ICEX España Exportación e Inversiones

FS FICHA SECTOR

ALEMANIA

Ciberseguridad en Alemania

A. CIFRAS CLAVE

La pandemia ha acelerado el proceso de digitalización y ha traído importantes cambios en la economía y sociedad alemanas (teletrabajo, *e-commerce*…). Con ello, han aumentado las ciberamenazas, en número e impacto, con especial incidencia en las grandes empresas, infraestructuras críticas e instituciones públicas del país. Una mayor concienciación sobre la seguridad informática, junto con los cambios disruptivos que se esperan en sectores insignia como vehículo autónomo, las redes inteligentes, o la incipiente transformación digital de la administración pública, sitúan al mercado de ciberseguridad alemán en una posición de especial atractivo y crecimiento potencial en los próximos años. Agendas locales, nacionales y europeas coindicen en definir la ciberseguridad como elemento transversal a la doble transformación digital y verde que se espera en Europa. Por ello, la ciberseguridad es un factor de competitividad clave para la economía alemana del presente y futuro.

Indicador	Valor
Ingresos sector ciberseguridad	5.940 millones de euros (2022)
Gasto de las empresas en ciberseguridad	6.200 millones de euros (2021)
Crecimiento anual de delitos informáticos	8 %
Daños causados por la ciberdelincuencia	223.500 millones de euros (2020/2021)
Importaciones servicios TI	32.900 millones de euros (2020)
Exportaciones servicios TI	26.400 millones de euros (2020)
Autoridad federal para la ciberseguridad	Agencia Federal para la Seguridad Digital (Bundesamt für Sicherheit in der Informationstechnik – BSI)

B. CARACTERÍSTICAS DEL MERCADO

B.1. Definición precisa del sector estudiado

La ciberseguridad es la aplicación de tecnologías, procesos y controles para proteger los sistemas, redes, programas, dispositivos y datos frente a los ciberataques. Según el informe *Risk in Focus 2022*[1] (informe que analiza los principales riesgos a los que se enfrentan las compañías en Europa), la ciberseguridad encabeza el *ranking* de riesgos prioritarios para las empresas por cuarto año consecutivo. La digitalización de todas las esferas de la economía y la sociedad, impulsada por la pandemia, ha multiplicado los ataques de ciberdelincuentes, que ganan en profesionalidad y sofisticación, ejecutando ataques con cada vez mayor impacto y coste asociado. Cybersecurity Ventures prevé que los costes mundiales de la ciberdelincuencia crezcan un 15 % anual en los próximos cinco años, hasta alcanzar los 10,5 billones de dólares anuales en 2025, frente a los 3 billones de dólares de 2015[2].

Algunos de los tipos de ciberataque más frecuentes se enumeran a continuación:

- ***Malware***: *software* que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Esta definición general incluye virus, gusanos, troyanos, *spyware*, etc.
- ***Ransomware*:** el ciberdelincuente toma control del equipo infectado y secuestra la información del usuario cifrándola, para luego pedir un rescate por los datos.
- ***Phishing:*** estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir información confidencial (contraseñas, datos bancarios, etc.) de usuarios legítimos de forma fraudulenta.
- **Ataques de denegación de servicio distribuido (DDoS):** su objetivo es sobrecargar un servidor y hacerlo colapsar, para que los usuarios legítimos no puedan utilizar sus servicios.
- **Ataques de intermediario (MitM):** consiste en un tercero intermediario que es capaz de situarse en el medio de dos comunicaciones y robar la información que se envía.
- **Inyección de SQL:** el *hacker* inserta código propio en un sitio web con el fin de quebrantar las medidas de seguridad y acceder a datos protegidos.
- ***Spoofing***: usurpar una identidad electrónica para ocultar la propia identidad y así cometer delitos en Internet.

El sector de la ciberseguridad se ubica de forma transversal dentro del sector de las TIC, y se divide en tres segmentos: desarrolladores de *software*, fabricantes de *hardware* y proveedores de servicios TI. Estos últimos han experimentado en los últimos años un importante crecimiento debido, entre otros, a que la opción de externalización de todos los aspectos relativos a la seguridad informática suele ser la opción preferida por muchas empresas. Por otro lado, el sector se caracteriza por unos elevados requerimientos de I+D+i para hacer frente a la rápida evolución de las amenazas y la tecnología. El mercado está dominado por las grandes tecnológicas estadounidenses, mientras que en Europa existe un creciente mercado de pequeñas empresas y *startups* de ciberseguridad que constituyen un mercado fragmentado y tendente a sufrir adquisiciones por parte de pesos pesados del mercado global.

