en el ámbito empresarial como en el individual.

Más de tres cuartas partes de los mexicanos son usuarios de Internet y/o teléfono celular, registrando estos grupos en los últimos años aumentos de 11,9 % y 6,2 %, respectivamente.

Los órganos legislativos están llevando a cabo discusiones para definir el contenido de una Ley Federal de Ciberseguridad que ayude a prevenir delitos cibernéticos. Este es un paso necesario para que México se sitúe al nivel de protección legislativa de otras economías desarrolladas.

TABLA I. EL MERCADO MEXICANO DE CIBERSEGURIDAD

	2020	2021	2022	2023 ³	2024 ³
Gasto total en productos y servicios de la información¹ (a)	1.005	1.155	1.305	1.439	1.538
Crecimiento interanual del gasto total	-	14,7 %	12,9 %	10,3 %	6,8 %
Penetración de Internet (b)	71,5 %	75,6 %	78,6 %	-	-
Ingresos por soluciones de ciberseguridad¹ (c)	514,7	654,7	736,6	839,8	952,6
Coste estimado del cibercrimen¹ (c)	24.970	31.630	41.290	55.290	75.600
Ingresos por servicios relacionados con la seguridad¹ (c)	996,9	1.170	1.258	1.317	1.369
Gasto por empleado en ciberseguridad² (c)	26,06	31,01	33,42	35,66	37,89

¹ En MUSD; ² En USD; ³ Previsión.

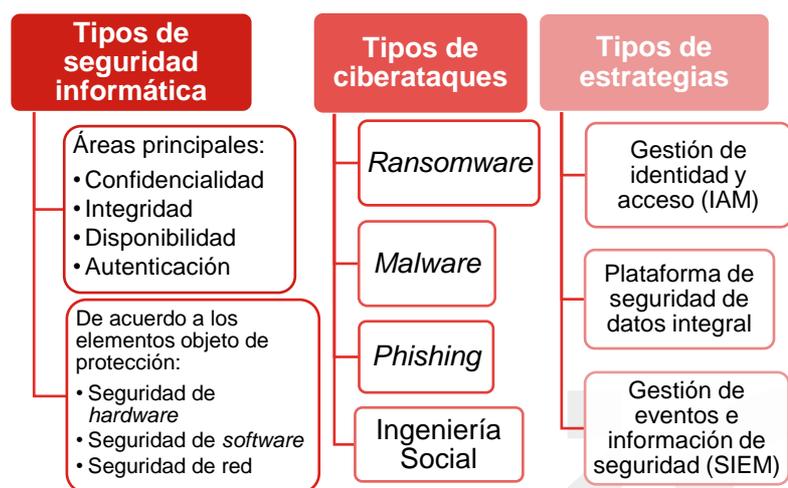
Fuente: (a) Gartner, (b) INEGI: Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH), (c) Statista.

B. CARACTERÍSTICAS DEL MERCADO

B.1. Definición precisa del sector

La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. En general, los ciberataques apuntan a acceder, modificar o destruir información confidencial; a extorsionar a los usuarios o interrumpir la continuidad del negocio¹.

GRÁFICO I. CIBERSEGURIDAD: TIPOS DE SEGURIDAD INFORMÁTICA, CIBERATAQUES Y ESTRATEGIAS



También conocida como seguridad de la tecnología de la información (TI), las medidas de ciberseguridad o seguridad cibernética están diseñadas para combatir amenazas contra sistemas en red y aplicaciones, originadas dentro o fuera de una organización. La ciberseguridad, por tanto, engloba la seguridad informática, los ciberataques a los que tiene que hacer frente, y las estrategias para llevar a cabo una solución frente a las amenazas.

Fuente: IBM, Cisco, InfoSecurity.

