ICEX España Exportación e Inversiones

FS FICHA SECTOR

FRANCIA

Ciberseguridad en Francia

A. CIFRAS CLAVE

La rápida evolución de la industria digital desde los años noventa ha traído consigo múltiples ventajas para el bienestar y desarrollo de particulares, empresas y administraciones. Sin embargo, al mismo tiempo, el crecimiento del universo digital ha provocado la aparición de un **nuevo tipo de delincuencia** que no necesita presencia física para cometer sus delitos, y que hace un uso malicioso de estas mismas redes y sistemas de información, poniendo en riesgo la economía y la seguridad de sus víctimas. El auge de los ciberataques en los últimos tiempos –algunos de gran envergadura, como WannaCry o NotPetya– ha resultado en una **regulación más rigurosa** por parte de las autoridades competentes y en una **inversión** decidida en ciberseguridad por parte de las empresas y administraciones, con el fin de reforzar sus sistemas de información ante potenciales amenazas.

Esto ha supuesto un claro **auge de la ciberseguridad** en el mundo. Según estima el instituto de estudios Xerfi, el mercado francés de la ciberseguridad alcanzó los 2.750 millones de euros en 2018, y seguirá creciendo hasta situarse en una cifra cercana a los **4.000 millones de euros en los próximos cuatro años**. Se encuentra todavía en fase de consolidación y acoge a multitud de empresas de diverso tamaño. Sus principales retos son la **capacitación de los recursos humanos**, la adaptación de los **servicios personalizados** a clientes de distintos tamaños, y la **concienciación** de empresas y particulares.

Datos	Cifras 2018
Valor mercado TIC	56.300 millones EUR
Valor mercado de ciberseguridad	2.750 millones EUR
Empleos	24.000
***Ranking* GCI Francia**	3 / 175

	Previsión 2022
Mercado ciberseguridad	4.000 millones EUR
Servicios	+9 %
Software	+6,4 %
Hardware	+3,1 %

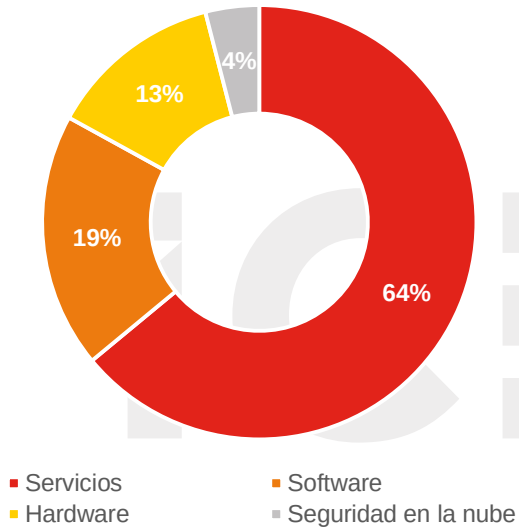
B. CARACTERÍSTICAS DEL MERCADO

B.1. Definición precisa de las actividades que conforman el sector estudiado

El sector de la ciberseguridad comprende el conjunto de medidas de seguridad susceptibles de ser implementadas para defenderse de los ciberataques. Así, el sector incluye todas las leyes, políticas, herramientas, tecnologías y acciones que pueden ser utilizadas para proteger los activos informáticos de las administraciones, empresas y particulares de un país.

De manera más concreta, el sector de la ciberseguridad puede dividirse en **servicios**, ***software***, ***hardware*** y **seguridad en la nube**. El peso de los **servicios** de ciberseguridad en el mundo alcanza prácticamente las dos terceras partes de la industria (IDC, 2018).

EL MERCADO MUNDIAL DE LA CIBERSEGURIDAD
Por tipo de prestación (%)



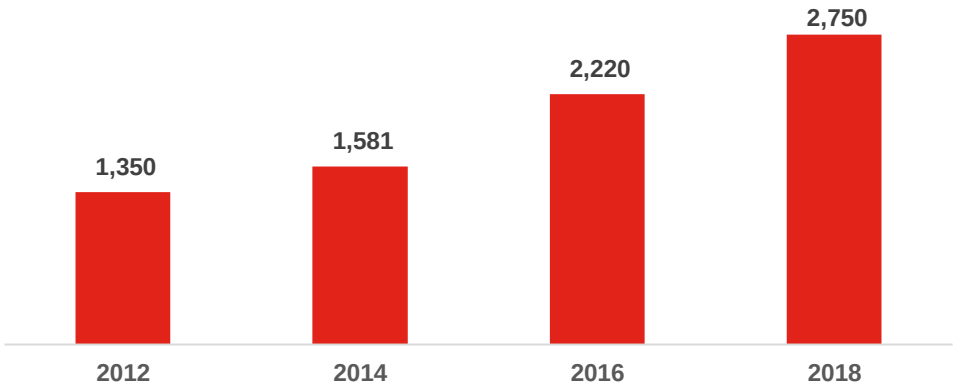
Fuente: IDC, 2018.