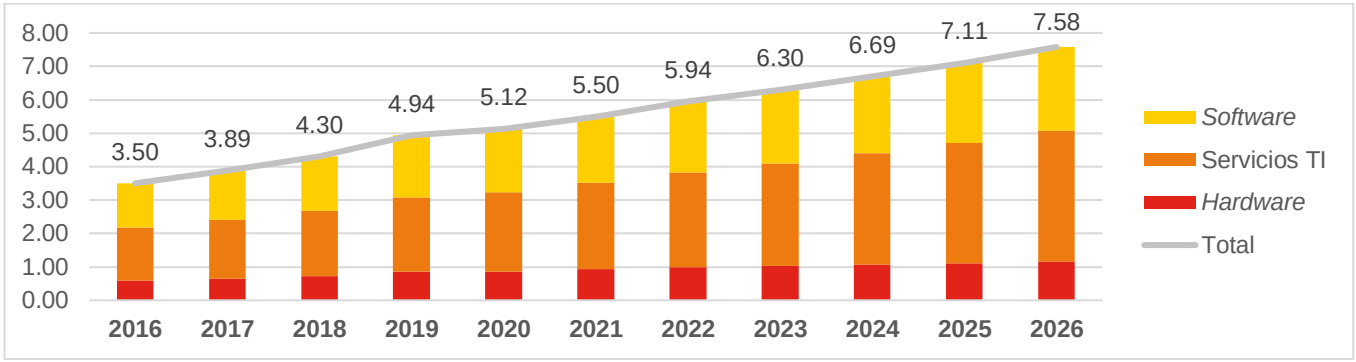
B.2. Tamaño del mercado

Los ingresos del mercado de la ciberseguridad en Alemania serán de unos 5.940 millones de euros en 2022. Se espera que los ingresos crezcan a una tasa de crecimiento anual compuesto (CAGR) 2022-2026 del 6,26 %[3]. El sector de la ciberseguridad en Alemania se divide en tres segmentos: la mayor parte de los ingresos que genera el sector corresponden al segmento de servicios TI, seguido del segmento *software* y, muy por debajo, por el segmento *hardware*. El segmento de servicios informáticos será el mayor mercado en 2022, con un volumen de mercado previsto de 2.850 millones de euros, y se espera que tenga un mayor crecimiento que el resto de segmentos.

[1] https://www.iia.org.uk/media/1691900/risk-in-focus-2022.pdf
[2] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
[3] https://de.statista.com/outlook/tmo/cybersecurity/deutschland

INGRESOS POR SEGMENTO DE MERCADO

Datos en miles de millones en euros



Fuente: Statista.

El porcentaje del gasto en TI que las empresas alemanas destinan a la ciberseguridad ha aumentado constantemente en los últimos años: ha pasado del 9 % en 2017 al 20 % en 2021, y se espera que alcance el 24 % en 2022[4]. En 2021 el gasto en seguridad informática ascendió a unos 6.200 millones de euros, y se espera que sea de 8.900 millones de euros en 2025[5]. Según datos de Eurostat, el 97 % de las empresas alemanas habian definido al menos una medida de seguridad TI, siendo este porcentaje mayor en el caso de las grandes empresas.

Este aumento del gasto está motivado por el continuo aumento de ciberataques tanto a empresas como a instituciones públicas, y su cada vez mayor potencial de impacto. En 2021, se produjeron 124.137 delitos informáticos en Alemania, casi un 14,4 % más que en 2020[6]. Según la asociación alemana del sector Bitkom e.V., los daños provocados por la ciberdelincuencia en el país ascendieron a 223.500 millones de euros en 2020/2021, más del doble que en 2018/2019. Sólo en el ámbito del *ransomware*, los daños se han multiplicado casi por cinco hasta los 24.300 millones de euros desde el último informe de 2019.