La [Corporación Internacional de Datos – IDC](#) notificó el registro de más de 80.000 millones de intentos de ciberataques en México en la primera mitad de 2022, lo que le convierte en el tercer país atacado a nivel mundial, y el primero de Latinoamérica. El impacto estimado de los ciberataques en México es de:

- 98 MUSD, coste medio de un ciberataque efectivo a las empresas.
- 39 segundos, promedio de tiempo en que se da un nuevo ataque en México.
- 3 horas en promedio, tiempo de exposición a riesgos de los mexicanos en Internet.

Según el Índice de Ciberseguridad Global elaborado por la [Unión Internacional de Telecomunicaciones \(UIT\)](#)², que monitorea el compromiso con la ciberseguridad de sus 194 Estados miembros, de 2018 a 2020, México pasó de la posición 63.^a a la 52.^a, siendo el cuarto país mejor ubicado de América, por detrás de Estados Unidos, Canadá y Brasil. México destacó en medidas técnicas y medidas de cooperación, y como áreas de potencial crecimiento, el organismo menciona las medidas regulatorias, que alcanzan la calificación más baja.

B.2. Tamaño del mercado

B.2.1. Mercado internacional

El último informe sectorial publicado por la consultora [DBK Informa](#) indica que el gasto mundial en productos y servicios de seguridad de la información creció un 67 % entre 2017 y 2022, y se prevé que el promedio anual de crecimiento será del 11,5 % para el período 2022-2026, alcanzando 261.900 MUSD en 2026.

Los servicios de seguridad, que incluyen consultoría, soporte de *hardware*, implementación y servicios subcontratados, concentraron en 2022 el 42,4 % del gasto en ciberseguridad. Les siguen la protección de

¹ Anatomía de un ataque. (10 de febrero de 2023). [Video]. Cisco. https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

² International Telecommunication Union (ITU). (2023). Global Cybersecurity Index 2020 (4^a. ed.): [Global Cybersecurity Index 2020 \(itu.int\)](#)

infraestructuras (16,2 %), equipos de seguridad de la red (11,3 %), y la administración de accesos e identidades (10,7 %). El resto, se repartió entre *software* de seguridad de consumo, gestión integrada de riesgos, seguridad de aplicaciones, seguridad de datos, seguridad en la nube, y otro *software* de seguridad de la información.

El daño económico por ataques de *ransomware* se estima que llegará a los 42.000 MUSD en 2026, con un crecimiento de más del doble desde 2021, cuando se registraron daños por valor de 20.000 MUSD. El informe de [Economist Intelligence Unit](#), menciona que la penetración de Internet alcanzará niveles cercanos al 90 % en 2026. Por otro lado, el gasto en TI en América Latina, incluyendo *hardware*, *software* y servicios, se prevé que aumente de 97.400 a 119.900 MUSD.

B.2.2. Mercado mexicano

Según datos de [Statista](#)³ y [Gartner](#)⁴, los ingresos del sector de la ciberseguridad en México alcanzarán 2.160 MUSD en 2023. El mayor subsector dentro del mercado es el de los servicios de seguridad, con una proyección de 1.320 MUSD para 2023. Se espera que los ingresos por ciberseguridad en México crezcan a una tasa anual compuesta (CAGR, por sus siglas en inglés) del 8,11 % hasta 2028, lo que representaría 3.190 MUSD ese año.

El gasto total en México ascendió a 1.155,9 y 1.305 MUSD en los años 2021 y 2022, respectivamente. En 2023, se espera que ese gasto crezca hasta los 1.439,8 MUSD, con una tasa de crecimiento anual del 8 % hasta 2027. En la Tabla II, se puede observar el desglose del gasto por usuario final en diferentes áreas.

