

Ciberseguridad en Reino Unido

A. CIFRAS CLAVE

Reino Unido, y especialmente Londres, es uno de los ecosistemas tecnológicos y financieros más vibrantes y complejos del mundo. Debido a la naturaleza interconectada e innovadora de estos sectores, la ciberseguridad lleva varios años siendo una de las prioridades nacionales.

Dato	Cifra	Fuente
Tamaño del mercado en 2019	8.300 millones de libras	UK Cyber Security Sectoral Analysis 2020
Inversión en 2019	348 millones de libras	UK Cyber Security Sectoral Analysis 2020
Crecimiento del mercado desde 2017	46 %	Department for Digital, Culture, Media, and Sport
Crecimiento de la inversión desde 2017	775 %	UK Cyber Security Sectoral Analysis and Deep-Dive Review 2018
Ranking mundial en ciberseguridad	1.º	ITU Global Cybersecurity Index 2018
Empleados sector en Reino Unido 2019	43.000	UK Cyber Security Sectoral Analysis 2020
Número de empresas 2019	1.221	UK Cyber Security Sectoral Analysis 2020
Crecimiento en número de empleados desde 2017	37 %	UK Cyber Security Sectoral Analysis 2020

B. CARACTERÍSTICAS DEL MERCADO

B.1. Definición precisa del sector estudiado

Los ataques cibernéticos son uno de los principales riesgos comerciales que sufren las empresas actualmente. En el Reino Unido, el 32 % de las empresas, ascendiendo a un 61 % para grandes empresas, ha sufrido un ciberataque en el último año. El coste medio del ataque se estima en 4.180 libras, aunque puede ser significativamente superior para las grandes empresas.

La práctica totalidad de las empresas, instituciones y administraciones públicas actuales utilizan equipos informáticos de algún tipo para llevar a cabo su actividad económica, almacenar información comercial y operativa y cumplir con sus obligaciones legales y fiscales. El sector de la ciberseguridad incluye todos los productos y servicios destinados a la **protección de estos equipos y la información que contienen**.

B.2. Tamaño y composición del mercado

En su [informe anual sobre ciberseguridad](#), el Ministerio de Transformación Digital, Cultura, Medios y Deporte dimensionaba en 2020 el mercado en 8.300 millones de libras. Esto representa un crecimiento del 46 % desde 2017, y un CAGR del 13 % para el periodo.

El ecosistema empresarial del sector está formado por 1.200 empresas, de las cuales más del 50 % se consideran microempresas (menos de 10 empleados y menos de 2 millones de libras de activos y facturación) y solamente el 22 % son medianas y grandes.

El sector es muy innovador y dinámico, con [soluciones que no han dejado de incrementar de precio en los últimos años](#), reflejando la constante carrera contra los nuevos métodos de los criminales. El cliente busca un proveedor que considere especialista, y esto se refleja en cómo se distribuye la oferta en el binomio especialización-diversificación: el 74 % de las empresas del sector están especializadas, es decir que su facturación corresponde en más de un 75 % a productos y servicios de ciberseguridad.

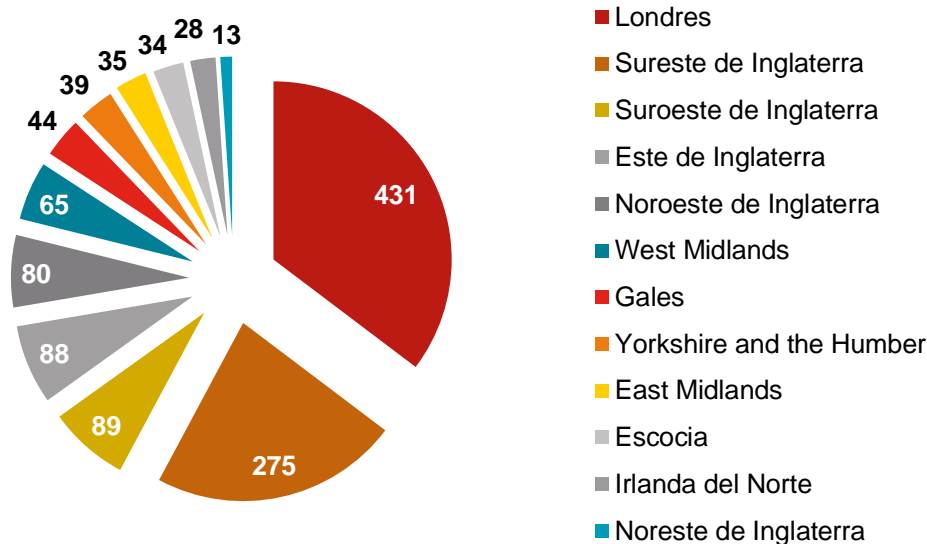
En términos de número de empleados, el sector ha crecido un 37 % en los dos últimos años, hasta alcanzar los 43.000 trabajadores a tiempo completo, de los cuales un 65 % trabajan para grandes empresas y multinacionales.

