ICEX España Exportación e Inversiones

FS FICHA SECTOR

ALEMANIA

Ciberseguridad en Alemania

A. CIFRAS CLAVE

en Alemania, como en la mayoría de países desarrollados, la ciberseguridad se ha convertido en un elemento clave para las empresas. La creciente complejidad de los entornos de TI, la agilidad y la cantidad de los ciberataques, así como los crecientes requisitos son cada vez más difíciles de controlar con los recursos de ciberseguridad existentes. La pandemia de COVID-19 y el auge del teletrabajo con ella asociado suponen una prueba más de la capacidad de la empresa para defenderse y reaccionar ante estos acontecimientos. La ciberseguridad se está volviendo cada vez más crucial para el éxito económico de toda empresa y organización.

Ciberseguridad	Alemania
Tamaño del mercado de los bienes de ciberseguridad en Alemania	26.800 millones de euros
Cuota de mercado de servicios	68,7 %
Cuota de mercado de *software*	30,4 %
Cuota de mercado de *hardware*	0,9 %
Exportaciones de bienes de ciberseguridad	4.400 millones de EUR
Importaciones de bienes de ciberseguridad	4.200 millones de EUR
Regulación	Ley de Seguridad Informática (IT-SiG 2.0)
	Nuevo Reglamento General de Protección de Datos (Datenschutzgrundverordnung – DSGVO)

B. CARACTERÍSTICAS DEL MERCADO

B.1. Definición precisa del sector estudiado

El sector de la ciberseguridad se engloba dentro del sector de las tecnologías de la información y comunicación o TIC. Se trata de un sector transversal que cuenta con presencia en diversas industrias y tecnologías, y se halla en constante cambio y digitalización.

Según una encuesta del año 2018, la ciberseguridad era considerada la tendencia más relevante del sector TIC (67 %), seguida de computación en la nube (61 %), el Internet de las cosas (48 %) y la industria 4.0 (47 %)[1].

B.1.1. Estructura de la industria

Según el Ministerio de Economía y Energía (Bundesministerium für Wirtschaft und Energie – BMWi), el sector de la ciberseguridad se subdivide en las siguientes partes:

- ***Software*:** antivirus, *firewall,* detección y prevención de intrusiones, control de acceso a redes, VPN (*Virtual Private Network*), aplicaciones y dispositivos de control, seguridad para dispositivos móviles, PKI (*Public Key Infraestructure*, usados para certificados digitales), gestión de derechos digitales, codificación, autorizaciones y autentificaciones, etc.
- ***Hardware*:** se trata principalmente de *tokens* de seguridad, tarjetas inteligentes, dispositivos de encriptación y escáneres de huellas digitales.
- **Servicios:** todas aquellas actividades relacionadas con la seguridad: análisis de seguridad, formación de seguridad y sensibilización y estrategia y arquitectura de seguridad. También engloba MSS (*Managed Security Services*, incluyendo servicios de seguridad de red externalizados), vigilancia y monitorización, gestiones de accesos y configuración, auditoría y certificación. Asimismo, se consideran parte de los servicios el cómputo forense, la seguridad en la nube (*cloud computing security*), codificación y servicios de archivo, y tests de código, entre otros.

B.1.2. Tipos de ciberataques

Según el estudio *The State of IT Security in Germany in 2019* de la Agencia Federal para la Seguridad Digital (Bundesamt für Sicherheit in der Informationstechnik – BSI), existen los siguientes tipos de ataques:

- **Suplantación de identidad**: robo de usuario y contraseña de correo electrónico, cuentas bancarias, etc.
- ***Malware*:** *software* malicioso (virus, troyanos, etc.) presente en archivos adjuntos de correo electrónico o tras consultar ciertas páginas web (*drive-by downloads*), o al pinchar sobre *banners* de publicidad con enlaces maliciosos. Según la Agencia Federal para la Seguridad Digital (BSI), existen 114 millones de *malware* diferentes registrados, de los que 65 millones afectan al sistema operativo de Windows, 3,4 millones afectan a Android, aproximadamente 0,09 millones afectan a MacOs, y otros 39 millones se categorizan como “otros”. De media hay 320.000 piezas nuevas de *malware* al día[2].
- ***Ransomware*:** *software* malicioso que impide al usuario acceder al sistema y a los datos propios, y los bloquea hasta que el afectado desembolse un rescate.
- **Ataques DDoS (*Distributed-Denial-of-Service*):** consisten en redes de *bots* que atacan simultáneamente un sistema ocupando todo su ancho de banda, impidiendo a los usuarios acceder al sistema, a menudo realizados con el objetivo de ocultar otro ataque. Las empresas alemanas han reportado pérdidas de hasta 40.000 millones de euros por estos ataques en 2018.
- **Redes de *bots*:** el uso de estas redes permite a los cibercriminales acceder a sistemas de terceros (ordenadores, móviles, *routers*, etc.) que pueden usar para sus propios intereses, como cometer fraudes a través de bancos *online*.

[1] Statista, encuesta *Welches sind die wichtigsten IT-Trends des Jahres 2018?*

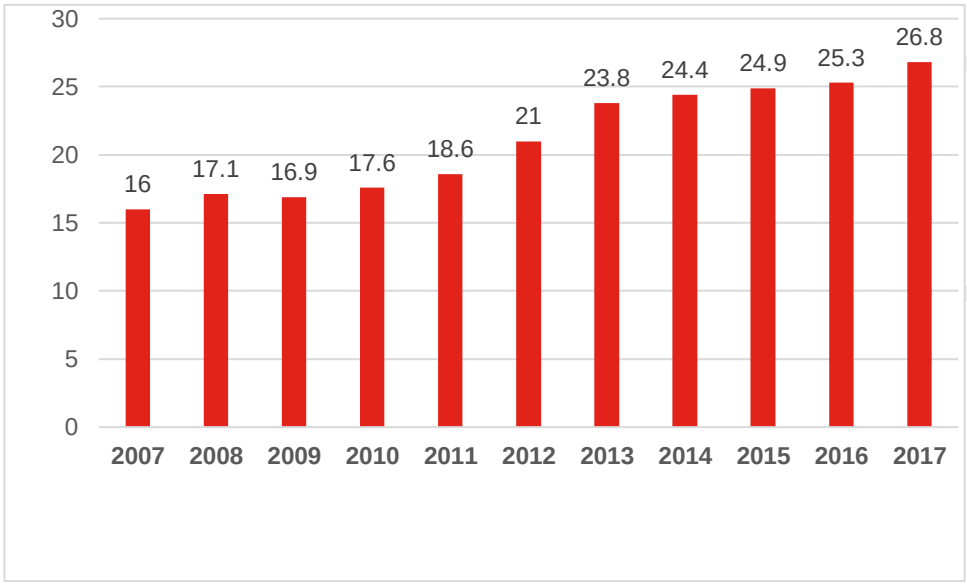
[2] *The State of IT Security in Germany in 2019*, Agencia Federal para la Seguridad Digital (BSI).

- ***Spam*:** correos electrónicos no deseados que pueden contener *software* malicioso.
- **Amenaza persistente avanzada (APT, *Advanced Persistent Threat*)**: consiste en el ataque de objetivos minuciosamente seleccionados, como gobiernos o grandes empresas. Con un objetivo económico o político, se integran sigilosamente en los sistemas durante largos periodos de tiempo.
- **Vectores de ataque en un contexto de criptografía**: ataques de canal lateral basados en informaciones secundarias (como señales de energía, magnéticas, sonidos, etc.) obtenidas durante la implementación física de un criptosistema.

B.2. Tamaño del mercado

Según un estudio elaborado por el WifOR Institute, sobre la evolución del mercado de la ciberseguridad en la década 2007-2017, el crecimiento de este mercado sólo se redujo en 2009 debido a la crisis económica, para recuperarse al año siguiente y continuar en línea ascendente, alcanzando en 2017 los 26.800 millones de euros[3].