TABLA II. GASTO POR USUARIO FINAL EN SEGURIDAD DE LA INFORMACIÓN EN MÉXICO (MUSD)

Gasto por segmentos	2021	2022	2023 ^P	2024 ^P
Servicios de seguridad	447,4	467,1	480,9	484,4
Protección de infraestructuras	185,3	216,1	244,0	265,6
Administración de accesos e identidades	142,2	163,1	180,5	191,8
Equipos de seguridad de la red	135,6	152,3	170,8	185,2
Software de seguridad de consumo	117,7	147,4	167,4	178,9
Seguridad de aplicaciones	31,2	42,4	53,2	63,9
Seguridad en la nube	34,1	41,0	51,6	62,7
Gestión integrada de riesgos	26,7	37,2	49,9	62,5
Seguridad de datos	21,6	22,9	24,0	24,4
Otro <i>software</i> de seguridad de la información	9,4	10,2	11,5	12,2
Privacidad de datos	4,8	5,4	5,9	6,7
Total	1.155,9	1.305,0	1.439,8	1.538,3

Fuente: Elaboración propia con datos de Gartner.

En cuanto a los subsectores de mayor gasto en México en 2022, en primer lugar, están los servicios de seguridad (36 %), seguidos por la protección de infraestructuras (17 %), la administración de accesos e identidades (12 %) y los equipos de seguridad de la red (12 %).

Por lo que hace al coste del cibercrimen en el territorio mexicano, en 2022 llegó a ser de 41.290 MUSD. En 2023, se espera que alcance los 55.290 millones, y en 2028 aumentaría hasta los 303.000 millones de dólares.

³ Statista. (s. f.). *Cybersecurity - Mexico | Statista Market Forecast*. <https://www.statista.com/outlook/tmo/cybersecurity/mexico>

⁴ *IT Key Metrics Data 2023: Overview*. (s. f.). Gartner. <https://www.gartner.com/en/documents/4021797>

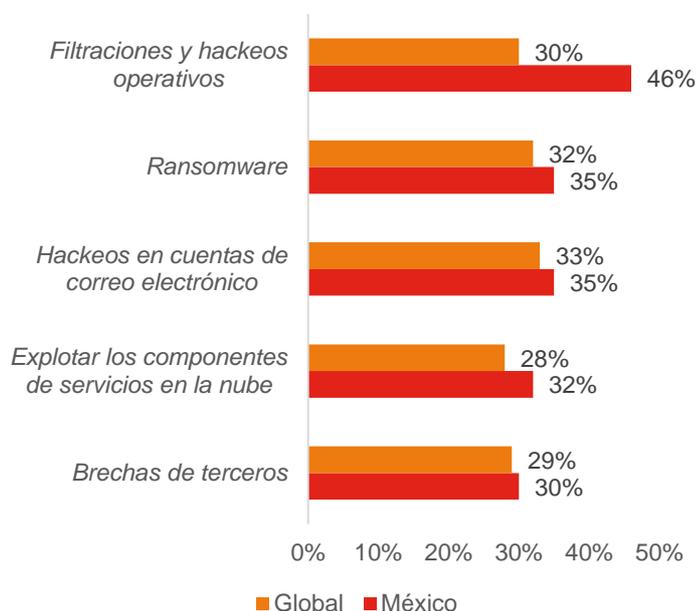
En términos comparativos, Estados Unidos presenta el mayor nivel de ingresos del mundo, y México se encuentra en niveles inferiores a los de España, pero cercanos a estos.

TABLA III. INGRESOS TOTALES DE CIBERSEGURIDAD (MUSD)

Comparativa de ingresos totales	2021	2022	2023 ^P	2024 ^P
México	1.825	1.995	2.157	2.321
España	2.292	2.311	2.475	2.741
Estados Unidos de América	57.480	62.700	68.680	74.190

Fuente: Elaboración propia con datos de Statista.

GRÁFICO II. VALORACIÓN DEL CRECIMIENTO DE ATAQUES A EMPRESAS EN 2023



Según el estudio publicado por la consultora [PWC⁵](#), en el que entrevistó a 147 ejecutivos mexicanos, los ciberataques que más preocupan a las empresas mexicanas son las filtraciones y los *hackeos* operativos.