Algunos aspectos clave que definen la situación actual del entorno cibernético en Alemania:

- **Empresas de mayor tamaño, KRITIS (infraestructuras críticas) y administración pública, los principales objetivos de los ciberdelincuentes en Alemania**: los ataques de *ransomware* se destinaron principalmente a la industria manufacturera, el sector financiero, el comercio minorista e instituciones públicas.
- **Diversificación y aumento de los ciberataques, que crecen en número, alcance e impacto:** además de la pandemia, la mayor interconexión y digitalización de las cadenas de suministro internacionales (más vectores de entrada para los ciberdelincuentes, más facilidad de propagación de los programas maliciosos y mayor riesgo de fallos en cascada en toda la cadena) y la digitalización contribuyen a este crecimiento.

B.2.1. Comercio exterior

Los datos sobre comercio exterior reflejan el mayor peso del segmento de servicios TI sobre la cuota total de mercado. En 2020, por la pandemia, se registró un drástico descenso en el comercio exterior del sector, especialmente en las exportaciones. Se exportaron a Alemania servicios TI por valor de unos 26.400 millones de euros (-27,1 % respecto al año anterior): las importaciones alcanzaron los 32.900 millones de euros (-16,7 %)[7]. En el segundo trimestre de 2021, Alemania importó servicios informáticos por valor de 9.800 millones de euros y las exportaciones de servicios fueron por valor de 7.300 millones de euros.

El impacto del coronavirus fue menor en el segmento *hardware*, en el que Alemania es tradicionalmente importador neto. En el tercer trimestre de 2021 se exportaron desde Alemania productos de *hardware* informático por valor de

[4] https://de.statista.com/statistik/daten/studie/1230053/umfrage
[5] https://de.statista.com/statistik/daten/studie/1041736/umfrage/ausgaben-fuer-it-security-in-deutschland/#statisticContainer
[6] https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html
[7] https://de.statista.com/statistik/studie/id/6470/dokument/it-branche-deutschland-statista-dossier/

5.600 millones de euros (+3,6 % respecto al mismo periodo del año anterior) y se importaron productos por valor de 8.700 millones (+1,5 %)[8].

B.3. Principales actores

- Agencia Federal para la Seguridad Digital (Bundesamt für Sicherheit in der Informationstechnik – BSI): autoridad federal central para la ciberseguridad en Alemania que pertenece al Ministerio del Interior. Es responsable de la seguridad y la protección de la red de Alemania y brazo ejecutor de la agenda gubernamental para la ciberseguridad.
- Alliance for Cyber Security (Allianz für Cybersicherheit): asociación que agrupa a los principales actores del campo de la ciberseguridad en Alemania. Su misión es aumentar la ciberseguridad y fortalecer la resiliencia de Alemania a través del intercambio de información y experiencia, entre otros.
- Asociación Federal de Seguridad Informática (TeleTrusT): comprende miembros de la industria, la administración, la consultoría y la investigación, así como organizaciones asociadas nacionales e internacionales. Ofrece foros multidisciplinarios, organiza eventos y conferencias y proporciona *expertise* en cuestiones técnicas, políticas y jurídicas relacionadas con la seguridad informática.
- BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien): asociación de empresas de la economía digital (*software*, TI, telecomunicaciones, servicios de Internet, *hardware*, electrónica, etc.) con más de 2.000 empresas. Su objetivo es impulsar la digitalización, el despliegue de infraestructuras digitales y el desarrollo de modelos de negocio basados en los datos.
- CERT-Bund: equipo federal de respuesta a emergencias informáticas. Como proveedor de servicios para la administración federal, el CERT-Bund define mejores prácticas para la prevención de daños, provee de información sobre vulnerabilidades de seguridad y formula recomendaciones y buenas prácticas.
- 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 lucha contra la ciberdelincuencia. Formado por grandes y medianas empresas, operadores de infraestructuras críticas, numerosos estados federados, grandes ciudades, así como expertos y responsables de la ciberseguridad.
- Nationales Cyber Abwehrzentrum (Cyber AZ): una plataforma de cooperación, comunicación y coordinación de las autoridades alemanas (de seguridad) y otras instituciones de diferentes ministerios, que se ocupa en particular de los asuntos cibernéticos de relevancia nacional. Depende de la BSI.
- UP-KRITIS: asociación público-privada para la protección de infraestructuras críticas en Alemania.
- TISiM (Transferstelle IT-Sicherheit im Mittelstand): oficina de transferencia de seguridad TI para pymes.