El sector aporta a la economía británica un valor añadido de 3.770 millones de libras, un incremento del 60 % en los dos últimos años. Esto muestra que las compañías británicas están consiguiendo posicionarse en las actividades de mayor valor añadido y escalabilidad, como el desarrollo de *software* y tecnologías innovadoras. Sin embargo, al estudiar el crecimiento en valor añadido por empleado, vemos que ha subido tan sólo un 18 % durante el mismo periodo, ya que las actividades de ciberseguridad más intensivas en capital humano, relativas a la integración y el soporte, tienden a tener menor escalabilidad y margen.

B.2.1. Distribución geográfica

La mayor parte del sector de la ciberseguridad se concentra en Londres y sus alrededores. El 50 % de las empresas se hallan en el sur de Inglaterra y el resto se reparten por las demás regiones del país de manera equitativa. Gales (3,6 %), Escocia (2,8 %), e Irlanda de Norte (2,3 %) alojan a un número reducido de proveedores de servicios locales. Se puede observar la distribución en detalle en el Gráfico 1.

GRÁFICO 1. DISTRIBUCIÓN GEOGRÁFICA DE LAS EMPRESAS DE CIBERSEGURIDAD BRITÁNICAS EN 2019

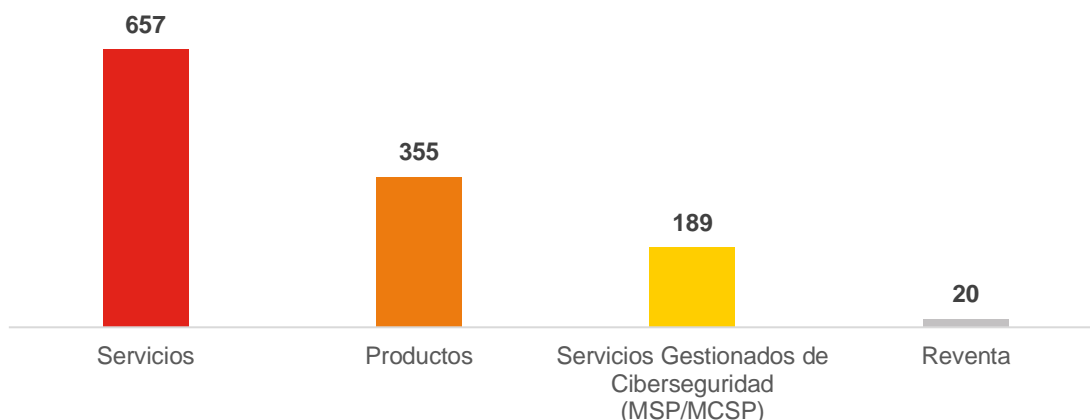


Fuente: [Department for Digital, Culture, Media and Sport](#)

B.2.2. Productos y servicios del mercado

Más de dos tercios de las empresas de Reino Unido se dedican a proveer servicios de ciberseguridad, en concreto un 69 %, contando a las empresas especializadas en proveer servicios gestionados de ciberseguridad, normalmente a cambio de un pago mensual o anual. Menos de un tercio tienen como actividad principal el desarrollo de productos de ciberseguridad (29 %).