En el Gráfico II, se puede observar cómo se espera que aumenten los ataques cibernéticos en 2023 respecto a 2022.

Cabe también mencionar que para el 67 % y 65 % de las organizaciones en México y el mundo, respectivamente, los cibercriminales son los agentes que encabezan la lista de amenazas, seguidos por los actores internos (52 % en México y 44 % global) y *hackers/hacktivistas* (50 % en México y 48 % global).

Fuente: *Digital Trust Insights 2023*, edición México, PwC.

B.3. Principales actores

La economía y ubicación geoestratégica de México son un objetivo atractivo para las actividades cibernéticas ilícitas. Por un lado, disfruta de una inversión extranjera directa importante y una evolución positiva del PIB y, por otro, sigue siendo relativamente vulnerable en ciberseguridad y ciberdefensa.

B.3.1. Organismos públicos

En México existen diferentes organismos con competencias en materia de ciberseguridad:

- **Secretaría de Seguridad Pública y Protección Ciudadana:** responsable de diseñar, planear, ejecutar y coordinar las políticas gubernamentales en materia de seguridad pública. De esta depende:
 - **Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional (CERT-MX):** “brinda servicios de apoyo en la respuesta a incidentes cibernéticos que afectan a las instituciones en el país que cuentan con infraestructura crítica de información”.

⁵ PricewaterhouseCoopers. (s. f.). *Digital Trust Insights 2023*. PwC. <https://www.pwc.com/mx/es/ciberseguridad/digital-trust.html>

Aseguran que las instituciones gubernamentales cumplan con el *Manual Administrativo de Aplicación General de Tecnologías de Información y Comunicaciones y de Seguridad de la Información* (MAAGTICSI), manual desarrollado en base a normas internacionales como la ISO 27001.

- **Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI):** Encargado de garantizar el acceso a la información pública y la protección de datos personales.
- **Secretaría de Marina – Armada de México:** El Acuerdo Secretarial 335/2022 del 1 de junio de 2022 dispuso que la Unidad de Ciberseguridad (UNICIBER) se constituyera en la Coordinadora General del Ciberespacio (EMCOGCIBER), dependiendo operativa, orgánica y administrativamente del Estado Mayor General de la Armada. Se encarga de proteger el ciberespacio, y cuenta con una *Estrategia Institucional para el Ciberespacio (2021-2024)*⁶.
- **Banco de México (BANXICO):** La principal institución financiera de México cuenta con una estrategia de protección frente a ciberataques que se puede consultar en su web: <https://www.banxico.org.mx/sistema-financiero/seguridad-informacion-banco.html>

B.3.2. Organismos privados, asociaciones y centros de investigación

El mercado de la ciberseguridad es global. En México, muchas de las empresas que operan en el mercado provienen de Estados Unidos, una de las economías más avanzadas en este sector. Empresas globales de ciberseguridad, como [Cisco México](#) (EE. UU.), [Fortinet](#) (EE. UU.), [IBM](#) (EE. UU.), [Palo Alto Networks](#) (EE. UU.), [Trellix](#) (antiguas McAfee + Fire Eye) (EE. UU.) o [ATOS](#) (Francia) también tienen aquí una considerable cuota del mercado. Sin embargo, cada vez más, otros actores irrumpen en el mercado, ya que existen oportunidades.

Las empresas mexicanas más importantes del sector en México son: [SCITUM](#) (división de Telmex), [2 Secure](#), [CERO UNO](#), [Grupo Scanda](#), [Totalsec](#) (Grupo Salinas), [NETRIX](#), [IQSEC](#), [Delta Protect](#), [KIO Networks](#) o [ProtektNet](#).