VOLUMEN DE MERCADO DE LOS BIENES DE CIBERSEGURIDAD EN ALEMANIA
(en miles de millones de euros)

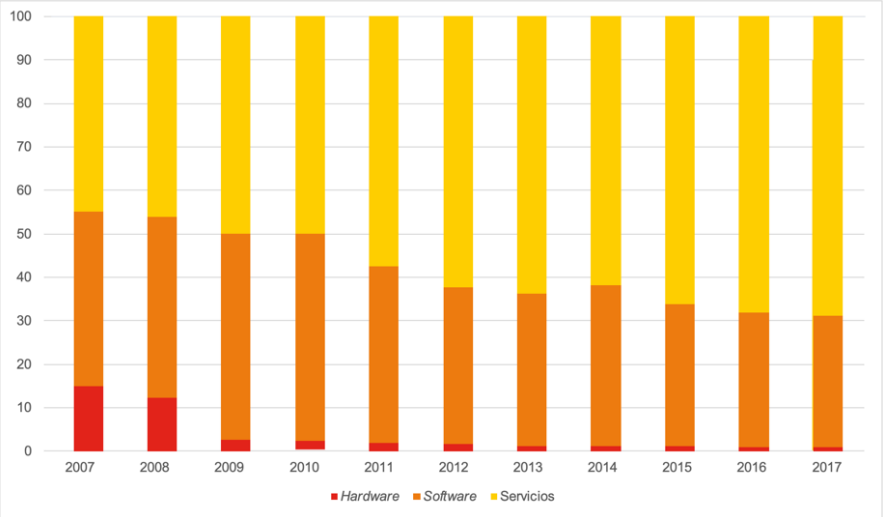


Fuente: Elaboración propia con datos de WifOR INSTITUTE.

Mientras que en el año 2007 las cuotas de mercado del *software* y de los servicios eran relativamente similares, con un 40,1 % y 44,9 %, respectivamente, se observa un desarrollo diferente de esta tendencia en el periodo hasta 2017. En el último año, la cuota de *software* se ha hundido hasta el 30,4 %, mientras que la cuota de servicios en el mercado de la ciberseguridad ha aumentado hasta el 68,7 %. La cuota de *hardware*, por su lado, se ha reducido de 15 % a 0,9 % en este tiempo, con motivo de una disminución de la necesidad de este tipo de productos.

[3] *Der IT-Sicherheitsmarkt in Deutschland,* WifOR INSTITUTE.

COMPOSICIÓN PORCENTUAL DEL MERCADO DE LA CIBERSEGURIDAD



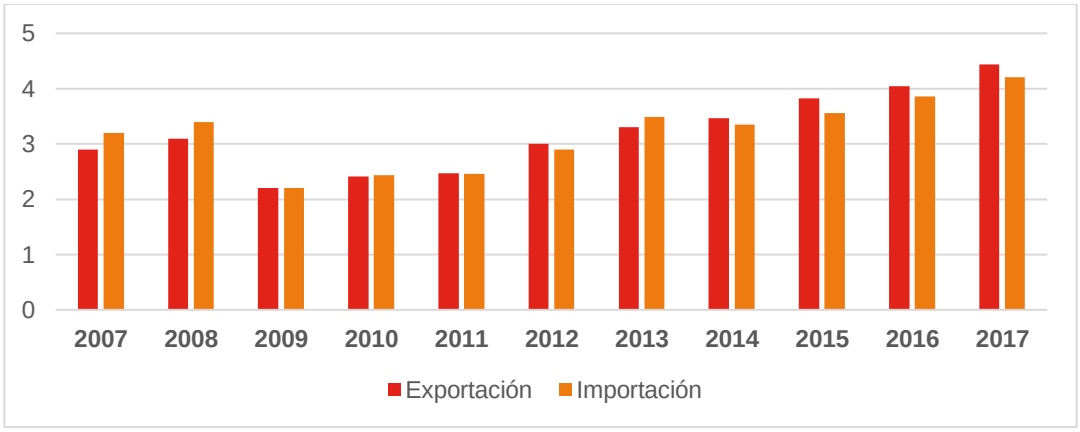
Fuente: Elaboración propia con datos de WifOR INSTITUTE.