Se trata de un sector íntimamente ligado a la rápida evolución de los **servicios digitales** en las últimas tres décadas, y que sigue progresando año tras año gracias al gasto de las empresas no financieras en tecnologías de la información, el grado de externalización de los servicios TIC, la digitalización de la economía y la creciente importancia de la computación en la nube. Solamente en Francia, los servicios digitales generaron en el año 2018 una cifra de negocio de 56.300 millones de euros (Syntec, 2018) debido, en gran parte, al alza de las inversiones digitales de las empresas y las administraciones nacionales. Este año, la inversión en TI en Francia ha vuelto a aumentar un 6 % a pesar de un contexto macroeconómico incierto.

B.2. Tamaño del mercado

El mercado francés de la ciberseguridad alcanzó en 2018 los 2.750 millones de euros (aproximadamente un 5 % del mercado TI total). Como puede apreciarse en el gráfico, esto supone que se ha doblado el mercado en sólo seis años. Esta progresión es aún más evidente en los últimos cuatro ejercicios: + 74 %.

MERCADO FRANCÉS DE CIBERSEGURIDAD, 2012-2018
Millones de euros



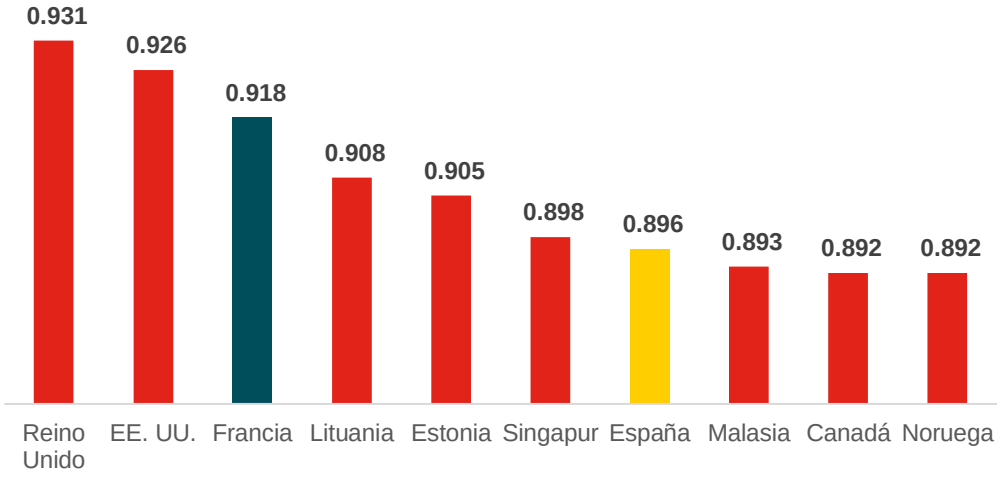
Fuente: Xerfi, Servicios Digitales (noviembre de 2019).

Esta clara tendencia al alza beneficia especialmente a los proveedores de servicios de ciberseguridad por la externalización generalizada de la respuesta a los ciberataques, a causa de una importante **falta de recursos humanos** especializados en las empresas. Además, la demanda se ha visto impulsada por la **reglamentación** cada vez más exigente en el ámbito nacional y europeo que, de alguna manera, obliga a las empresas a contratar servicios de auditoría y control de sus sistemas de ciberseguridad para garantizar la protección de los datos.

Al mismo tiempo, un estudio del gabinete IDC (diciembre de 2018) revela que casi la mitad de las empresas francesas no han establecido todavía una política de detección ni de respuesta a los ciberataques, por lo que es de esperar que el mercado continúe creciendo conforme más empresas tomen conciencia de la necesidad de asegurar sus sistemas. Así, IDC anticipa un tamaño del mercado de alrededor de **4.000 millones de euros en 2022**.