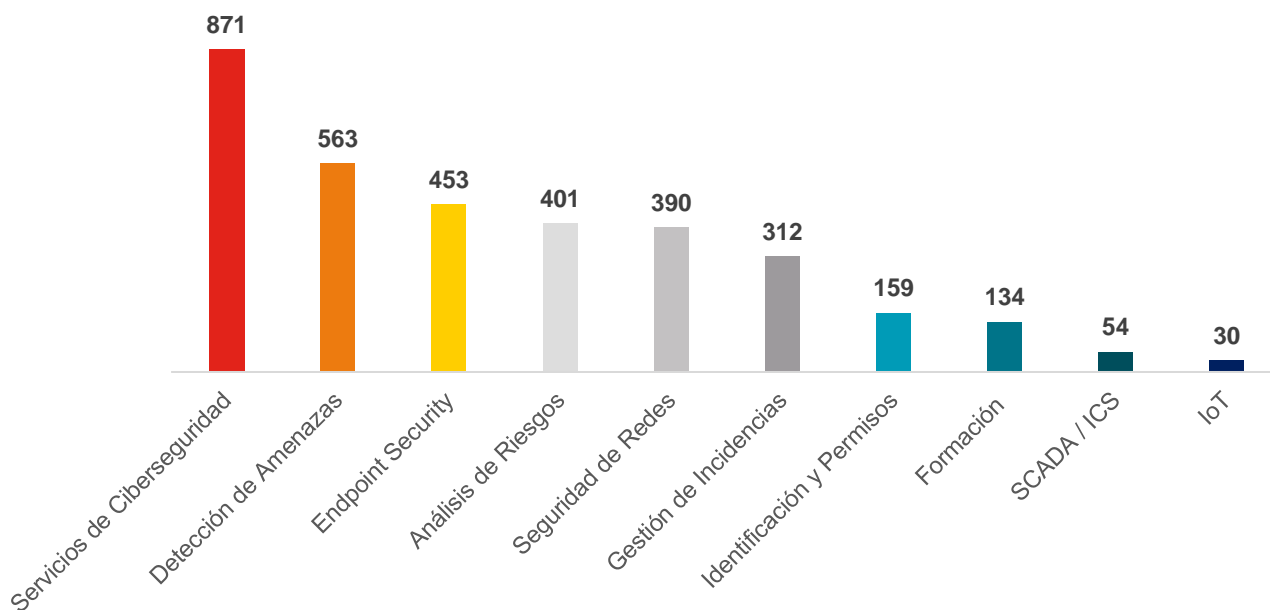
GRÁFICO 2. NÚMERO DE EMPRESAS DE CIBERSEGURIDAD EN CADA CATEGORÍA DE PRODUCTO O SERVICIO EN REINO UNIDO EN 2019



Fuente: [UK Cyber Security Sectoral Report 2020](#)

En cuanto a los productos y servicios más ofertados en Reino Unido, un 71 % de las empresas del sector ofrecen servicios profesionales de ciberseguridad. Esto se debe principalmente a que proveer servicios de consultoría presenta barreras de entrada muy bajas en comparación con el desarrollo de productos. Ahora mismo, las tecnologías como SCADA (Supervisión, Control o adquisición de datos por sus siglas inglesas) o IoT (Internet de las Cosas) comprenden al 6 % del sector, pero se espera que esto aumente en los próximos años, a medida que se incrementa su tasa de penetración.

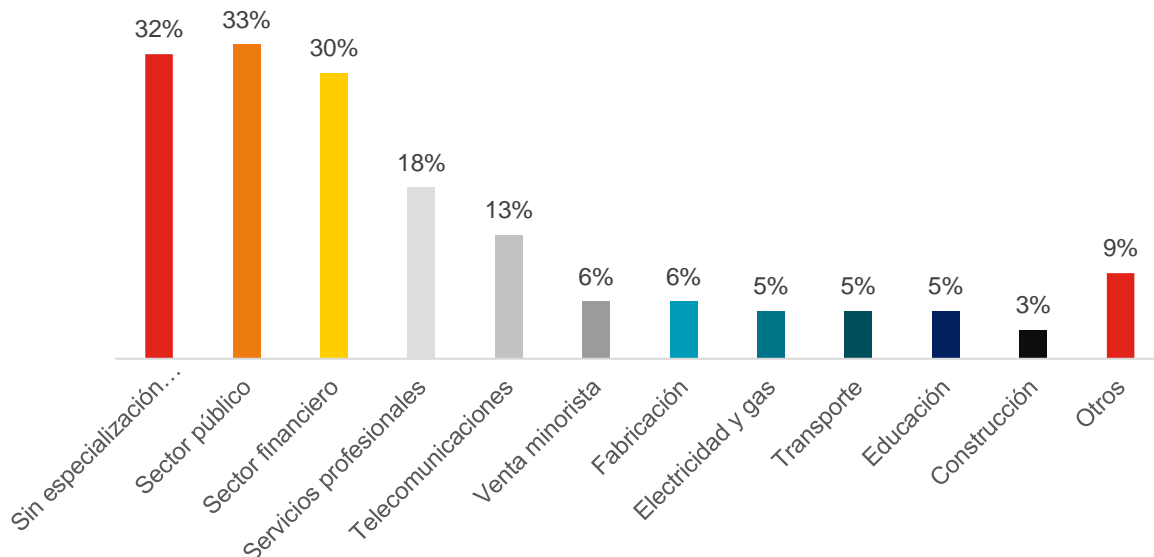
GRÁFICO 3. NÚMERO DE EMPRESAS POR CATEGORÍA DE PRODUCTO O SERVICIO OFERTADO



Fuente: [UK Cyber Security Sectoral Report UK 2020](#)

Los clientes de las empresas de ciberseguridad británicas se encuentran principalmente en el sector público, sector financiero y telecomunicaciones. Un tercio (32 %) no tiene especialización sectorial.