B.2.1. Comercio exterior

Siguiendo con el estudio elaborado por el WifOR Institute, con la excepción de la caída del año 2009 con motivo de la crisis económico-financiera, las exportaciones han crecido de manera continuada. En el año 2017, se produjeron bienes de ciberseguridad para la exportación por valor de 4.400 millones de euros. En el periodo entre 2007 y 2017 el valor de las exportaciones aumentó un 53 %, dando lugar a un crecimiento anual del 4,4 %. En comparación con el crecimiento de 3,6 % anual de las exportaciones de la economía general alemana en este periodo, la ciberseguridad muestra un desarrollo superior a la media.

De forma paralela a las exportaciones, las importaciones del sector de la ciberseguridad aumentaron tras la recesión a partir del año 2010. De esta manera, el crecimiento de las importaciones en el periodo observado asciende a 31 % en total, dando lugar a unas importaciones en el año 2017 por valor de 4.200 millones de euros. Con ello, las importaciones han experimentado un crecimiento de un 2,7 % anual, significantemente inferiores a las exportaciones, y presentando el sector una balanza comercial superavitaria.

DESARROLLO DEL COMERCIO EXTERIOR DE BIENES DE CIBERSEGURIDAD
(en miles de millones de EUR)



Fuente: Elaboración propia con datos de WifOR INSTITUTE.

En la comparación del comercio exterior según sus subdivisiones, en el año 2017 se observa que la exportación de *software* y de servicios es ligeramente superior a la importación, mientras que el intercambio de bienes de tipo *hardware* es similar en ambas direcciones[4].

BALANZA COMERCIAL DE CIBERSEGURIDAD, 2017
(en millones EUR)

	Hardware	*Software*	Servicios
Exportaciones	300	1.300	2.900
Importaciones	300	1.200	2.700

Fuente: Elaboración propia con datos de WifOR INSTITUTE.

B.3. Principales actores

Los principales organismos y asociaciones de la ciberseguridad en Alemania son los siguientes:

- **Agencia Federal para la Seguridad Digital** (Bundesamt für Sicherheit in der Informationstechnik – BSI): perteneciente al Ministerio del Interior (Bundesministerium des Innern, für Bau und Heimat – BMI), tiene el objetivo de promover la ciberseguridad en Alemania. Se trata del primero y, especialmente, el principal proveedor de ciberseguridad para el Gobierno federal alemán. Sin embargo, también proporciona sus servicios a empresas del sector TI, así como a usuarios privados y proveedores de tecnologías de la información.

  TeleTrusT: se trata de la Asociación Federal de Ciberseguridad. Fundada en 1989, consiste en una red de competencias que engloba miembros nacionales e internacionales procedentes de la Industria, Administración, Asesoramiento y Ciencia, así como organizaciones asociadas relacionadas. Con unos miembros muy variados y organizaciones asociadas, TeleTrusT representa la mayor asociación de competencias para la ciberseguridad en Alemania y Europa. TeleTrusT apoya a sus miembros con información de calidad. Los órganos de trabajo preparan publicaciones, actos organizados y posiciones sectoriales. Sus actividades y eventos ofrecen la posibilidad de *networking* en el área de la ciberseguridad.

- **BITKOM** (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien): se trata de una asociación de empresas activas en la economía digital: *software,* TI, telecomunicaciones, servicios de Internet, *hardware*, electrónica, etc. Representa a más de 2.700 empresas de la economía digital y tiene el objetivo de establecer a Alemania como el motor de cambio en Europa y en el mundo.

- **Instituto para la Ciberseguridad** (Institut für Internet-Sicherheit if(is)): se trata de unas instalaciones científicas, independientes e innovadoras de la Universidad Westfälische Hochschule. Además de sus labores en I+D, es un proveedor de servicios con foco en la ciberseguridad.