Algunas de las asociaciones relevantes en el sector son:

- **Asociación Mexicana de Ciberseguridad (AMECI):** Organización que ofrece consultoría, capacitación, servicios y soluciones relacionadas con la seguridad de la información.
- **Asociación Mexicana de la Industria de las Tecnologías de la Información (AMITI):** representa a las empresas de tecnología de México, para impulsar la interacción dentro de la industria y facilitar la conexión entre la administración pública, la academia y con organismos empresariales nacionales e internacionales.
- **Asociación de Internet de México (AIMX):** Provee información sobre distintas temáticas del mundo digital. Actúa como marco de referencia en temas claves para el desarrollo e implementación de proyectos normativos y de política pública que coadyuvan en la productividad y la competitividad de México.

México cuenta también con algunos de los centros de investigación del sector más importantes de Latinoamérica:

- **Centro de Investigación en Computación del Instituto Politécnico Nacional.**
- Coordinación de seguridad de la información (CSI) de la Universidad Nacional Autónoma de México / [UNAM-CERT](#).
- CIIC MÉXICO – **Clúster TIC de Nuevo León (csoftmty):** subcomité del Clúster TIC de Monterrey donde se educa e investiga sobre el conocimiento integral acerca de la protección de la información.

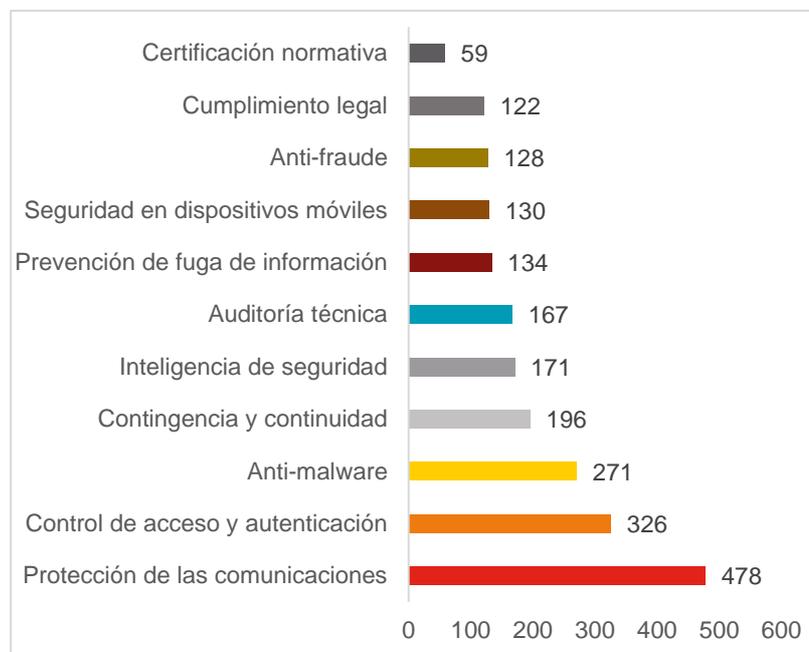
C. LA OFERTA ESPAÑOLA

El sector de la ciberseguridad crece en número de empresas en España, de nueva creación o por la diversificación de actividades desde otros sectores. Según datos del [Instituto Nacional de Ciberseguridad](#) (INCIBE), en enero de 2023 se contabilizaban en España 1.854 agentes dedicados a la comercialización de productos y prestación de servicios de ciberseguridad, 330 más que en mayo de 2022.

⁶ De Marina, S. (s. f.). *Estrategia Institucional de Ciberespacio*: [Estrategia Institucional de Ciberespacio | Secretaría de Marina | Gobierno | gob.mx](#)

Algunas de las empresas españolas presentes en el mercado mexicano son: [TelefonicaTech](#), [Minsait](#) (Grupo Indra), [Ayesa](#), [S21Sec](#), [s2 grupo](#), [Innotec Security](#) (Grupo Entelgy), [Mnemo](#), [OpenCloudFactory](#), [One Esecurity](#), [Ondata Mex](#), [Encora](#), [Grupo Antea](#), [Irium](#), [Konfido](#), [Ikusi](#) (Grupo Velatia), [Veridas Hornet Security](#), [Gestact](#) o [CS2](#).