C. LA OFERTA ESPAÑOLA

Según la última edición del informe GCI (*Global Cibersecurity Index*) sobre el compromiso de los países con la ciberseguridad, España es el tercer país europeo mejor posicionado, sólo por detrás de Reino Unido y Estonia[9]. España también está bien posicionada en el índice DESI (Índice de la Economía y la Sociedad Digitales), elaborado por la Comisión Europea para supervisar los avances digitales de los Estados miembro[10].

El número de empresas TIC en España era de 25.905 en 2019 (3,4 % más que el año anterior), de las cuales el 96,5 % eran empresas de prestación de servicios TIC. En ese mismo año, las exportaciones nacionales crecieron un 11,5 % (hasta los 17.563 millones de euros). Los servicios representaron más de tres cuartas partes de las exportaciones TIC, con una tasa de crecimiento del 10 % respecto al año anterior, y supusieron el 9,5 % de las

[8] https://de.statista.com/statistik/studie/id/6470/dokument/it-branche-deutschland-statista-dossier/
[9] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[10] https://digital-strategy.ec.europa.eu/en/policies/desi-spain

exportaciones globales de servicios del país. Dentro de Europa (receptora del 70,4 % de las exportaciones), Alemania (10,7 %) está sólo por detrás de Francia (15,1 %) como destino de las exportaciones españolas[11].

Según INCIBE (Instituto Nacional de Ciberseguridad), la cadena de valor española de la ciberseguridad está compuesta por tres grandes eslabones (fabricación de componentes *hardware* y *software*, distribución de productos de ciberseguridad y prestación de servicios de ciberseguridad) cuyo consumidor final son las administraciones públicas, las grandes empresas y operadores críticos, las pymes, autónomos y los particulares. La buena posición de la industria TIC y de la ciberseguridad española en los índices analizados, así como una intensa actividad de I+D en centros de investigación punteros, un creciente ecosistema emprendedor y un impulso a la inversión pública en la materia en el marco del Plan de Recuperación, Transformación y Resiliencia, otorgan al sector unas buenas perspectivas y la oportunidad de convertirse en uno de los polos de ciberseguridad europeos.

Algunos casos de éxito internacional de empresas españolas del sector son **Eleven Paths** (filial de Telefónica) o la multinacional tecnológica **GMV**. En el universo *startup* español también ha habido casos de éxito, como la compra de **AlienVault** por la estadounidense AT&T o la compra de **VirusTotal** por Google. Sin embargo, la falta de un ecosistema unificado, de una agenda única y la escasa oferta de oportunidades de inversión en Europa (a diferencia de EE. UU.), así como un cierto proteccionismo de los Estados en la gestión de su seguridad informática, lastran la competitividad del sector en Europa, y por extensión, en España. El mercado español de ciberseguridad está muy fragmentado, lo que impide que las empresas puedan escalar e incrementar su presencia en mercados exteriores.

D. OPORTUNIDADES DEL MERCADO

Alemania se encuentra en una posición intermedia en el uso de las tecnologías digitales por parte de la comunidad empresarial, y el desarrollo de dichas tecnologías no está entre los puntos fuertes del sistema de innovación alemán. La inversión de las pymes en digitalización es baja y crece despacio. Además, desde hace años se viene advirtiendo que el sector público alemán está atrasado en materia de innovación tecnológica y digitalización. La falta de personal cualificado en tecnologías digitales es un hándicap y factor inhibidor de esta transformación. Si bien es cierto que en los últimos años los esfuerzos en esta materia se han intensificado a través de políticas y estrategias sectoriales de apoyo a la transformación digital, el país sigue presentando importantes deficiencias digitales.

El hecho de que las pymes se encuentren inmersas en procesos incipientes de transformación digital hace prever un importante crecimiento del sector de ciberseguridad (tanto servicios como desarrollo de *software* y *hardware*) y de la demanda interna. Cabe destacar el importante potencial de seguridad informática en el sector manufacturero, y en el de automoción, en particular, a medida que la producción se vuelve cada vez más digital y crece la concienciación sobre las ciberamenazas. Las empresas alemanas se encuentran en importantes cadenas de suministro globales muy susceptibles de sufrir ciberataques por el elevado impacto y coste potencial, lo que las hace especialmente atractivas para los ciberdelincuentes. Según el informe del BSI sobre *El estado de la seguridad TI en Alemania*, los sectores más atacados durante 2021 fueron la energía y la infraestructura sanitaria[12].