- **CERT-Bund**: se trata del equipo alemán de respuesta a incidencias de ciberseguridad.

- **Consejo de Ciberseguridad de Alemania** (Cyber-Sicherheitsrat Deutschland e.V.) asociación dedicada a asesorar a empresas, autoridades y a la política alemana en materia de ciberseguridad y la lucha contra la cibercriminalidad.

[4] *Der IT-Sicherheitsmarkt in Deutschland* | WifOR INSTITUTE.

C. LA OFERTA ESPAÑOLA

Tanto España como Alemania colaboran en la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) y en el consorcio europeo European Cyber Security Organisation (ECSO). España continúa escalando en el índice global de ciberseguridad, habiendo llegado al 7.º puesto en 2019 (frente al 19.º en la anterior edición), y quedado por encima de Alemania. A pesar de ello, a nivel de mercado no cuenta con especial renombre.

Destacan los grandes proveedores de ciberseguridad como Telefónica con Eleven Paths, Indra con Minsait o GMV Innovating Solutions, pero más allá de este tipo de empresas existe un amplio número de pymes que tratan de competir mediante especialización, avances tecnológicos o vía precio. Este hecho pone de manifiesto que la oferta española se encuentra muy **atomizada**, lo que implica que a menudo cuando hay alguna pyme que destaca, tiende a ser absorbida por grandes multinacionales americanas, israelíes o asiáticas, como ha ocurrido con el caso de Panda Security, que ha sido comprada en 2020 por la empresa estadounidense WatchGuard.

En conclusión, la escasa percepción de España como *partner* tecnológico y la predilección por el *made in Germany* de un sector tan proteccionista como el de la ciberseguridad, ponen de manifiesto la necesidad de reforzar la propuesta de valor de las empresas españolas, en un mercado donde la la generación de confianza entre los clientes locales, especialmente con las pymes, y la adaptación a sus problemas suponen factores clave del éxito.

D. OPORTUNIDADES DEL MERCADO

El mercado alemán de ciberseguridad cuenta con una serie de características que lo hacen especialmente atractivo, tales como el tamaño de su mercado interno y su sólido tejido empresarial e industrial, con una especial relevancia en cuanto a sectores críticos como, por ejemplo, el financiero (especialmente tras el BREXIT); los elevados precios de servicios y productos de ciberseguridad, lo cual permite poder complementar la oferta disponible con gamas más accesibles y económicas; y también, su estratégica ubicación geopolítica en Europa y como miembro de referencia de la UE.

En la actualidad, no hay suficientes proveedores de ciberseguridad en Alemania para atender toda la demanda, por lo que todavía se necesitan soluciones internacionales para cubrir esta brecha. Si bien las grandes empresas suelen tener sus necesidades cubiertas, existen sin embargo cada vez más pymes que demandan este tipo de productos y servicios, y las grandes buscan siempre nuevas soluciones más avanzadas. Esto brinda a las empresas españolas la oportunidad de establecerse en Alemania como proveedoras de productos y servicios a largo plazo para todo tipo de empresas (clientes finales, integradoras, consultoras, etc.).

En el mercado alemán destacan en concreto las siguientes oportunidades:

- Establecer la **ciberseguridad como facilitador de procesos**, especialmente en los nuevos desarrollos tecnológicos relacionados con la digitalización y que marcarán la diferencia en las cadenas de valor mundiales; como son la conducción autónoma, el *big data*, IoT, nube, etc.
- Las **soluciones para empresas medianas** (conocidas en Alemania como *Mittelstand*), en muchos casos empresas exportadoras, industriales y sólidas económicamente, pero, por regla general, con ciertas carencias en cuanto a digitalización y seguridad informática.
- Las soluciones para el **teletrabajo**, especialmente tras el impulso provocado por las repercusiones de la COVID-19.