GRÁFICO 4. ESPECIALIZACIÓN SECTORIAL DE LAS EMPRESAS DE CIBERSEGURIDAD EN REINO UNIDO



Fuente: [UK Cyber Security Sectoral Report UK 2020](#)

B.3. Principales actores

B.3.1. Actores públicos y asociaciones

National Cyber Security Centre (NCSC)

Este organismo se encarga de asesorar y proteger a actores públicos e industria y a establecer y promocionar estándares en materia de ciberseguridad. Nació en octubre de 2016 como parte del GCHQ, la agencia de inteligencia y comunicaciones británica, y funciona como punto de contacto único para cualquier agente británico que busque protegerse de ciberataques

En su [Estrategia Nacional de Ciberseguridad 2016-2021](#), establece el NCSC como especialista técnico que concentra las funciones y capacidades de otra antiguas agencias públicas, como CERT UK, que es el antiguo equipo de resolución de incidencias informáticas.

NCSC cuenta también con una aceleradora que gestiona junto a Telefónica llamada [Wayra](#), a través de la cual ofrece servicios a proyectos innovadores del sector. En su página web hay más información sobre sus [programas](#) y el [proceso de solicitud](#) para participar en estos, que ya cuentan con éxitos como [CounterCraft](#) o [iHackLabs](#).

UK Cybersecurity Association

Es una organización sin ánimo de lucro que busca alinear los intereses de particulares y empresas del sector de la ciberseguridad, complementando la existencia de asociaciones profesionales. Se centra en asesoramiento, formación y acreditación, trabajando para diseminar la información y novedades técnicas entre el público general.

British Security Industry Association (BSIA)

Es la asociación profesional de referencia en el ámbito general de la seguridad. Sus miembros representan el 70 % de los bienes y servicios de seguridad de Reino Unido en términos de facturación. Cuentan con un área de ciberseguridad con distintos grupos de trabajo, como el [BSIA Cybersecurity Product Assurance Group \(CysPAG\)](#), que entre otras funciones establece mejores prácticas para sus miembros, como es el caso del [código de conducta para instaladores](#).

TechUK

Es una asociación profesional transversal que influencia la creación de nuevas regulaciones y promueve el desarrollo de la innovación tecnológica en Reino Unido. Ofrece formación, servicios profesionales y eventos de promoción a sus miembros, que incluyen administraciones públicas, empresas e individuos.

B.3.2. Universidades

El NCSC publicó en 2015 junto al Engineering and Physical Sciences Research Council (EPSRC) un [listado que reconocía algunas universidades británicas](#) como **Academic Centres of Excellence in Cyber Security Research (ACE-CSR)**, centros de excelencia para la investigación en ciberseguridad. Desde entonces, se han añadido nuevos centros hasta llegar al total actual de 19 ACE-CSR:

[Queens University Belfast](#); [University of Birmingham](#); [University of Bristol](#); [University of Cambridge](#); [Cardiff University \(2018\)](#); [De Montfort University \(2019\)](#); [University of Edinburgh](#); [University of Kent \(2018\)](#); [Kings College London \(2018\)](#); [Lancaster University](#); [Imperial College London](#); [University College London](#); [Royal Holloway, University of London](#); [Newcastle University](#); [Northumbria University \(2019\)](#); [University of Oxford](#); [University of Southampton](#); [University of Surrey](#) y [University of Warwick \(2017\)](#).

El NCSC apoya a estudiantes de posgrado en todos los ACE-CSR, y cuenta además con un programa de formación doctoral en tres centros: [Universidad de Bristol con la Universidad de Bath](#); Royal Holloway, Universidad de Londres y University College London.

Queens University Belfast es además la sede del [Centre for Secure Information Technologies \(CSIT\)](#), que es el centro de investigación y desarrollo universitario más importante de Reino Unido en materia de ciberseguridad.