La Estrategia alemana de Ciberseguridad de 2021 identifica los sectores en que se concentrarán esfuerzos y para los que se adoptarán medidas específicas para mejorar su seguridad informática: la industria de la movilidad y automoción, el sector energético, el hogar inteligente, el IoT y las ciudades, Industria 4.0, sanidad, finanzas y la industria de la seguridad informática en los ámbitos de la biometría, conservación digital a largo plazo y tecnologías cuánticas.

E. CLAVES DE ACCESO AL MERCADO

E.1. Distribución

Existen diferentes métodos de entrada al mercado alemán:

[11] https://www.mineco.gob.es/portal/site/mineco/
[12] https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

- **Mayoristas:** se dedican a la compra de productos de ciberseguridad y su venta principalmente a consultoras, integradores y a los proveedores de servicios gestionados de seguridad.
- **Distribuidores:** venden los productos directamente a empresas de ciberseguridad o 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.

Algunas empresas de ciberseguridad optan por la figura del **agente o socio tecnológico** para vender sus productos a clientes finales. Por otro lado, las soluciones de mayor complejidad técnica y mayor necesidad de adaptación al cliente suelen ser implementadas por una integradora o consultora local alemana. Completar la cartera de productos de empresas locales o establecer alianzas con lideres del mercado con productos y servicios de alto valor añadido puede favorecer la entrada en el mercado.

E.2. Barreras reglamentarias y no reglamentarias

E.2.1. Legislación

Las principales leyes relacionadas con la ciberseguridad son el Reglamento General Europeo de Protección de Datos (RGPD), la Ley Federal de Protección de Datos y la Ley sobre la Oficina Federal de Seguridad de la Información. Existen a su vez regulaciones específicas para sectores concretos.

Como pais miembro de la UE, Alemania está vinculada a la consecución de los objetivos marcados por las directivas europeas en materia de ciberseguridad. La Directiva (UE) 2016/1148, de 6 de julio de 2016, relativa a las medidas para lograr un elevado nivel común de seguridad de las redes y los sistemas de información en toda la UE, es la directiva más influyente para el sector y fue traspuesta a la legislación federal alemana en 2017, modificando la Ley sobre la Oficina Federal de Seguridad de la Información (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik – BSI Gesetz*) y varias otras leyes en el ámbito de los servicios públicos.

La *BSI Gesetz* es lo más parecido a una ley de ciberseguridad que se puede encontrar en el ordenamiento jurídico alemán. En ella se encomienda a la BSI la tarea de garantizar la seguridad de la información a nivel nacional y asigna un catálogo de derechos a la BSI para dotarla de capacidad de actuación. En 2015, esta ley fue reforzada por la primera ley de seguridad informática (*Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme - IT-Sicherheitsgesetz*) y complementada por un reglamento específico sobre infraestructuras críticas. En 2021 se produjo una importante actualización en materia de seguridad TI: en mayo el Consejo Federal aprobó la Segunda ley para aumentar la seguridad de los sistemas de tecnologías de información (*IT-Sicherheitsgesetz 2.0*[13]), que otorga al BSI nuevas competencias que fortalecen significativamente su trabajo como la autoridad federal de seguridad cibernética.

E.2.2. Homologación y certificación

El BSI es la Autoridad Nacional de Certificación de Ciberseguridad de Alemania y cumple las funciones de certificación y supervision de productos, componentes y sistemas TI. Como entidad supervisora y de acuerdo con el Reglamento (UE) 2019/881, puede solicitar la información que considere pertinente, llevar a cabo auditorías, obtener acceso a las instalaciones, revocar certificados o imponer sanciones. El BSI ha cerrado acuerdos con ciertos organismos de certificación del sector privado alemán. Desde el 1 de octubre de 2021 existe un procedimiento denominado Certificación de Seguridad Acelerada (BSZ)[14] llevado a cabo por centros reconocidos por el BSI, que permite ejecutar el proceso de certificación en periodos más manejables y con menos esfuerzo burocrático.