Este último punto se pone de manifiesto en el *Estudio de IDC sobre Ciberseguridad 2020+*,[5] que señala, que con los cambios pertinentes dada la nueva situación provocada por la COVID-19, las empresas han incrementado el gasto en ciberseguridad en los siguientes ámbitos:

[5] El *IDC Studie zu Cyber Security 2020+* es un estudio basado en una encuesta realizada en agosto de 2020 en Alemania a 210 organizaciones con más de 100 trabajadores.

1) Seguridad del teletrabajo
2) Seguridad de redes
3) Seguridad de datos

La transformación digital propulsada por la COVID-19 ha llevado a muchas empresas alemanas a introducir la modalidad del teletrabajo. Muchas de estas empresas no contaban con la preparación necesaria para esta forma de trabajo al inicio de la pandemia, por lo que ha tenido lugar un incremento de demanda de productos que la faciliten y garanticen una protección de los trabajadores y de los equipos. Tanto la seguridad de redes como de datos suponen un blanco fácil para los ciberataques, especialmente entre las empresas que acaban de iniciarse en el teletrabajo y no cuentan aún con estructuras lo suficientemente desarrolladas para su protección. Esto también ha propiciado que las empresas incrementen su gasto y estén abiertas a probar nuevos productos y servicios. Además, con la proliferación de los ciberataques, se espera que áreas como DFIR (*Digital Forensics and Incident Response*) crezcan sustancialmente en los próximos años.

Los sectores que más invierten son los de suministro de energía, transporte y logística y el de la banca y las aseguradoras[6]. Asimismo, cada vez se observa una mayor demanda que no proviene de los sectores tradicionales únicamente, sino de los sectores *retail,* F&B, farmacéutico y sanitario.

E. CLAVES DE ACCESO AL MERCADO

E.1. Distribución

Los principales canales de distribución son los siguientes:

- **Mayoristas:** se dedican a la compra de productos de ciberseguridad y la venta principalmente a consultoras, integradores y a los proveedores de servicios gestionados de seguridad.
- **Distribuidores:** venden los productos directamente a empresas de ciberseguridad o a clientes finales. En ocasiones, tanto distribuidores como mayoristas comercializan sus productos a los revendedores de valor añadido.
- **Minoristas:** se trata de tiendas de informática, grandes superficies o pequeñas consultoras orientadas a pymes y particulares.

Lo habitual es que las soluciones más complejas técnicamente y que requieren una adaptación al cliente sean realizadas por una integradora o consultora local alemana, lo que supondría la forma más fácil de introducirse en el mercado alemán, completando con soluciones la cartera de productos de las empresas locales.

E.2. Barreras reglamentarias

E.2.1. Homologación y certificación

La Agencia Federal para la Seguridad Digital (BSI) es la encargada de la homologación y la certificación local en ciberseguridad. En principio, la certificación estándar ISO/IEC 15408 valdría para operar en Alemania y los productos podrían certificarse en España en el Organismo de Certificación de la Seguridad de las Tecnologías de la Información (CCN).

En el caso de las soluciones complejas se recomienda registrarse a través de la Agencia Federal para la Seguridad Digital (BSI). Asimismo, esta agencia reconoce la certificación de productos mediante empresas privadas (como T-Systems o TÜV Informationstechnik GmbH).

[6] Fuente: https://www.bundesdruckerei.de/system/files/dokumente/pdf/Studie-Digitalisierung_und_IT-Sicherheit.pdf

E.2.2. Regulación

Desde 2015, la Ley de Seguridad Informática (IT-Sicherheitsgesetz) contribuye a que los sistemas de TI y las infraestructuras digitales de Alemania sean de los más seguros del mundo[7]. Particularmente se garantiza la seguridad del área de las infraestructuras críticas, como el suministro de agua y electricidad, las finanzas o la nutrición, donde una falla o deterioro de los servicios de suministro tendría consecuencias dramáticas para la economía, el Estado y la sociedad.