University College London es a su vez la sede del [Research Institute for Sociotechnical Cyber Security \(RISCS\)](#), el principal centro de investigación de Reino Unido focalizado en el estudio de la seguridad integral de las empresas, incluyendo las tecnologías, personas y procesos que las constituyen.

B.3.3. Otros actores

Cylon

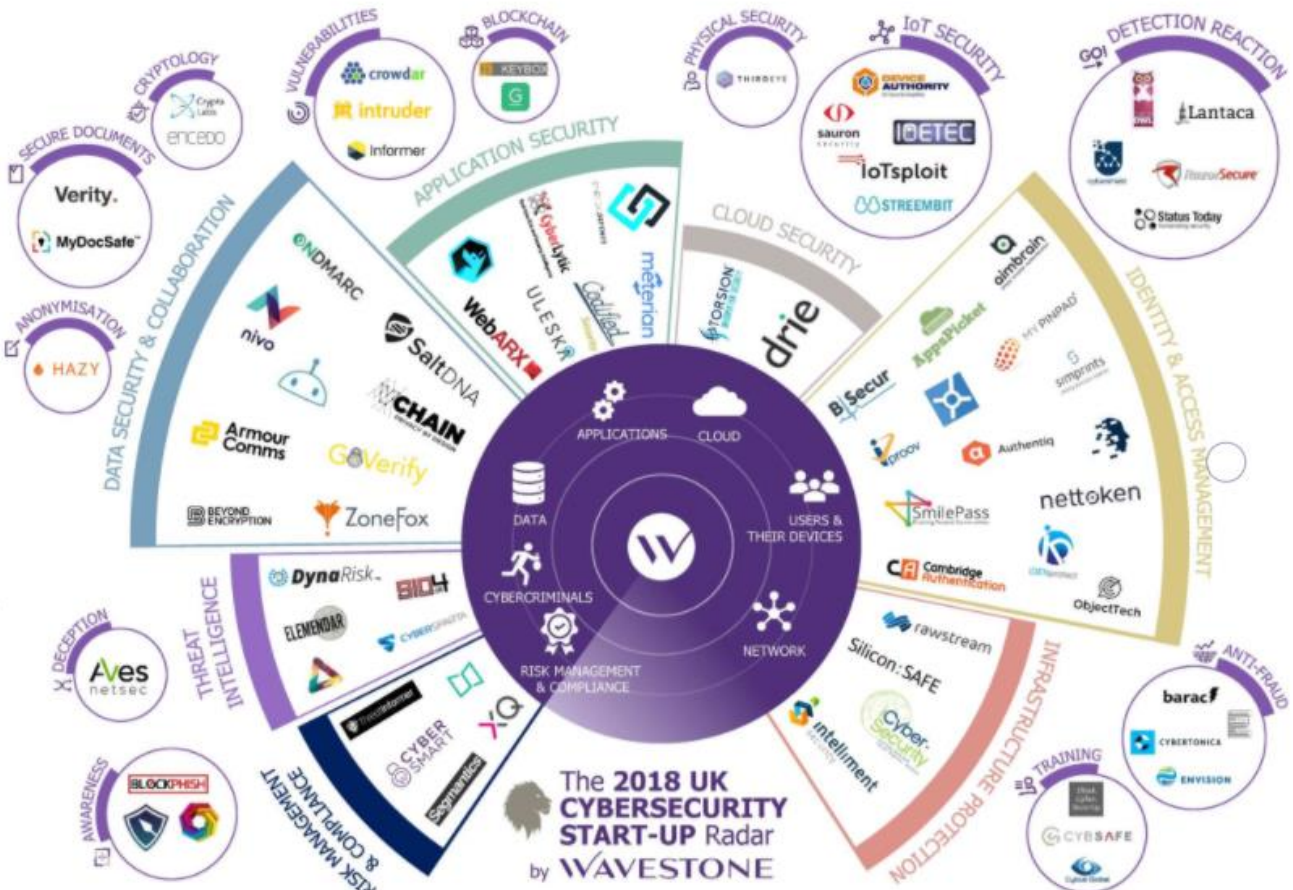
Es una incubadora y aceleradora iniciada en 2015 que apoya *startups* de ciberseguridad en todos los ámbitos, desde la formación a la identificación de amenazas, que también cuenta con programas en Singapur y Corea del Sur. Las empresas apoyadas por Cylon tiene un valor colectivo que supera los 600 millones de libras.

Cuenta con tres programas con los que da servicio al sector: Cylon Scale (hasta 150.000 libras para expansión de la red de clientes), Cylon Spark (programa de innovación y habilitación para emprendedores) y Cylon Go (programa para integración de grupos sociales con poca representación en la ciberseguridad).