Asimismo, Francia se sitúa en el podio de los países con mayor **grado de compromiso** respecto a la ciberseguridad según el índice GCI (*Global Cybersecurity Index*). Esta clasificación, realizada por la Unión Internacional de Telecomunicaciones (ITU), evalúa el esfuerzo de los países alrededor de cinco grandes pilares estratégicos: legal, técnico, organizativo, desarrollo de capacidades y cooperación.

LOS DIEZ PRIMEROS PAÍSES DEL *RANKING* GCI
(Puntuación sobre 1; año 2018)



Fuente: *Global Cibersecurity Index 2018*, ITU.

B.3. Principales actores

B.3.1. Sector público

En el ámbito público, la principal organización en Francia es la **Anssi** (Agencia Nacional de la Seguridad de los Sistemas de Información). Creada en el año 2009, desde 2011 es la autoridad nacional para la defensa de los sistemas de información del Estado y cuenta con 568 agentes y un presupuesto anual de 100 millones de euros. Se encarga además de la regulación nacional y la vigilancia de su aplicación, y fue el organismo responsable de la transposición a la legislación nacional de la Directiva (UE) 2016/1148, del Parlamento Europeo y del Consejo, de 6 de julio de 2016, conocida por Directiva NIS (de *Network and Information Security*).

Asimismo, la Anssi se ocupa de la auditoría y control de los niveles de seguridad de los llamados **Operadores de Servicios Esenciales (OSE)**, una figura introducida por la Directiva NIS y que señala las organizaciones públicas o privadas que proveen un servicio esencial y que necesitan un control más exhaustivo para proteger la integridad de los países. En 2019, estos operadores son 122, aunque se prevén dos rondas más para la identificación e inclusión de empresas como OSE.

Además, desde 2013 la agencia se encarga de la asistencia y soporte a los **Operadores de Importancia Vital (OIV)**. Los OIV son empresas críticas de la economía francesa, clasificadas como tales en aplicación de la Ley de la Programación Militar (2013), con obligaciones de seguridad aún más rigurosas que en el caso de los OSE. Por ejemplo, estas organizaciones deben pasar un proceso de aprobación de sus sistemas de detección de ataques, informar a la Anssi sobre los ataques que puedan sufrir, y están expuestas a sanciones penales en caso de no respetar sus obligaciones. En total, existen doscientos OIV, repartidos casi al 50 % entre el sector público y el privado, pertenecientes a doce sectores clave de la economía, entre los que se encuentran la energía, la sanidad, los transportes, las finanzas, o la gestión del agua.

En su informe anual de 2018, la Anssi identificó como principales amenazas de seguridad la filtración de datos estratégicos, los ataques indirectos a través de proveedores o prestatarios de servicios, las operaciones de desestabilización o influencia, y el fraude en línea.

B.3.2. Sector privado

El mercado francés de la ciberseguridad atrae a un número creciente de participantes. A las empresas especializadas se les unen, cada vez más, otros operadores del universo digital (IBM, Microsoft), actores de la defensa (Airbus, Thales) y operadores de telecomunicaciones (Orange). Se podría decir que se trata de un mercado todavía muy atomizado, que se está formando, y donde se empiezan a producir numerosas adquisiciones que poco a poco irán consolidando su estructura.

Así, entre las principales operaciones del año destaca la adquisición de la holandesa SecureLink por parte de **Orange Cyberdéfense** en una operación valorada en alrededor de 500 millones de euros. En sentido contrario, también empresas extranjeras están comprando compañías francesas, como es el caso de la adquisición del distribuidor galo Abbakan por parte de la americana **Ingram Micro**.

A pesar de los diferentes dispositivos nacionales para la ayuda a la innovación, las pymes francesas tienen problemas para alcanzar un tamaño crítico que les permita acceder a mercados importantes, especialmente en el plano internacional, por lo que la tendencia se encamina hacia un mercado con participantes de gran tamaño. Además, las grandes compañías digitales como Google, Microsoft o Amazon Web Services han entrado en escena en los últimos tiempos, como muestra la creación de la filial de Google para la ciberseguridad en 2018 bajo el nombre de Chronicle Security.