El objetivo de la Ley de Seguridad Informática es también mejorar la seguridad en las empresas y en la Administración federal, así como asegurar una mejor protección de los ciudadanos en Internet. Las empresas de telecomunicaciones también se enfrentarán a mayores exigencias: están obligadas a advertir a sus clientes si descubren un uso indebido de una línea de cliente. Además, deben mostrar a los afectados posibles soluciones cuando sea factible. La autoridad supervisora responsable en estos casos es la Agencia Federal de Redes (*Bundesnetzagentur*). Para lograr estos objetivos, entre otros, se ampliaron las tareas y competencias de la Agencia Federal para la Seguridad Digital (BSI).

Esta Ley ha sido objeto de numerosas modificaciones y muy recientemente (finales de noviembre de 2020) el Gobierno alemán ha acordado el proyecto de una nueva Ley de Seguridad Informática (IT-SiG 2.0)[8]. En concreto, especifica un nuevo reglamento que estipula un procedimiento de examen en dos fases que prueba tanto la fiabilidad técnica de los componentes de red como la fiabilidad política de los fabricantes.

Esta Ley contempla la prohibición de los componentes críticos en caso de poner en peligro los intereses públicos primordiales. Asimismo, uno de los artículos del proyecto exige a los proveedores de equipos de red que emitan una garantía en la que aseguren que su tecnología no puede ser objeto de ciberataques; de este modo, en caso de demostrarse que alguna empresa no cumple este requisito, podría ser excluida por completo de la red alemana.

Por otro lado, desde el 25 de mayo de 2018, las disposiciones de protección de datos contenidas en el nuevo Reglamento General Europeo de Protección de Datos (RGPD) son vinculantes en los respectivos Estados miembros, incluso sin la trasposición por separado a la legislación nacional. Este reglamento tiene como objetivo fortalecer los derechos de los consumidores en particular.

Una violación del Reglamento General de Protección de Datos de la UE puede conllevar multas de hasta 20 millones de euros, o de hasta el 4 % de las ventas globales del infractor.

Este nuevo Reglamento General de Protección de Datos (Datenschutzgrundverordnung – DSGVO) sustituye a la antigua Ley Federal de Protección de Datos (Bundesdatenschutzgesetz – BDSG), que regulaba la protección de datos en Alemania y proporcionaba instrucciones a los organismos públicos y privados para la recopilación y el procesamiento de datos personales.

Además de la DSGVO, muchas otras leyes y ordenanzas regulan la protección de datos en Alemania, tanto a nivel federal como estatal. Cada región tiene su propia ley de protección de datos.

Cabe destacar que el derecho penal alemán contempla la tipificación penal de actos delictivos relacionados con la cibercriminalidad como la falsificación, la sustitución, o la alteración de datos; ataques de denegación de servicio; la piratería, etc.

E.3. Ayudas

Destacan las siguientes ayudas:

[7] Agencia Federal para la Seguridad Digital (BSI).
[8] *Handelsblatt*.

- Iniciativa "**Ciberseguridad en la Economía**" (*IT-Sicherheit in der Wirtschaft*). Este programa de subvenciones del Ministerio de Economía y Energía está dirigido especialmente a pymes para lograr una sensibilización y un fortalecimiento en el tema de la ciberseguridad durante su transformación digital. La iniciativa prevé una subvención por hasta tres años y de hasta el 90 % de los costes subvencionables, o hasta el 100 % de los gastos subvencionables.

- Subvención "**Digital ahora – incentivo a la inversión para pymes**" (*Digital Jetzt – Investitionsförderung für KMU*): el programa ofrece ayudas económicas y tiene como objetivo animar a las empresas a invertir más en tecnologías digitales y en la cualificación de sus empleados. Un objetivo del programa en particular es una mayor ciberseguridad en las empresas. El importe máximo de financiación asciende a 50.000 euros por empresa; para inversiones en cadenas de valor y/o redes, puede ser de hasta 100.000 euros por empresa.