Inversores privados

La explosión inversora de la ciberseguridad en Reino Unido comenzó en 2013, año en el que cerraron rondas de financiación muchos de los grandes nombres del sector, como [Digital Shadows](#), [my1login](#), [Darktrace](#) o [Tessian](#). Los principales inversores privados del sector son [TenEleven Ventures](#), [KKR](#) y [Summit Partners](#), que han participado en rondas de financiación por valor total de 400 millones de libras. La lista de principales inversores británicos en ciberseguridad incluye también [Albion Capital](#), [Octopus Ventures](#) y [Winton Investment](#).

GRÁFICO 5. MAPA DE *STARTUPS* BRITÁNICAS DE CIBERSEGURIDAD EN 2018, POR ACTIVIDAD





C. LA OFERTA ESPAÑOLA

Según un [informe sectorial de DBK sobre ciberseguridad](#), el mercado español tenía un tamaño de 1.200 millones de euros en 2018, menos de una quinta parte del británico el mismo año. Igual que en el mercado británico, la prestación de servicios representa más de dos tercios del valor total (70 %), aunque el sector se encuentra más concentrado, con un 75 % de la facturación correspondiendo a las cinco grandes empresas de servicios profesionales (Deloitte, PWC, EY, KPMG y Accenture).

Según la [Unión Internacional de Telecomunicaciones de las Naciones Unidas](#), en 2018 España era el séptimo país del mundo más comprometido con la ciberseguridad. Este *ranking* lo encabeza Reino Unido. Uno de los factores que alinea a ambos países es el papel similar que desarrollan las agencias nacionales de ciberseguridad (NCSC en Reino Unido e INCIBE en España).

La oferta de ciberseguridad española goza de cierto reconocimiento en Reino Unido, debido en gran parte a la labor realizada por multinacionales como **Telefónica**, que gracias a [Wayra](#), [ElevenPaths](#) y [iHackLabs](#) tiene un muy buen posicionamiento. Sin embargo, es un sector en el que las barreras reputacionales son difíciles de sortear, y donde la compra se basa en la confianza del cliente en empresas, soluciones y tecnologías específicas. Además de las empresas del Grupo Telefónica, hay presencia española en el sector a través de desarrolladores de soluciones como [Countercraft](#) y [Panda](#) (ahora parte del grupo americano [WatchGuard](#)) y distribuidores e integradores como [Technorizon Group](#).

Reino Unido cuenta con una oferta local muy desarrollada, además de contar con la presencia de la gran mayoría de las multinacionales del sector, incluyendo [Accenture](#), [Cisco](#) o [SonicWall](#). Esto incrementa la competitividad en el sector, sobre todo teniendo en cuenta que ciertos segmentos, como el desarrollo de productos, son infinitamente escalables y tienen un mercado global.

D. OPORTUNIDADES DEL MERCADO

Durante abril de 2020, y debido a las medidas de distanciamiento social impuestas en Reino Unido, casi un **50 % de los trabajadores** llevaron a cabo al menos parte de sus funciones a través del teletrabajo. Este crecimiento ha llevado consigo un incremento en la demanda de productos y servicios de ciberseguridad, buscando adaptarse a la conexión de terminales externos con soluciones de seguridad de redes y autenticación.

La externalización de la ciberseguridad a proveedores especializados es una tendencia que se da en los países con mayor desarrollo del sector. [Según PwC](#), la externalización de servicios significa un 32 % del gasto total en ciberseguridad en Reino Unido. Existe un gran número de empresas que proveen servicios gestionados de ciberseguridad en España, y a medida que esta tendencia se consolida habrá oportunidades para ellas en el mercado británico.

La implementación de la regulación europea en materia de protección de datos (GDPR) ha significado una de las mayores oportunidades del sector en los últimos años. Reino Unido adoptó la directiva en 2018, y todo indica que no se desviará del estándar europeo en su regulación de la gestión de datos de terceros. Sin embargo, tras el Brexit, según la legislación europea pasará a ser país tercero.

Las tecnologías punteras como SCADA, Internet de las Cosas (IoT) o *Machine Learning* tendrán una tasa de crecimiento muy alta, y existen compañías españolas con experiencia exportable a Reino Unido en sectores como el industrial o de infraestructuras. La especificidad de las soluciones de seguridad relativas a estas tecnologías será una oportunidad para fabricantes y distribuidores especializados.