Entre los principales actores privados en Francia se pueden destacar los siguientes:

- **Thales.** Líder europeo en ciberseguridad y líder mundial en protección de datos. Cubre prácticamente toda la gama de actividades: tecnologías de cifrado, detección, auditoría o *tests* de intrusión. Está presente en 68 países con más de 80.000 empleados en los sectores aeroespacial, defensa, seguridad y transportes. En abril de 2019, Thales completó la adquisición de Gemalto por 4.800 millones de euros, lo que le permite posicionarse como líder mundial en materia de identidad y seguridad digital.

- **Airbus Cybersecurity.** Su misión es proteger a los gobiernos, los organismos de defensa y seguridad, y las infraestructuras nacionales críticas contra las amenazas digitales. Junto con la también francesa Atos consiguió un importante contrato en octubre de 2018 para la protección de los sistemas informáticos de diecisiete instituciones, servicios y agencias de la UE por un periodo de seis años.

- **Atos.** Líder internacional de la transformación digital y con presencia en 73 países, Atos está presente en los sectores de defensa, finanzas, sanidad, industria, energía, sector público, telecomunicaciones y transportes. Desde 1992, Atos es el socio digital de los Juegos Olímpicos, donde gestiona y asegura los servicios informáticos de este evento deportivo que en 2024 tendrá a la ciudad de París como sede.

- **Orange Cyberdéfense.** El operador francés continúa con su estrategia bautizada como *Essentiels 2020* alrededor de cinco grandes pilares, entre los que se encuentran la transformación de las empresas y la ciberseguridad. Además de la adquisición de SecureLink antes mencionada, este año adquirió también la británica SecureData, mostrando una clara disposición a convertirse en un actor clave del mercado de la ciberseguridad. Según sus propias declaraciones, su objetivo estratégico es superar a Atos o IBM en el mercado europeo en los próximos cuatro años.

Las grandes ventajas del mercado francés –como son el crecimiento de los servicios digitales o la regulación favorable, entre otros– se enfrentan sin embargo a un reto de gran importancia: **las dificultades para la contratación** de verdaderos expertos en ciberseguridad. En el estudio *El puzzle imposible de la ciberseguridad* (Sophos, 2018), un 78 % de las compañías francesas entrevistadas declaraban que la contratación de profesionales con las habilidades necesarias supone un verdadero reto para la industria. Esto ha provocado que los sueldos en el sector se hayan disparado en los últimos años, lo que provoca que estos trabajadores se concentren en las grandes empresas proveedoras de servicios, motivando así la externalización de las actividades de ciberseguridad de las empresas hacia estos grandes actores especialistas.

C. LA OFERTA ESPAÑOLA

Como se ha visto antes, el índice GCI ha colocado a **España en séptima posición mundial** en 2018 por el grado de compromiso del país con la ciberseguridad. A pesar de todo, la situación española es parecida a la de Francia, en el sentido de que muchas empresas todavía no se encuentran preparadas para enfrentarse al problema de la seguridad en el entorno digital, y se debe realizar aún un esfuerzo para que se entienda la ciberseguridad como una parte más de la estrategia de los negocios.

En España, las diferentes normas y reglamentos sectoriales son implementados por el **INCIBE** (Instituto Nacional de Ciberseguridad), que además organiza anualmente el **encuentro Enise** en el Palacio de Exposiciones de León con el objetivo de conectar a profesionales del sector con emprendedores y con representantes del mundo académico e investigador a nivel internacional. Existe un claro interés por parte de las empresas españolas de cualquier tamaño por internacionalizarse y comercializar sus productos y servicios en el exterior, incluyendo en Francia.

Según *Business Insider* (2018), entre las principales empresas españolas del sector destacan **ElevenPaths (Telefónica)**, con una cartera de servicios que incluye soluciones de seguridad de los dispositivos, protección de redes, y gestión de identidades y procesos; o **InnoTec System (Entelgy)**, que cuenta con su propio centro de operaciones de seguridad (SOC) y es patrocinador del encuentro Enise, aunque en estos momentos desarrolla su actividad principalmente en España y América Latina.

En este sentido, es importante destacar que, a pesar de la alta demanda de servicios de ciberseguridad en Francia, actualmente las empresas de mayor tamaño prefieren contratar con los grandes grupos especialistas, locales o extranjeros, por motivos de fiabilidad, por lo que, desde ese punto de vista, Francia se podría considerar como un mercado de difícil acceso, al menos, en lo tocante a la contratación con grandes clientes.