GRÁFICO III. NÚMERO DE EMPRESAS EN ESPAÑA POR SOLUCIÓN (ENERO DE 2023)



Según un informe de [DBK](#), los productos con mayor penetración son los relacionados con la protección de las comunicaciones (26 % de las empresas los ofrecen), el control de acceso y la autenticación (18 %), y el *antimalware* (15 %).

En cuanto a los servicios, la mayor penetración está en el área de cumplimiento legal (57 %), la auditoría técnica (54 %), la implantación de soluciones (54 %) y el soporte y mantenimiento (42 %).

En México, la percepción del producto español es buena. Gracias a la labor de las empresas implantadas en el país, y la colaboración interinstitucional promovida desde España con [INCIBE](#) a través de sus actividades de formación y promoción de la ciberseguridad, se consigue que el país se posiciona como referente en el sector en México.

Fuente: DBK, INCIBE.

D. OPORTUNIDADES DEL MERCADO

En México abunda el talento y el capital humano. Sin embargo, en el sector de la ciberseguridad existen carencias de personal cualificado que haga frente a la creciente necesidad de protección frente a las amenazas. No obstante, existen oportunidades en el mercado; el idioma o los precios más competitivos que los de EE. UU., hacen atractiva la propuesta española en el país. Por otro lado, la fiabilidad y trayectoria de España y la Unión Europea en la protección del ciberespacio, en términos de calidad-precio-conocimiento, ayudan al buen posicionamiento del sector español en el país.

Los sectores de especial interés de demanda de servicios de ciberseguridad en México son:

- **Sector financiero:** Dada la sensibilidad de la información, es un objetivo primario a la hora de recibir ataques.
- **Administración Pública:** El Gobierno gestiona gran parte de las infraestructuras críticas del país (agua, energía, transporte), lo que le hace propenso a los ataques.
- **Sanidad:** Como el sector financiero, el sanitario maneja información muy sensible de sus usuarios.
- **Sector minorista:** El *e-commerce* abre la puerta a que los comercios reciban más ataques a medida que se digitalizan los negocios.
- **Sector industrial:** Uno de los de mayor tamaño en la economía mexicana, lo que aumenta su exposición a ser atacado, a medida que se implanta más tecnología en la producción.

Dos factores principales potenciarán las oportunidades en el mercado mexicano:

- **Inteligencia Artificial Generativa:** La IA puede detectar y prevenir potenciales amenazas, desarrollando modelos predictivos de ciberataques. Por otro lado, la IA también puede utilizarse para cometer delitos cibernéticos con mayor precisión y sofisticación, lo que incrementa el riesgo en la red. A pesar de todo, existen oportunidades ya que, en un futuro cercano, va a permitirse que las *compañías replanteen sus procesos administrativos y productivos*, lo que implicará un aumento de la inversión en ciberseguridad en tanto aumente

el uso de la IA entre los empleados de la empresa. Según información de *El Economista*⁷, el 55 % de usuarios de Internet en México cree que la IA es una herramienta útil, mientras el 22 % está preocupado por el ascenso en popularidad de la IA.

- **Papel del CISO:** El papel del CISO (*Chief Information Security Officer*)⁸ será fundamental en los próximos años, al invertir las empresas en seguridad de la información. En México, estos profesionales, aunque escasos, se enfrentan a presupuestos reducidos por la falta de conciencia en las organizaciones sobre las amenazas cibernéticas. En España, existe una creciente preocupación de estos profesionales ante ataques en sus empresas, especialmente por el auge del teletrabajo. En cambio, en México todavía falta que llegue esa inversión y concienciación en protección, por lo que, en este aspecto, se podría considerar una oportunidad conseguir *concienciar a las empresas mexicanas de la importancia que tiene una buena estrategia de ciberseguridad*.