El sector se está volviendo cada vez más transparente, a través de iniciativas como [Cyber Exchange](#), y esto ha permitido que las empresas tengan más información sobre las principales métricas y condiciones de mercado. Esto está posibilitando que pequeñas y medianas empresas que ofrecen soluciones y servicios competitivos sorteen las barreras de acceso reputacionales.

En su informe sectorial sobre ciberseguridad, *Fortune* señala las siguientes tendencias en el sector de la ciberseguridad para el periodo 2020-2027:

- El incremento en popularidad de servicios basados en la nube está aumentando también los ciberataques a servidores *cloud*.
- Identifica las soluciones con enfoque *Endpoint Security* como el segmento de mayor crecimiento, a medida que continúa la tendencia a interconectar dispositivos externos de forma cada vez más compleja a redes corporativas.
- La implantación de la tecnología 5G en Reino Unido traerá consigo una nueva serie de vulnerabilidades, además de un incremento en el número de dispositivos IoT que las empresas deberán proteger.

E. CLAVES DE ACCESO AL MERCADO

E.1. Distribución

El primer eslabón de la cadena de valor del sector es la fabricación, protagonizada por las multinacionales que desarrollan productos de ciberseguridad. Tienen presencia global y, normalmente, realizan sus ventas a través de intermediarios especializados. Es una actividad muy concentrada por el alto nivel de inversión que requiere, y en Reino Unido destacan fabricantes como **Sophos** (especialista en antivirus y encriptación) o **Clearswift** (especialista en protección de datos). Suelen estar especializados en *hardware* o *software*, aunque también existe la figura del fabricante mixto.

La distribución se lleva a cabo por mayoristas y distribuidores, que comercializan al cliente final o a revendedores de valor añadido. En el caso de la venta mayorista, cada vez más son compañías especializadas en seguridad TI, aunque también las hay más generalistas de informática o electrónica. En el caso de la venta minorista, se suele realizar compra directa a fabricante o a través de tiendas de informática y electrónica físicas y *online*.

El último eslabón incluye todos los servicios asociados a la incorporación de soluciones y la gestión de amenazas, que incluye los siguientes actores:

- Proveedores locales que ofrecen servicios especializados.
- Revendedores de valor añadido que agregan valor creando un paquete de productos que funciona como solución propia.
- Consultoras de negocio para asuntos legales y organizativos.
- Consultoras tecnológicas para asesoramiento, respuesta y soporte técnico.
- Integradores que combinan soluciones propias y de distintos fabricantes para la adaptación a realidades TIC complejas.
- Proveedores de servicios gestionados de ciberseguridad que tienen un enfoque integral, gestionando totalmente la ciberseguridad de sus clientes a cambio de un *fee* mensual o anual.

E.2. Barreras reglamentarias y no reglamentarias

En cuanto a los aranceles aplicables a la entrada del producto en el Reino Unido, solamente en caso de NO ACUERDO entre la UE y el Reino Unido, a partir de enero de 2021, se incluyen a continuación dos fuentes donde se puede obtener información al respecto:

- **UK Global Tariff:** Se trata de una herramienta proporcionada por el Gobierno británico, que recoge los aranceles que aplicaría el Reino Unido en caso de una salida sin acuerdo de la Unión Europea. No cubre otros derechos o medidas de importación, como los derechos *antidumping*, compensatorios o de salvaguardia, o cualquier otra forma de restricción a las importaciones.
- **Portal Access2Markets:** Se trata de una herramienta telemática que la Comisión Europea pone a disposición de las empresas para conocer los aranceles e impuestos, procedimientos aduaneros, normas de origen, obstáculos comerciales y requisitos específicos de acceso al mercado para exportar a terceros.



países. La Comisión ha incluido en esta herramienta información relativa a las exportaciones desde la UE al Reino Unido a partir del 1 de enero de 2021, simulando un escenario de no acuerdo.

Es importante que los exportadores conozcan los estándares aplicables en materia de calidad, en forma de [British Standards for Cybersecurity](#).

E.3. Ayudas

Digital Security by Design: Es un fondo gestionado por la agencia de innovación británica, [Innovate UK](#), que ofrece subvenciones a pequeñas y medianas empresas para el desarrollo de tecnologías de ciberseguridad. En 2019 se pusieron 10 millones de libras en ayudas a disposición de los 9 ganadores de la competición, que buscaba ideas innovadoras en el campo de la arquitectura de soluciones de ciberseguridad. La nueva fase del programa, [abierta desde el 30 de noviembre de 2020 al 13 de enero de 2021](#), cuenta con hasta 1,5 millones de libras para proyectos entre 40.000 y 80.000 libras de coste. En su nueva fase, busca innovaciones que hagan crecer el ecosistema *software* necesario para la implementación de soluciones de seguridad digital por diseño.