D. OPORTUNIDADES DEL MERCADO

Según el informe *Ciberamenaza: aviso de tormenta*, del Institut Montaigne, la actual oferta de productos y servicios de seguridad en Francia está dirigida claramente a las empresas de mayor tamaño, que son, por otra parte, las que mayor concienciación han alcanzado sobre la problemática. Esto significa que las empresas de menor tamaño que pretenden reforzar sus sistemas de seguridad no encuentran servicios adaptados a sus necesidades. Así el Institut Montaigne aboga por una simplificación en los productos de ciberseguridad para adaptarse a la realidad de las pymes galas, lo que puede constituir, en definitiva, una oportunidad para los proveedores españoles de *hardware*, *software* o servicios que decidan acudir a este mercado.

En cualquier caso, las principales oportunidades están relacionadas con las últimas novedades normativas nacionales y europeas, así como con los planes y estrategias sectoriales de Francia en materia de ciberseguridad que se recogen a continuación. En conjunto, suponen una mayor concienciación respecto al problema de la seguridad, establecen unas reglas más rigurosas que requieren actualización por parte de las empresas, y fomentan una mayor inversión en estos productos y servicios:

- **Ley de Programación Militar (2013).** Establece una serie de obligaciones adicionales para los considerados operadores de importancia vital (OIV) en materia de aseguramiento de sus redes, lo que incluye la necesidad de una mejor cualificación de sus sistemas de detección, información sobre los ataques sufridos, y la sumisión a controles externos.

- **Estrategia Nacional para la Seguridad Digital (2015).** Se basa en cinco líneas de acción: garantizar la soberanía nacional, aportar una respuesta fuerte contra los ataques informáticos, informar al gran público, convertir la seguridad digital en una ventaja competitiva para las empresas francesas (a través del apoyo a la inversión, la innovación y la exportación), y reforzar el papel internacional de Francia en esta materia.

- **Plan de Ciberseguridad (2015).** Entre sus acciones destacan la necesidad de colocar a la ciberseguridad en el centro de la gobernanza de las empresas y crear una "marca Francia" en el sector con prioridad para la contratación pública. El objetivo a corto plazo es aumentar las ventas francesas un 20 % anual. A medio plazo, los objetivos son reforzar la formación de los especialistas franceses, fomentar la creación de fondos de inversión privados para el sector, y apoyar la consolidación de la industria de la ciberseguridad.

- **Directiva NIS.** Adoptada en julio de 2016 por el Parlamento Europeo y el Consejo. Refuerza las capacidades nacionales en materia de ciberseguridad, establece un marco de cooperación entre Estados Miembros, e instaura unas reglas europeas comunes en materia de ciberseguridad para los prestatarios de servicios digitales. La transposición al ordenamiento jurídico francés se realizó en mayo de 2018, con la participación de Anssi.

- **Reglamento General de Protección de Datos (2016).** Refuerza los derechos existentes y establece un mejor control de los datos de carácter personal para la protección de los ciudadanos. Al mismo tiempo, implanta nuevas obligaciones para las empresas en cuanto al manejo y custodia de esa información personal.

D.1. Distribución

El **sector público** es uno de los mayores clientes de productos y servicios de ciberseguridad. Sin embargo, como se verá más adelante, las compras públicas están limitadas de alguna manera ya que es la agencia Anssi la que debe certificar los productos y, desde 2014, se ha dado preferencia a la contratación con las empresas nacionales. El **sector privado** tiene, asimismo, una serie de requisitos no formales que son comunes a multitud de sectores en Francia. Estos requisitos normalmente están relacionados con la necesidad de contar con una presencia física en el país, una cartera de proyectos anteriores o unas relaciones de confianza con actores del panorama nacional.

D.2. Barreras reglamentarias y no reglamentarias

Con el objetivo de responder a los riesgos de espionaje y ataques informáticos, el 20 de febrero de 2014 el entonces primer ministro francés, Jean-Marc Ayrault, anunció que las administraciones debían acudir únicamente a los

productos y servicios de seguridad informática **certificados por la Anssi**. Un año más tarde, el Plan de Ciberseguridad incluía entre sus objetivos desarrollar ofertas nacionales de confianza para las necesidades de Francia, y entre sus acciones señalaba que se priorizaban estos **sellos de calidad** en las compras públicas. En la práctica, esto supone una clara ventaja para la industria local, al mismo tiempo que dificulta el acceso de los vendedores extranjeros a los contratos públicos.