E. CLAVES DE ACCESO AL MERCADO

E.1. Distribución

La cadena de distribución de la ciberseguridad comprende tres tipos de agentes en general: fabricantes, distribuidores y prestadores de servicios, que ofertan *hardware*, *software*, o servicios especializados.

A pesar de que los servicios de ciberseguridad se pueden prestar de forma remota, en México es importante estar presente físicamente de alguna forma, hecho que en este mercado se valora mucho, y genera imagen de marca. Se recomienda la creación de una filial que dé soporte técnico y atención al cliente o establecer alianzas estratégicas con socios locales con capacidad de venta y distribución de productos /servicios, con conocimiento del mercado.

También es recomendable registrar la marca y/ derechos de autor del *software* propio en México a través del [Instituto Mexicano de Propiedad Industrial – IMPI](#). En el siguiente enlace, se puede consultar un informe sobre [Propiedad Industrial en México 2023](#) elaborado por esta Oficina Económica y Comercial de España en México.

E.2. Legislación aplicable y otros requisitos

México no cuenta con legislación en materia de ciberseguridad; aunque desde 2018 se han propuesto 11 iniciativas de leyes sobre ciberseguridad, ninguna ha llegado a concretarse⁹. Se esperaba que una Ley Federal de Ciberseguridad se aprobase en diciembre de 2022, sin embargo, hasta la fecha, no se ha publicado en el *Diario Oficial de la Federación*. Esta última propuesta de Ley tiene 11 títulos y 71 artículos, en cuatro ejes¹⁰:

- Garantizar la seguridad nacional mediante la defensa del espacio digital.
- Crear un marco legal que permita sancionar o tipificar los ciberataques.
- Realización de pruebas de penetración o *pentesting* anualmente a las instituciones públicas y privadas.
- Crear una Agencia Nacional de Ciberseguridad controlada por el Ejecutivo, tomando como modelo las de la UE, Estados Unidos o Brasil.

El Gobierno federal anunció la creación de la [Comisión Intersecretarial de Tecnologías de Información y Comunicación \(TIC\), y de la Seguridad de la Información](#) (CITICSI) para sustituir la Comisión para el Desarrollo del Gobierno Electrónico creada en 2005, cuya finalidad es coordinar e implementar las políticas federales en materia de TIC y de seguridad de la información, impulsando actividades y estrategias para su aprovechamiento. Previsiblemente sus decisiones impactarán en el contenido de la nueva ley de ciberseguridad.

E.3. Ferias

- [InfoSecurity México](#). Próxima edición: 4 y 5 de octubre de 2023. Centro Citibanamex, CDMX
- [Expo Seguridad México](#). Próxima edición: 16 -18 de abril de 2024. Centro Citibanamex, CDMX

⁷ *El Economista*. (2023, 26 mayo): [55 % de usuarios de internet en México cree que la inteligencia artificial es una herramienta útil](#)

⁸ INCIBE (2023, 20 junio): <https://www.incibe.es/empresas/blog/roles-en-ciberseguridad-desde-el-ceo-los-usuarios-finales>

⁹ *Expansión*. (2023, 25 abril): [Iniciativa de Ley de Ciberseguridad es ingresada a la Cámara de Diputados \(expansion.mx\)](#)

¹⁰ Rivera, S. F. (2023). *Ley de Ciberseguridad en México: Conoce la Nueva Ley*: <https://www.deltaprotect.com/blog/ley-de-ciberseguridad-mexico>

F. 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:

Oficina Económica y Comercial de España en México

Avenida Presidente Masaryk 473,

Polanco, C.P. 11530

CIUDAD DE MÉXICO – MÉXICO

Teléfono: +52 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) [913 497 100](tel:+34913497100) (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.

AUTOR

Daniel Flores Bravo

Oficina Económica y Comercial
de España en Ciudad de México

mexico@comercio.mineco.es

Fecha: 30/06/2023

NIPO: 114-23-013-7

www.icex.es



FICHAS SECTOR MÉXICO



ICEX España
Exportación
e Inversiones