- **Ciberseguridad para el sector sanitario:** El Gobierno británico puso a disposición de las empresas privadas del sector sanitario 500.000 libras en septiembre de 2020, para cubrir todos los costes de certificación y consultoría derivados de adaptar el sector al nuevo contexto post-COVID-19.
- **Acuerdo ICEX-INCIBE:** INCIBE e ICEX tienen un acuerdo para la promoción del sector de la ciberseguridad español en el extranjero, en el marco del cual se han desarrollado y se desarrollarán actividades que incluyen misiones comerciales directas e inversas, en las cuales Reino Unido es un país prioritario. Un claro ejemplo de ello es el Foro Internacional desarrollado en el marco de [14ENISE](#), que contó con compradores británicos.

E.4. Ferias y eventos

[CyberUK](#)

Es el evento insignia del Gobierno británico en materia de ciberseguridad, organizado por el NCSC. Se celebra de forma anual y suele contar con más de 2.000 delegados del sector, que incluyen por un lado a todos los profesionales y gestores de ciberseguridad del ámbito público, y por el otro a representantes de los principales gestores de infraestructuras, servicios críticos y proveedores de seguridad informática.

Su última edición fue la de 2019 en Glasgow, ya que se decidió suspender la edición de 2020 por la situación de pandemia. CyberUK 2021 se celebrará el 11 y 12 de mayo en [ICC Gales](#) en Newport, Gales.

[Cloud & Cybersecurity Expo](#)

Es una feria organizada por [CloserStill Media](#), que da cita a las principales empresas y profesionales del sector de la ciberseguridad de Reino Unido. Se desarrolla junto ferias relacionadas sobre los sectores de IoT, *blockchain* y *Big Data* en el mismo recinto, y el registro a un evento incluye los demás. Cuenta con más de 150 expositores, 200 ponentes y la asistencia de más 700 empresas líderes del sector de la ciberseguridad. Su edición de 2021 se celebrará los días 7 y 8 de julio en [Excel, Londres](#).

[International Cyber Expo](#)

Es una feria organizada por [Nineteen](#), y cuenta con más de 50 expositores que unen servicios de seguridad físicos y cibernéticos. Recibe anualmente más de 14.000 visitantes, de todos los sectores y ámbitos públicos y privados. Algunos de los temas tratados incluyen seguridad de redes, sistemas industriales, seguridad de terminales móviles y seguridad en la nube. Su edición de 2021 se celebrará los días 28 y 29 de septiembre en [Olympia, Londres](#).

[World Data Compliance](#)

Es un evento que reúne a los profesionales en materia de gestión y protección de datos de carácter personal. Se celebra anualmente gestionado por [Growth Innovation Agility](#), que también desarrolla otros eventos internacionales en el [ámbito de la ciberseguridad](#).



Debido a las medidas de distanciamiento post-COVID 19, el evento se celebrará de manera totalmente virtual los días 30 y 31 de marzo de 2021, y ya está [abierto el plazo de registro](#).

F. INFORMACIÓN ADICIONAL

F.1. Enlaces de interés

[UK Cyber Security Sectoral Analysis 2020](#) del Ministerio de Digital, Cultura, Medios y Deporte.

[National Cyber Security Strategy 2016-2021](#) del Gobierno de Su Majestad.

[State of Cyber Security Report 2020](#) de Accenture.

[Global Cybersecurity Index \(GCI\)](#) de ITU, Naciones Unidas.

[UK Cybersecurity Deep Dive Review 2018](#) de RSM y CSIT.

icex

G. CONTACTO

La **Oficina Económica y Comercial de España en Londres** está especializada en ayudar a la internacionalización de la economía española y la asistencia a empresas y emprendedores en el **Reino Unido**

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

125 Old Broad Street
Londres EC2N 1AR – Reino Unido
Teléfono: 00 (44) (0) 2077767730
Email: londres@comercio.mineco.es
<http://reinounido.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) 97 10 00 00 (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

Claudio Garrido Turranzas

Oficina Económica y Comercial
de España en Londres

londres@comercio.mineco.es

Fecha: 23/10/2020

NIPO: 114-20-022-X

www.icex.es



FICHAS SECTOR REINO UNIDO



ICEX España
Exportación
e Inversiones