- **Go-digital**: con sus tres módulos "Procesos de negocio digitalizados", "Desarrollo del mercado digital" y "Seguridad informática", el go-digital está dirigido específicamente a las pequeñas y medianas empresas del sector comercial y los oficios especializados.

Asimismo, existen programas de ayuda de cada región, como es el caso del programa **Digitalbonus** de la región de Baviera.

E.4. Ferias

Destacan las siguientes ferias en el ámbito de la ciberseguridad en Alemania:

- **IT-SA:** se trata de la feria de ciberseguridad más grande de Europa. Los temas principales son gestión de la nube, ciberseguridad, seguridad móvil, de datos y de la red. Se celebra desde 2009 en Messezentrum Nürnberg de manera anual. La próxima edición tendrá lugar del 12 al 14 de octubre de 2021.

- **Cyber Security Fairevent (CSF)**; se celebra anualmente en marzo en Messe Dortmund y la próxima edición tendrá lugar entre el 3 y el 4 de marzo de 2021. Se abordan los temas de la ciberseguridad, soluciones prácticas, seguridad de la información, seguridad operativa, seguridad de datos, protección de datos, *backup,* seguridad móvil, web y en el correo electrónico, etc.

- **SecIT by Heise**: punto de encuentro entre proveedores y usuarios de ciberseguridad. Tiene lugar anualmente en Messe Hannover y la próxima edición será del 23 al 25 de febrero de 2021. Gira en torno a tecnologías de red, procesos comerciales, cifrado, autenticación y protección de aplicaciones de Internet, así como conceptos para simplificar la infraestructura de TI, soluciones para reducir costes de TI.

- **Innosecure:** consiste en un congreso con exposiciones de innovaciones de las tecnologías de la seguridad. Tiene lugar en Düsseldorf cada dos años y pone en contacto a proveedores y compradores. Los temas principales son: RFID, biométrica, mecatrónica, *wireless,* IT, integración de sistemas y automatización. Se desconoce la fecha para la próxima edición.

- **DMEA** (antiguamente ConhIT – Connecting Healthcare IT): se trata de la feria europea líder en TI para sanidad que conecta a los responsables de las decisiones del sector sanitario, de la formulación de políticas y ciencia. Se celebra una vez al año y la próxima edición tendrá lugar entre el 13 y el 15 de abril de 2021.

F. INFORMACIÓN ADICIONAL

Las siguientes fuentes resultan de interés para recabar más información sobre el sector:

- Statista: https://www.statista.com/

- *The State of IT Security in Germany in 2019*, Agencia Federal para la Seguridad Digital (BSI). https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2019.pdf?__blob=publicationFile&v=3
- *Der IT-Sicherheitsmarkt in Deutschland,* WifOR INSTITUTE: https://www.wifor.com/uploads/2019/08/it-sicherheitsmarkt-in-deutschland-studie-2019.pdf
- *IDC Studie zu Cyber Security 2020+*: https://www.idc.com/de/research/multi-client-project/detail?id=899252acf4675e03e232
- *Digitalisierung und IT-Sicherheit in deutschen Unternehmen (2017),* Bundesdruckerei: https://www.bundesdruckerei.de/system/files/dokumente/pdf/Studie-Digitalisierung_und_IT-Sicherheit.pdf
- *Die Lage der IT-Sicherheits, 2019,* Agencia Federal para la Seguridad Digital (Bundesamt für Sicherheit in der Informationstechnik – BSI): https://www.bsi.bund.de/DE/Home/home_node.html
- *Jahresbericht 2018*, TeleTrust: https://www.teletrust.de/fileadmin/docs/jahresbericht/TeleTrusT-Jahresbericht_2018.pdf

G. CONTACTO

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

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

Lichtensteinallee 1
BERLIN 10787 – ALEMANIA
Teléfono: +49 302292134
Email: berlin@comercio.mineco.es
http://alemania.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
Carolina Seminario Herrera

Oficina Económica y Comercial
de España en Berlín
berlin@comercio.mineco.es
Fecha: 15/12/2020

NIPO: 114-20-022-X