Además, en el campo de las inversiones extranjeras, Francia establece doce sectores de actividad donde las inversiones desde el exterior necesitarán de una **autorización previa**, según señala el Código Monetario y Financiero tras el Decreto n.° 2014-479. Entre estos sectores, se incluyen las actividades relativas a la seguridad de los sistemas de información de una compañía relacionada por contrato con un operador público o privado que gestione instalaciones de importancia vital, y también otras actividades que resulten esenciales para la garantía de los intereses del país en materia de orden público, de seguridad pública o de defensa nacional, como el aprovisionamiento de energía, agua, transporte, redes de comunicaciones electrónicas o sanidad.

D.3. Ayudas si existen

En Francia existen una serie de dispositivos que, sin ser específicos de la industria de la ciberseguridad, pueden favorecer el desarrollo de las empresas participantes en el sector.

Así, en primer lugar, destacan los **incentivos fiscales** para empresas e investigadores con el objetivo de favorecer la innovación. Entre ellos, los más importantes son el *Crédit d'Impôt Recherche* (CIR) y el *Crédit d'Impôt Innovation* (CII). El CRI tiene una limitación del 30 % de los gastos (hasta un máximo de 100 millones de euros) y del 5 % a partir de esa cifra, y puede cubrir gastos de personal o de bienes y edificios relacionados con la investigación. El CII está reservado a las pymes y cubre hasta un 20 % de los gastos relacionados con la concepción o la realización de prototipos o de instalaciones piloto de algún producto innovador.

Asimismo, **Bpifrance** cuenta con distintos dispositivos que facilitan **financiación** para las actividades relacionadas con la innovación, entre los que destaca la **ayuda a la innovación**. Bajo la forma de subvención o de anticipo reembolsable, esta ayuda se dirige a empresas de cualquier tamaño, incluso en fases iniciales, si el proyecto implica una innovación reconocida. La ayuda es financiada por dotaciones del Estado, de las administraciones o de la Unión Europea.

D.4. Ferias

Forum International de la Cybersécurité
Lille Grand Palais. 28-30 de enero de 2020
https://www.forum-fic.com/accueil.htm

El foro internacional de la ciberseguridad es el evento de referencia en Europa en materia de seguridad digital. En la edición de 2019 se dieron cita más de 10.000 participantes de 80 países. Entre sus objetivos se encuentra la apuesta por favorecer la innovación, la construcción de puentes entre los esferas públicas y privadas, y la promoción de un verdadero mercado europeo de ciberseguridad.

E. INFORMACIÓN ADICIONAL

E.1. Asociaciones

- Alliance pour la Confiance Numérique: https://www.confiance-numerique.fr/
- Tech in France: https://www.techinfrance.fr/
- Hexatrust: https://www.hexatrust.com/

E.2. Instituciones oficiales

- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI): https://www.ssi.gouv.fr/
- Bpifrance: https://www.bpifrance.fr/
- Institut National de la Statistique et des Études Économiques (INSEE): https://www.insee.fr/fr/accueil

E.3. Fuentes de información

- XERFI – Estudios sectoriales:
  - *Les Enjeux et stratégies gagnantes sur le marché de la cybersécurité* – junio de 2019
  - *Les Services numériques* – noviembre de 2019

E.4. Otras direcciones de interés

- CyberDB – The Cyber Research Databank: https://www.cyberdb.co/database/france/page/3/
- INCIBE: https://www.incibe.es/
- International Data Corporation (IDC): https://www.idc.com/
- International Telecommunication Union (ITU): https://www.itu.int/en/Pages/default.aspx

E.5. Publicaciones del sector

- *L'Usine Nouvelle*: https://www.usinenouvelle.com/

F. CONTACTO

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

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

13 rue Paul Valéry
PARÍS 75016 – Francia
Teléfono: +33 153 579 550
Email: paris@comercio.mineco.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
900 349 000 (9 a 18 h L-V)
informacion@icex.es

AUTOR
Félix González García

Oficina Económica y Comercial
de España en París
Buzón oficial de la Oficina: paris@comercio.mineco.es
Fecha: 17/12/2019

NIPO: 114-19-040-2

www.icex.es

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO · ICEX España Exportación e Inversiones