Para evitar la certificación de un mismo producto en diferentes Estados se ha acordado el reconocimiento mutuo de los certificados de seguridad informática, si estos se basan en ITSEC o Criterios Comunes (CC)[15] y bajo ciertas condiciones. Organismos nacionales de varios países (España a través del Organismo de Certificación de la

[13] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html

[14] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung

[15] Los Criterios Comunes para la Evaluación de la Seguridad de las Tecnologías de la Información o CC son la norma internacional ISO/IEC 15408 para la certificación de la seguridad los productos y sistemas de las tecnologías de la información.

Seguridad de las Tecnologías de la Información), han firmado un acuerdo sobre el reconocimiento mutuo de estos certificados y los perfiles de protección basados en los CC hasta el nivel de confianza EAL 4.

E.3. Ayudas

En el ámbito estatal destacan las siguientes ayudas:

- Digital Jetzt: programa de financiación dirigido a facilitar la digitalización de las pymes. Ofrece subvenciones a la inversión en tecnologías digitales, inversión en formación y cualificación de empleados en tecnologías digitales.
- Go-Digital: programa de financiación para pymes del sector comercial y oficios especializados con 3 módulos de financiación, procesos empresariales digitalizados, desarrollo del mercado digital y seguridad informática.
- StartUpSecure: iniciativa para impulsar la aplicación de nuevas ideas en materia de seguridad informática con potencial de mercado. Ofrece financiación para la creación de nuevas empresas en ese ámbito y se han creado una red de incubadoras de *startups* de seguridad TI en Darmstadt, Saarbrücken, Karlsruhe o Bochum.
- IT-Sicherheit in der Wirtschaft: iniciativa para apoyar a las pymes en el establecimiento de mejoras en sus procesos de seguridad informática y en su uso de sistemas TIC, contribuyendo a mejorar su ciberseguridad en el contexto de la transformación digital.
- Tecnologías portuarias innovadoras II: subvenciones para apoyar la digitalización de infraestructuras en el ámbito portuario, a través de proyectos de diferentes tipologías, entre otros proyectos de mejora de la seguridad informática, procesos de automatización e interacción hombre-tecnología, etc.
- Otras ayudas regionales: Digitalisierungsprämie Plus - Zuschussvariante (Baden-Württemberg), BIG Digital (Brandenburg), Digitalbonus (Baviera), etc.

E.4. Ferias

Nombre	Descripción	Lugar y fecha
IT-SA	Mayor feria europea de seguridad informática y plataforma para soluciones de gestión de la nube, seguridad móvil y ciberseguridad, seguridad de los datos y redes.	Núremberg, 25-27 de octubre de 2022
Security Fairevent	Seguridad funcional y operativa, seguridad de la información, seguridad y protección de datos, estrategias innovadoras de seguridad informática, últimos desafíos y tendencias.	Dortmund, 8-9 de junio de 2022
secIT by Heise	Seguridad informática, gestores de centros de datos, administradores de redes y responsables de la toma de decisiones en materia de seguridad.	Hannover, 29-31 de marzo de 2022
Sicherheits Expo	Seguridad de edificios, control de entradas, CCTV, prevención de incendios, protección perimetral, seguridad informática, equipos de alarma, seguridad doméstica inteligente	Múnich, 29-30 de junio de 2022
DMEA	Evento de salud digital más importante de Europa, centrado en soluciones para la mejora de la eficiencia, calidad y mejora de la asistencia médica.	Berlín, 26-28 de abril de 2022
automatica	Automatización, robótica, visión artificial, sensores, sistemas de control y comunicación industrial, tecnología de seguridad, *software* y servicios, *cloud computing*.	Múnich, 21-24 de junio de 2022

F. INFORMACIÓN ADICIONAL

- *Alemania en el DESI (Índice de Economía y Sociedad Digital)*
- *Cybercrime. Bundeslagebild 2021*
- *Estrategia Alemana de Ciberseguridad*
- *Índice de ciberseguridad global*
- *Informe sobre el estado de la ciberseguridad en Alemania 2021*
- *Oficina Federal de Seguridad Informática*
- *Statista. Cybersecurty. Deutschland*

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: 0034 917 3231 20
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
Olatz Lejarza Loizaga

Bajo la supervisión de la
Oficina Económica y Comercial
de España en Berlín
berlin@comercio.mineco.es
Fecha: 01/07/2022

NIPO: 114-22-016-9